Oracle Utilities Smart Grid Gateway

Installation Guide

Release 2.4.0.0.0

F38825-01

April 2021

Oracle Utilities Smart Grid Gateway Installation Guide,

Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Appendix A

Appendix B

Appendix C

Appendix D

Preface

Welcome to the Oracle Utilities Smart Grid Gateway Installation Guide.

This guide provides instructions to install Oracle Utilities Smart Grid Gateway.

The preface includes:

- Audience
- Related Documents
- Updates to this Documentation
- Conventions
- Acronyms
- Additional Resources

Audience

This guide is intended for database administrators who will be installing and maintaining the database for Oracle Utilities Smart Grid Gateway.

To complete installation you should have:

- Administrative privileges on the host where you are installing the software.
- Experience installing and configuring application servers and other software.

Related Documents

The following documentation is included with this release.

Installation Guides and Release Notes

- *Oracle Utilities Smart Grid Gateway Release Notes*
- *Oracle Utilities Smart Grid Gateway Quick Install Guide*
- *Oracle Utilities Smart Grid Gateway Installation Guide*
- *Oracle Utilities Smart Grid Gateway Database Administrator's Guide*
- *Oracle Utilities Smart Grid Gateway Licensing Information User Manual*

Configuration and User Guides

- *Oracle Utilities Meter Solution Business User Guide*
- *Oracle Utilities Meter Solution Administrative User Guide*

Supplemental Documents

- *Server Administration Guide*
- *Security Guide*

Updates to this Documentation

This documentation is provided with the version of the product indicated. For latest updates to documentation visit Oracle Technology Network.

Additional and updated information about the operations and configuration of the product is available on My Oracle Support.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Acronyms

The following acronyms and terms are used in this document:

Acronym	Definition
ADF	Oracle Application Development Framework
EAR	Enterprise Archive
EJB	Enterprise JavaBeans
HTML	HyperText Markup Language
JAR	Java Archive
JDBC	Java database connectivity
JMX	Java Management Extensions
JNDI	Java Naming and Directory Interface
JSP	JavaServer Pages
JVM	Java Virtual Machine.
MPL	Multi Purpose Listener
OUAF	Oracle Utilities Application Framework
OAM	Oracle Access Manager
OIM	Oracle Identity Management
ONS	Oracle Notification Service
OSB	Oracle Service Bus
Oracle RAC FCF	Oracle Real Application Clusters Fast Connection Failover
RMI	Remote Method Invocation
SOAP	Simple Object Access Protocol

Acronym	Definition
SOA	Service-oriented architecture
SPLEBASE	The location where the application will be installed.
SPLOUTPUT	This location is used for storing batch log files and output from batch jobs
WAR	Web application Archive
WLS	WebLogic
XAIApp	XML Application Integration

Additional Resources

For more information and support, visit the Oracle Support website.

Chapter 1

Introduction

This chapter provides an overview of the Oracle Utilities Smart Grid Gateway installation. It includes the following sections:

- Installation Overview
- Application Architecture
- Installation Components
- Installation Types
- Media Pack Components

Installation Overview

Installing Oracle Utilities Smart Grid Gateway involves the following steps:

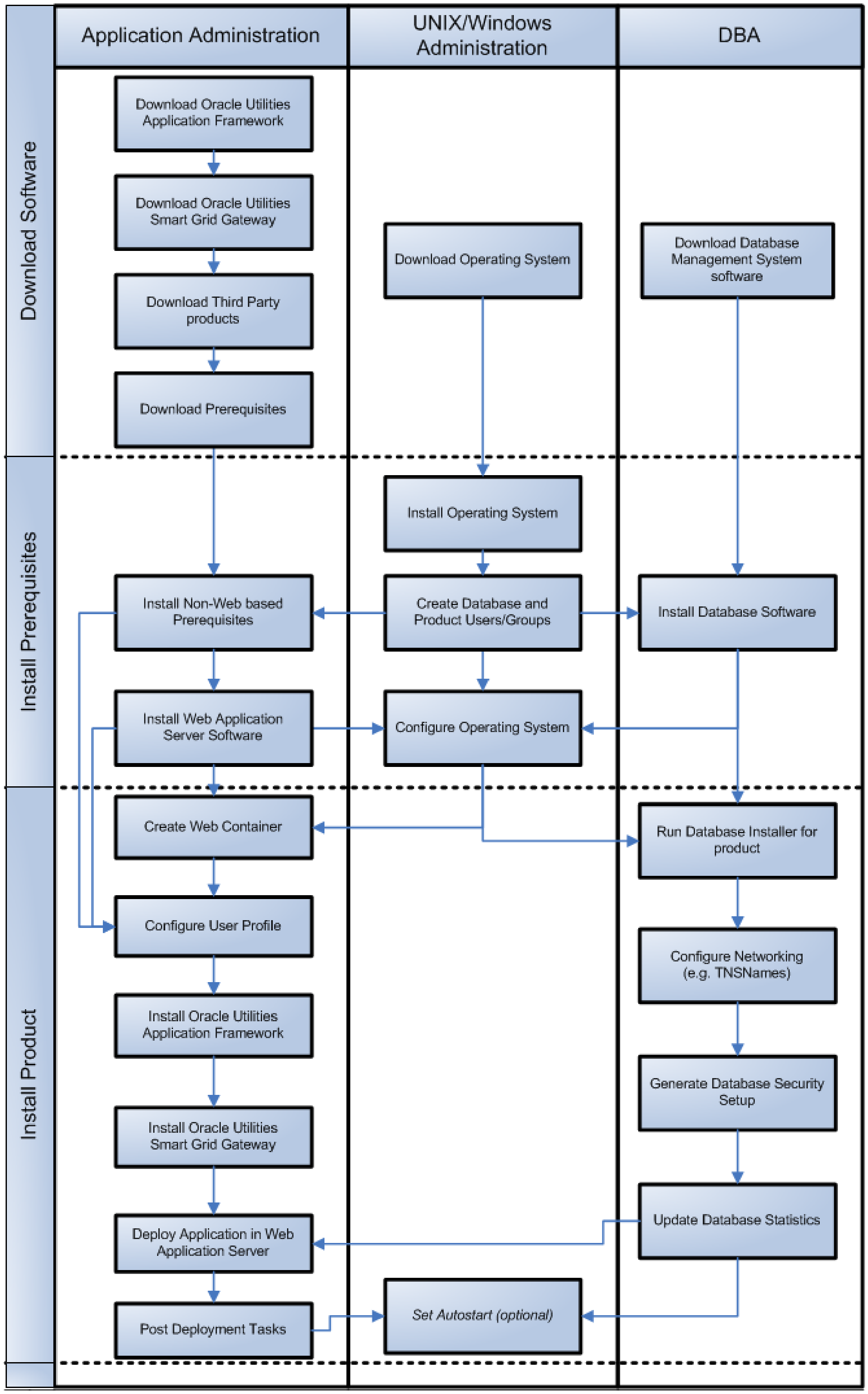
> **Note**: For instructions to install Oracle Utilities Service Order Management, refer to Chapter 8: Installing Oracle Utilities Service Order Management.

1. Review the different tiers of the application architecture as described in Application Architecture.
2. Understand the hardware requirements for installing the application and the supported platforms for the application and database servers as described in Chapter 2: Supported Platforms and Hardware Requirements.

   > **Note:** The installation and administration of the database server tier is described in detail in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide.*
3. Plan your installation as described in Chapter 3: Planning the Installation. This chapter includes lists of the required software for each supported combination of operating system and application server.
4. Install the database as described in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide.*

   > **Note**: When implementing Oracle Utilities Smart Grid Gateway with Oracle Utilities Meter Data Management, both the Smart Grid Gateway and Meter Data Management database components should be installed in the same database.
5. Install all required third-party software as described in Chapter 3: Installing Prerequisite Software. The required software is listed for each supported combination of operating system and application server.
6. Install the Oracle Utilities Application Framework.
7. Install Oracle Utilities Smart Grid Gateway.
8. Complete the post-installation and configuration tasks for your Oracle Utilities Smart Grid Gateway adapter as described in Chapter 7: Configuring the Oracle Utilities Smart Grid Gateway Adapters.
9. Follow the installation guidelines described in Chapter 9: Additional Tasks.

The following diagram provides an overview of the steps to install and configure Oracle Utilities Smart Grid Gateway:


Application Administration
UNIX/Windows Administration
DBA
Download Software
Install Prerequisites
Install Product
Download Oracle Utilities Application Framework
Download Oracle Utilities Smart Grid Gateway
Download Third Party products
Download Prerequisites
Download Operating System
Download Database Management System software
Install Operating System
Install Non-Web based Prerequisites
Create Database and Product Users/Groups
Install Database Software
Install Web Application Server Software
Configure Operating System
Create Web Container
Run Database Installer for product
Configure User Profile
Configure Networking (e.g. TNSNames)
Install Oracle Utilities Application Framework
Generate Database Security Setup
Install Oracle Utilities Smart Grid Gateway
Update Database Statistics
Deploy Application in Web Application Server
Post Deployment Tasks
Set Autostart (optional)

Application Architecture

The Oracle Utilities Smart Grid Gateway application is deployed on multiple tiers.

Refer to the *Server Administration Guide* (included in this release) for a more detailed description of the application architecture and individual tiers.

Tier 1: Desktop/Client, or Presentation Tier

This tier is implemented in a browser-based client. Users use a desktop client web browser to log in to and use the Oracle Utilities Smart Grid Gateway application. Note also that a desktop machine running Microsoft Windows and the Oracle client is required to perform some of the Oracle Utilities Smart Grid Gateway product installation steps.

Tier 2: Web Application Server, Business Application Server, Batch Server Tier

This tier is implemented in a web application server, business application server, or the batch server. The business application component can be installed as part of the web application server, or as a separate component. Except where explicitly noted, most of the Oracle Utilities Smart Grid Gateway installation documentation assumes that the web application and business application servers reside together. The batch infrastructure also runs within this tier. There can be multiple batch server instances serving the application.

Tier 3: Database, or Persistence Tier

This tier is implemented in a database server. The database server stores data maintained by the Oracle Utilities Smart Grid Gateway application. More specifically, the database tier contains the data server files and database executables that physically store the tables, indexes, and other database objects for your system.

Installation Components

The Oracle Utilities Smart Grid Gateway product installation consists of the following components:

- Database Components
    - Oracle Utilities Application Framework database
    - Oracle Utilities Meter Data Management database
- Application Components
    - Oracle Utilities Application Framework application
    - Oracle Utilities Meter Data Management application

For a successful installation, you must install ALL of the above components.

Installation Types

The first step in the installation procedure is to determine the installation type that meets your business requirements. The following are the possible installation types:

- Initial Installation - A base installation, typically used for a production environment.
- Demo Installation - A base installation with pre-populated demo data, typically used for demonstration or training purposes.
- Upgrade Installation - An upgrade installation from V2.3.0.2.0 to V2.4.0.0.0

See Recommendations for Creating a Production Environment for information about which installation type is appropriate for a production environment.

The following sections describe these installation types in detail.

Initial Installation

This installation type is applicable when installing Oracle Utilities Smart Grid Gateway for the first time or from scratch. For an initial install, you must install all of the following components:

- Database components

  Refer to the **Initial Install** section in *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for more information.

- Application components
  - Oracle Utilities Application Framework application
  - Oracle Utilities Meter Data Management application

  Refer to Chapter 4: Installing Oracle Utilities Smart Grid Gateway—Initial Installation for the instructions for installing these components.

Demo Installation

This installation type is applicable when installing a demo application of Oracle Utilities Smart Grid Gateway for demonstration or training purposes. For a demo install, you must install all of the following components:

- Demo Database components

  Refer to the **Demo Install** section in *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for more information.

- Application components
  - Oracle Utilities Application Framework application
  - Oracle Utilities Meter Data Management application

  Refer to Chapter 5: Installing Oracle Utilities Smart Grid Gateway—Demo Installation for the instructions for installing these components.

Upgrade Installation

This installation type is applicable when upgrading Oracle Utilities Smart Grid Gateway from V2.3.0.2.0 to V2.4.0.0.0.

> **Note:** If you have a version prior to 2.3.0.2.0, upgrade to 2.3.0.2.0 before upgrading to 2.4.0.0.0.

For an upgrade, you must upgrade all of the following components:

- Database components

  Refer to the **Upgrade Install** section in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for more information.

- Application components

  - Oracle Utilities Application Framework application
  - Oracle Utilities Meter Data Management application

  Refer to Chapter 6: Installing Oracle Utilities Smart Grid Gateway—Upgrade Installation for instructions to install these components.

Recommendations for Creating a Production Environment

For a production environment, Oracle recommends that you use the Initial Installation installation type as described above.

If there is any custom configuration that needs to be migrated from a development or “gold” environment into production, the migration can be done by using the Configuration Migration Assistant (CMA).

Oracle does not recommend creating a production environment by using the Demo Installation installation type or by cloning an existing Demo installation.

Media Pack Components

The Oracle Utilities Smart Grid Gateway Media Pack consists of the following packages:

Documentation Packages

- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 Release Notes
- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 Quick Install Guide
- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 Install Documentation
- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 User Documentation
- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 Supplemental Documentation
- Oracle Utilities Service Order Management V2.4.0.0.0 User Documentation

Installation Packages

- Oracle Utilities Smart Grid Gateway V2.4.0.0.0 Multiplatform
- Oracle Utilities Application Framework V4.4.0.3.0 Multiplatform
- Oracle Utilities Application Framework V4.4.0.3.0 Oracle Database

Chapter 2

Supported Platforms and Hardware Requirements

This section provides an overview of the tiers on which the product is implemented, and shows each of the operating system/server combinations that the product is certified for, including:

- Software and Hardware Considerations
- Operating Systems and Application Servers
- Hardware Requirements
- Application Server Memory Requirements
- Support for Software Patches and Upgrades

Software and Hardware Considerations

There are many factors that can influence software and hardware decisions. For example, your system may have to satisfy specific performance, availability, or scalability requirements, or to support running in a language other than English. These business requirements, together with the chosen system architecture, should be used in initial software and hardware planning.

Some of the questions that you should answer before beginning the installation include:

- On which hardware platform and operating system will Oracle Utilities Smart Grid Gateway be deployed?
- On which web server product will Oracle Utilities Smart Grid Gateway deploy?
- On which database product will Oracle Utilities Smart Grid Gateway deploy?
- Do you plan to deploy multiple Oracle Utilities Smart Grid Gateway instances on the same physical server?
- How do you plan to deploy Oracle Utilities Smart Grid Gateway?
  - Web/application/database on the same physical server
  - Web/application on one server and database on separate server
  - Each component on its own server

For detailed descriptions of various deployment architecture choices that may aid in planning, refer to the *Oracle Utilities Application Framework Architecture Guidelines (Article ID 807068.1)* document available on My Oracle Support.

The final hardware and software decisions must comply with the specific requirements of Oracle Utilities Smart Grid Gateway.

Operating Systems and Application Servers

This section provides information on the operation system, web browser and OSB and SOA adapter combinations that are supported. Refer to the notes below the table for additional details regarding WebLogic support.

> **Note**: SOA Suite (including OSB) is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

This section details the operating system and application server combinations on which this version of Oracle Utilities Smart Grid Gateway is supported.

Application Server Operating Systems

- Oracle Linux 7.x for x86_64*
- Oracle Linux 8.x for x86_64
- Oracle Solaris 11.4+ for SPARC (64-bit)
- IBM AIX 7.1 TL5 for POWER (64-bit)
- IBM AIX 7.2. TL3+ for POWER (64-bit)

* For Oracle Linux 7.x, refer to the Oracle Lifetime Support Policy: Oracle and Sun System Software and Operating Systems document for the applicable end of support dates.

Prerequisite Application Server Software

- Oracle Database Client 19c
- Oracle Java SE Development Kit 1.8.0_261 (Windows, Solaris and Linux platforms only)
- IBM 64-bit SDK for AIX 8.0.0.x (IBM platforms only)
- Select jars from Hibernate ORM 4.1.0
- Oracle WebLogic Server 12c (Release 12.2.1.4) 64-bit

Notes

- Oracle Linux is 100% user space-compatible with Red Hat Enterprise Linux, therefore, Oracle Utilities Application Framework is also supported on Red Hat Enterprise Linux.
- Refer to the *Oracle Utilities Application Framework Database Administrator's Guide* for the Oracle database server requirements.

Refer to the *Certification Matrix for Oracle Utilities Products (Document ID 1454143.1)* document on My Oracle Support to determine if support for newer versions of the listed products have been added.

Please note the following:

- Version numbers marked with a "+" are the MINIMUM version supported. That version and all future 4th digit updates will be supported.

  Example: Oracle 12.1.0.2+ means that 12.1.0.2 and any higher 12.1.0.x versions of Oracle are supported.
- An "x" indicates that any version of the digit designed by the "x" is supported.

  Example: Linux 8.x indicates that any version of Linux 8 (8.0, 8.1, 8.2 etc) will be supported.

Windows Server

- Windows Server is **not** supported for Production environments. Wherever Windows Server is referenced within this guide, it is supported for Test or Development environments **only**.

WebLogic Server

- Oracle WebLogic Server (Fusion Middleware Infrastructure) Release 12.2.1.4
- Although Oracle Utilities Smart Grid Gateway is supported only on the Oracle WebLogic application server, it can write to any JMS compliant queuing application by way of Oracle Service Bus. For more information about Oracle Service Bus, refer to the *Oracle Fusion Middleware Developers Guide for Oracle Service Bus*.
- **OSB and SOA Adapters are only supported on WebLogic V12.2.1.4. The browser version supports V12.2.1.x.

- Oracle Utilities Service Order Management is only supported on WebLogic V12.2.1.x.
- Customers must download Oracle WebLogic Server from the Oracle Software Delivery Cloud.

Oracle Database Server

Prerequisite database server software (on any vendor supported platform where x is vendor supported version):

- Oracle Database Server Enterprise Edition 19c
- Oracle Database Server Standard Edition 2 19c

  Note: Oracle Database Enterprise Edition and the Partitioning and Advanced Compression options are strongly recommended in all situations.

Oracle VM Support

This version of Oracle Utilities Smart Grid Gateway is supported on Oracle VM Server for x86 for supported releases of Oracle Linux and Microsoft Windows operating systems.

Refer to My Oracle Support knowledge base article 249212.1 for Oracle's support policy on VMWare.

Hardware Requirements

This section provides information on client side hardware requirements for Oracle Utilities Smart Grid Gateway.

Configuration	Processor	Memory (RAM)	Monitor (Display)
Minimum	Pentium IV - 2.0 GHz	1024 MB	1024X768** 16-bit Color
Recommended*	Pentium IV -3.0+ GHz, (or) any Core 2 Duo (or) any Athlon X2	2048 MB	1280X1024** 32-bit Color

* The Recommended configuration supports better performance of the client.

** To reduce the amount of scrolling required for pages that are longer than 768 or 1024 pixels, consider placing a monitor into vertical position (with narrow side on the bottom).

Application Server Memory Requirements

For each application server environment a minimum of 4 GB of real memory is required, plus 6 GB of swap space. The approximate disk space requirements in a standard installation are as follows (the size represents the MINIMUM required):

Location	Size	Usage
Install Dir ("$SPLEBASE") Location	10 GB recommended 5 GB minimum	This is the location where the application and Framework get installed. Startup, shutdown and other online log files are stored here. The size and space that is used should be monitored because various debugging options can significantly affect the size of log files. **Note**: This does not include the size of the edge product.
Log Dir ("$SPLOUTPUT") Location	10 GB recommended 2 GB minimum	This location is used for storing batch log files and output from batch jobs. The size of this space should be influenced by which batches are run and how often, and the amount of debugging information that is collected.
Location of the application web work files on the web servers	5 GB recommended 2 GB minimum	This location is used by various web server vendors to expand the application. It should be considered when installing these products. Refer to the individual web server documentation to determine the location of the temporary files.
Installation Temporary Area	10 GB minimum	The application gets installed from this location. You need enough space to un-compress the files and install the application.
Oracle Data Area	10 GB minimum	This location is where the Oracle database data files are stored. The size of this space should be based on the requirements of the production environment. For an initial or demo database install 4 GB should be sufficient.

Support for Software Patches and Upgrades

Due to the ongoing nature of software improvement, vendors will periodically issue patches and service packs for the operating systems, application servers and database servers on top of specific versions that Oracle products have already been tested against.

If it is necessary to apply an upgrade, please do so in a test environment that is running on the same platform as your production environment prior to updating the production environment itself. The exception to this is Hibernate software 4.1.0 which should not be upgraded.

Always contact Oracle Support prior to applying vendor updates that do not guarantee backward compatibility.

Chapter 3

Planning the Installation

This chapter provides information for planning an Oracle Utilities Smart Grid Gateway installation, including:

- Before You Install
- Prerequisite Software List
- Installing Prerequisite Software
- Additional Prerequisite Software Information
- Readiness Checklist

Before You Install

Visit My Oracle Support for up-to-date additional information about installing Oracle Utilities Smart Grid Gateway.

WebLogic Native Installation

With Oracle Utilities Application Framework 4.4.0.3.0, a WebLogic native installation is required. Refer to the *Oracle WebLogic 12.2.1.x Configuration Guide for Oracle Utilities Framework (Doc ID 2413918.1)* document on My Oracle Support for more information.

Application Server Clustering

If you are considering application server clustering, refer to the *Oracle WebLogic 12.2.1.x Configuration Guide for Oracle Utilities Framework (Doc ID 2413918.1)* document on My Oracle Support.

Additional information about WebLogic clustering, refer to the Fusion Middleware Using Clusters for Oracle WebLogic Server documentation.

Directory Names

Directory cannot contain whitespace characters.

Prerequisite Software List

Before you install Oracle Utilities Smart Grid Gateway, you must install prerequisite software.

Refer to the respective installation documentation of the software for instructions on downloading and installing.

Prerequisite Software for Database Server

The prerequisite software for the database component of Oracle Utilities Smart Grid Gateway is as follows:

- **Oracle Database Server 19c** - This is required for installing the database component of the Oracle Utilities Smart Grid Gateway product. The following version of the database server is supported:

  - Oracle Database Enterprise Edition

  Important: Oracle Database Enterprise Edition and the Partitioning and Advanced Compression options are strongly recommended in all situations.

Prerequisite Software for Application Server

The prerequisite software for the application component of Oracle Utilities Smart Grid Gateway is as follows:

- Oracle Database 19c Client
- JDK 1.8.0_261+ (64-bit)
- Oracle WebLogic 12c (12.2.1.4)

  Note: Only WebLogic Fusion Middleware Infrastructure Installer should be used.
- Hibernate 4.1.0 Final
- Oracle Service Bus 12.2.1.4

  Oracle Service Bus is required for an implementation that plans to use a productized adapter or the Adapter Development Kit to process meter reading or device event data.

  Note: Oracle Service Bus 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.
- Oracle SOA Suite 12.2.1.4

  Oracle SOA Suite (specifically, BPEL Process Manager) is required for middleware implementations that plan to use a productized adapter or the Adapter Development Kit to implement two-way communications for processing meter commands.

  Note: SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

Oracle Security Fix Updates

It is recommended that you keep the Oracle prerequisite software up to date with the latest security fixes provided by Oracle.

Web Browser Requirements

The web browsers listed below are supported when used on each of the operating systems indicated:

Browser	Windows Operating System
Microsoft Edge for Business 81+ (Edge Chromium)	Microsoft Windows 10 Version x 64-bit
Mozilla Firefox ESR 78.x	Microsoft Windows 10 Version x 64-bit
Google Chrome Enterprise 81+	Microsoft Windows 10 Version x 64-bit
Apple Mobile Safari	Apple iPad iOS 12.x

Installing Prerequisite Software

This section describes the software that needs to be installed for each of the supported operating system and application server combinations. The sections for this chapter are:

- AIX 7.1 TL5/ AIX 7.2 TL3+ Application Server
- Oracle Linux 7.x/8.x or Red Hat Linux 7.x/8.x Operating System
- Oracle Solaris 11 Application Server
- Windows Server 2012 R2 Application Server

AIX 7.1 TL5/ AIX 7.2 TL3+ Application Server

This section describes the software requirements for operating the application using the AIX application server.

Supported Application Servers

Operating System	Chipsets	Application Server
AIX 7.1 TL5/ AIX 7.2 TL3+	POWER 64-bit	Oracle WebLogic 12c (12.2.1.4) 64-bit

AIX 7.1 TL5 Operating System Running on Power5 and Power6 Architecture

UNIX Administrator User ID

The following user groups and accounts have to be created to install and administer the application:

Description	Default Value	Customer Defined Value
Oracle Utilities Smart Grid Gateway Administrator User ID	cissys	
Oracle Utilities Smart Grid Gateway User Group	cisusr	

Note: It is recommended that you change the default values for security reasons.

Throughout this document the administrator user id is often referred to as the “cissys” user id. You should substitute that with the customer defined user id when not using the default value. After the initial install, the software should always be managed using that user id.

By default, the cissys user ID is the only one given access to the installed files.

1. Create a group ‘cisusr’ (user group).

2. Create a user ‘cissys’. Primary group cisusr. Set the primary shell for the cissys user to Korn Shell.

The shell scripts use the “>” to overwrite shell functionality. Your operating system may be configured to not allow this functionality by default in the users shell.

To avoid file access permission problems when executing scripts, consider placing the following command into cissys profile script:

```
set +o noclobber
```

Security Configuration

Various options exist to secure a system. In this application all files will be created with the minimum permissions required to ensure that group-readable, group-writable, and group-executable files will have the correct user groups and to restrict the permissions available to legitimate users. In this way, a low privileged end user cannot directly edit configuration files and thereby bypass application security controls.

The following users and group categories must be defined to implement this security. For demonstration purposes the following users and groups will be used. These users must be created according to industry standards (including password policies). All users should be created with a default umask of 022 to ensure files created during normal operation have the correct permissions.

Please replace these users and groups for your installation defaults:

User	Group	Description
cissys	cisusr	This user will be used to install the application and to apply patches. This user will own all the application files. The same care should be taken with this user ID as if it is 'root'. This user will be able to add, delete, and modify all the files within the application.
cisadm	cisusr	Administrative and Operation functions will be available to this user. This user will be able to stop and start the application and batch processes, but will not have access to modify any file other than generated log files
cisoper	-------	Low level operator. This user will only be able to read logs files and collect information for debugging and investigative purposes. Care should be taken in production to disable debugging as debugging information could contain potential sensitive data which this user should not have privy to.

Note: The Oracle Client and WebLogic should be installed as the user who will stop and start the application. For example, if you plan to run the application as the install user these components must belong to cissys.

Oracle Client 19c - Runtime Option

Install the Oracle Client as described in the Oracle Client installation documentation. Use the cissys account to install the Oracle Client. If another user installs the Oracle Client, make sure the cissys user ID has the proper execute permissions.

For the cissys user ID, ensure that the environment variable ORACLE_CLIENT_HOME is set up, and that ORACLE_CLIENT_HOME/perl/bin is the first Perl listed in the cissys account's PATH variable.

IBM Java Software Development Kit v8.0 SR15 64-bit, IBM SDK, Java Technology Edition v8.0

Installation of Java is a prerequisite for using Oracle WebLogic as a web application server.

At the time of release, AIX Java packages could be obtained from:

http://www.ibm.com/developerworks/java/jdk/aix/service.html

The web server requires the 64-bit Java platform in order to function. The main prerequisite for the web server is the version of java mentioned above.

For the Administrator user ID (cissys), make sure that the environment variable JAVA_HOME is set up, and that "java" can be found in cissys' PATH variable.

Hibernate 4.1.0 FINAL

You must install Hibernate before installing the product.

To install Hibernate external jar files to the Hibernate 3rd party jars depot:

1. Create a Hibernate jar external depot:

   ```
   export HIBERNATE_JAR_DIR=<Hibernate 3rd party jars depot>
   ```

2. Download the hibernate-release-4.1.0.Final.zip file from http://sourceforge.net/projects/hibernate/files/hibernate4/.
3. Click the "4.1.0.Final" link to download the zip file.
4. Extract the contents of the archive file:

   ```
   unzip hibernate-release-4.1.0.Final.zip
   ```

   > **Note**: You must have Java JDK installed on the machine to use the jar command. Make sure you install the JDK supported for your platform.

5. Copy the jar files to your Hibernate jar directory ($HIBERNATE_JAR_DIR) using the following commands:

   ```
   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/ ehcache-
   core-2.5.2.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/hibernate-
   ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-commons-
   annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-core-
   4.1.0.Final.jar $HIBERNATE_JAR_DIR
   ```

```
cp hibernate-release-4.1.0.Final/lib/required/hibernate-jpa-2.0-
api-1.0.1.Final.jar $HIBERNATE_JAR_DIR

cp hibernate-release-4.1.0.Final/lib/required/javassist-3.15.0-
GA.jar $HIBERNATE_JAR_DIR

cp hibernate-release-4.1.0.Final/lib/required/jboss-logging-
3.3.0.Final.jar $HIBERNATE_JAR_DIR

cp hibernate-release-4.1.0.Final/lib/required/jboss-transaction-
api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
```

Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle WebLogic software can be downloaded from the Oracle website. This application server will run as a 64-bit application.

- Download and install 64-bit Java (as documented above) before installing WebLogic.
- Download and install WebLogic Fusion Middleware Infrastructure Installer.

Oracle Service Bus 12.2.1.4

Oracle Service Bus is required for implementations that plan to use middleware implementations of adapters or the generic adapter to process meter reading or device event data.

Oracle Service Bus is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle Service Bus 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle Service Bus must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle Service Bus can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle SOA Suite 12.2.1.4

Oracle SOA Suite, specifically BPEL Process Manager, is required for implementations that plan to use middleware implementations of adapters or the generic adapter to implement two-way communications for processing meter commands.

SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle SOA Suite 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle SOA Suite must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle SOA Suite can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle Linux 7.x/8.x or Red Hat Linux 7.x/8.x Operating System

This section describes the software requirements for operating the application using the Oracle Linux or Red Hat Linux application server.

Supported Application Servers

Operating System	Chipsets	Application Server
Oracle Linux 7.x/8.x (64-bit) based on Red Hat Enterprise Linux (64- bit)	x86_64	Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle Linux or Red Hat Enterprise Linux Operating System Running on x86_64 64-bit Architecture

UNIX Administrator User ID

The following user groups and accounts have to be created to install and administer the application:

Description	Default Value	Customer Defined Value
Oracle Utilities Smart Grid Gateway Administrator User ID	cissys	
Oracle Utilities Smart Grid Gateway User Group	cisusr	

Note: It is recommended that you change the default values for security reasons.

Throughout this document the administrator user ID is often referred to as the “cissys” user id. You should substitute that with the customer defined user ID when not using the default value. After the initial install, the software should always be managed using that user id.

By default, the cissys user ID is the only one given access to the files installed.

1. Create a group called cisusr (user group).
2. Create a user called cissys. Primary group cisusr. Set the primary shell for the cissys user to Korn Shell.

The shell scripts use the “>” to overwrite shell functionality. Your operating system may be configured to not allow this functionality by default in the users shell.

To avoid file access permission problems when executing scripts, consider placing the following command into cissys profile script:

```
set +o noclobber
```

Security Configuration

Various options exist to secure a system. In this application all files will be created with the minimum permissions required to ensure that group-readable, group-writable, and group-executable files will have the correct user groups and to restrict the permissions available to legitimate users. In this way, a low privileged end user cannot directly edit configuration files and thereby bypass application security controls.

The following users and group categories must be defined to implement this security. For demonstration purposes the following users and groups will be used. These users must be created according to industry standards (including password policies). All users should be created with a default umask of 022 to ensure files created during normal operation have the correct permissions.

Please replace these users and groups for your installation defaults:

User	Group	Description
cissys	cisusr	This user will be used to install the application and to apply patches. This user will own all the application files. The same care should be taken with this user ID as if it is 'root'. This user will be able to add, delete, and modify all the files within the application.
cisadm	cisusr	Administrative and Operation functions will be available to this user. This user will be able to stop and start the application and batch processes, but will not have access to modify any file other than generated log files
cisoper	-------	Low level operator. This user will only be able to read logs files and collect information for debugging and investigative purposes. Care should be taken in production to disable debugging as debugging information could contain potential sensitive data which this user should not have privy to.

Note: The Oracle Client and WebLogic should be installed as the user who will stop and start the application. For example, if you plan to run the application as the install user these components must belong to cissys.

Oracle Client 19c - Runtime Option

Install the Oracle Client as described in the Oracle Client installation documentation. Use the cissys account to install the Oracle Client. If another user installs the Oracle Client, make sure the cissys user ID has the proper execute permissions.

For the cissys user ID, ensure that the environment variable ORACLE_CLIENT_HOME is set up, and that ORACLE_CLIENT_HOME/perl/bin is the first Perl listed in the cissys account’s PATH variable.

Oracle Java Development Kit v8.0 Update 261, 64-bit

At time of release, Oracle Java packages could be obtained from:

http://www.oracle.com/technetwork/java/archive-139210.html

The Oracle WebLogic Server requires the 64-bit version. The main prerequisite for the web server is the version of Java mentioned above.

For the user ID cissys, ensure that the environment variable JAVA_HOME is setup, and that java_home/bin and java_home/lib can be found in cissys' PATH variable.

Hibernate 4.1.0 FINAL

You must install Hibernate before installing the product.

To install Hibernate external jar files to the Hibernate 3rd party jars depot:

1. Create a Hibernate jar external depot:

   ```
   export HIBERNATE_JAR_DIR=<Hibernate 3rd party jars depot>
   ```

2. Download the hibernate-release-4.1.0.Final.zip file from http://sourceforge.net/projects/hibernate/files/hibernate4/.
3. Click the "4.1.0.Final" link to download the zip file.
4. Extract the contents of the archive file:

   ```
   unzip hibernate-release-4.1.0.Final.zip
   ```

   > **Note**: You must have Java JDK installed on the machine to use the jar command. Make sure you install the JDK supported for your platform.

5. Copy the jar files to your Hibernate jar directory ($HIBERNATE_JAR_DIR) using the following commands:

   ```
   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/ ehcache-
   core-2.5.2.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/hibernate-
   ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-commons-
   annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-core-
   4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-jpa-2.0-
   api-1.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/javassist-3.15.0-
   GA.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-logging-
   3.3.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-transaction-
   api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
   ```

Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle WebLogic software can be downloaded from the Oracle website. This application server will run as a 64-bit application.

- Download and install 64-bit Java (as documented above) before installing WebLogic.
- Download and install WebLogic Fusion Middleware Infrastructure Installer.

Oracle Service Bus 12.2.1.4

Oracle Service Bus is required for implementations that plan to use middleware implementations of adapters or the generic adapter to process meter reading or device event data.

Oracle Service Bus is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle Service Bus 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle Service Bus must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle Service Bus can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle SOA Suite 12.2.1.4

Oracle SOA Suite, specifically BPEL Process Manager, is required for implementations that plan to use middleware implementations of adapters or the generic adapter to implement two-way communications for processing meter commands.

SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle SOA Suite 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle SOA Suite must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle SOA Suite can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle Solaris 11 Application Server

This section describes the software requirements for operating the application using the Oracle Solaris application server.

Supported Application Servers

Operating System	Chipsets	Application Server
Oracle Solaris 11 (64-bit)	SPARC	Oracle WebLogic 12c (12.2.1.4) 64-bit

Solaris Operating System Running on SPARC-based 64-bit Architecture

UNIX Administrator User ID

The following user groups and accounts have to be created to install and administer the application:

Description	Default Value	Customer Defined Value
Oracle Utilities Smart Grid Gateway Administrator User ID	cissys	
Oracle Utilities Smart Grid Gateway User Group	cisusr	

> **Note:** It is recommended that you change the default values for security reasons.

Throughout this document the administrator user id is often referred to as the "cissys" user id. You should substitute that with the customer defined user id when not using the default value. After the initial install, the software should always be managed using that user id.

By default, the cissys user ID is the only one given access to the files installed.

1. Create a group called cisusr (user group)
2. Create a user called cissys. Primary group cisusr. Set the primary shell for the cissys user to Korn Shell.

The shell scripts use the ">" to overwrite shell functionality. Your operating system may be configured to not allow this functionality by default in the users shell.

To avoid file access permission problems when executing scripts, consider placing the following command into cissys profile script:

```
set +o noclobber
```

Security Configuration

Various options exist to secure a system. In this application all files will be created with the minimum permissions required to ensure that group-readable, group-writable, and group-executable files will have the correct user groups and to restrict the permissions available to legitimate users. In this way, a low privileged end user cannot directly edit configuration files and thereby bypass application security controls.

The following users and group categories must be defined to implement this security. For demonstration purposes the following users and groups will be used. These users must be created according to industry standards (including password policies). All users should be created with a default umask of 022 to ensure files created during normal operation have the correct permissions.

Please replace these users and groups for your installation defaults:

User	Group	Description
cissys	cisusr	This user will be used to install the application and to apply patches. This user will own all the application files. The same care should be taken with this user ID as if it is 'root'. This user will be able to add, delete, and modify all the files within the application.
cisadm	cisusr	Administrative and Operation functions will be available to this user. This user will be able to stop and start the application and batch processes, but will not have access to modify any file other than generated log files
cisoper	-------	Low level operator. This user will only be able to read logs files and collect information for debugging and investigative purposes. Care should be taken in production to disable debugging as debugging information could contain potential sensitive data which this user should not have privy to.

Note: The Oracle Client and WebLogic should be installed as the user who will stop and start the application. For example, if you plan to run the application as the install user these components must belong to cissys.

Oracle Client 19c - Runtime Option

Install the Oracle Client as described in the Oracle Client installation documentation. Use the cissys account to install the Oracle Client. If another user installs the Oracle Client, make sure the cissys user ID has the proper execute permissions.

For the cissys user ID, ensure that the environment variable ORACLE_CLIENT_HOME is set up, and that ORACLE_CLIENT_HOME/perl/bin is the first Perl listed in the cissys account's PATH variable.

Oracle Java Development Kit v8.0 Update 261, 64-bit

At time of release, Oracle Java packages could be obtained from:

http://www.oracle.com/technetwork/java/archive-139210.html

The Oracle WebLogic Server requires the 64-bit version. The main prerequisite for the web server is the version of Java mentioned above.

For the user ID cissys, ensure that the environment variable JAVA_HOME is setup, and that java_home/bin and java_home/lib can be found in cissys' PATH variable.

Hibernate 4.1.0 FINAL

You must install Hibernate before installing the product.

To install Hibernate external jar files to the Hibernate 3rd party jars depot:

1. Create a Hibernate jar external depot:

```
export HIBERNATE_JAR_DIR=<Hibernate 3rd party jars depot>
```

2. Download the hibernate-release-4.1.0.Final.zip file from http://sourceforge.net/projects/hibernate/files/hibernate4/.
3. Click the "4.1.0.Final" link to download the zip file.
4. Extract the contents of the archive file:

   ```
   unzip hibernate-release-4.1.0.Final.zip
   ```

   > **Note**: You must have Java JDK installed on the machine to use the jar command. Make sure you install the JDK supported for your platform.

5. Copy the jar files to your Hibernate jar directory ($HIBERNATE_JAR_DIR) using the following commands:

   ```
   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/ ehcache-
   core-2.5.2.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/hibernate-
   ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-commons-
   annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-core-
   4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-jpa-2.0-
   api-1.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/javassist-3.15.0-
   GA.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-logging-
   3.3.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-transaction-
   api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
   ```

Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle WebLogic software can be downloaded from the Oracle website. This application server will run as a 64-bit application.

- Download and install 64-bit Java (as documented above) before installing WebLogic.
- Download and install WebLogic Fusion Middleware Infrastructure Installer.

Oracle Service Bus 12.2.1.4

Oracle Service Bus is required for implementations that plan to use middleware implementations of adapters or the generic adapter to process meter reading or device event data.

Oracle Service Bus is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle Service Bus 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle Service Bus must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle Service Bus can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle SOA Suite 12.2.1.4

Oracle SOA Suite, specifically BPEL Process Manager, is required for implementations that plan to use middleware implementations of adapters or the generic adapter to implement two-way communications for processing meter commands.

SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle SOA Suite 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle SOA Suite must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle SOA Suite can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Windows Server 2012 R2 Application Server

This section describes the software requirements for operating the application using the Windows application server.

Supported Application Servers

Operating System	Chipsets	Application Server
Windows Server 2012 R2 (64-bit)	x86_64	Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle Client 19c - Runtime Option

Install the Oracle Client as described in the Oracle Client installation documentation. Use the cissys account to install the Oracle Client. If another user installs the Oracle Client, make sure the cissys user ID has the proper execute permissions.

For the cissys user ID, ensure that the environment variable ORACLE_CLIENT_HOME is set up, and that ORACLE_CLIENT_HOME/perl/bin is the first Perl listed in the cissys account's PATH variable.

Oracle Java Development Kit v8.0 Update 261, 64-bit

At time of release, Oracle Java packages could be obtained from:

http://www.oracle.com/technetwork/java/archive-139210.html

The Oracle WebLogic Server requires the 64-bit version. The main prerequisite for the web server is the version of Java mentioned above.

For the user ID cissys, ensure that the environment variable JAVA_HOME is setup, and that java_home/bin and java_home/lib can be found in cissys' PATH variable.

Hibernate 4.1.0 FINAL

You must install Hibernate before installing the product.

To install Hibernate external jar files to the Hibernate 3rd party jars depot:

1. Create a Hibernate jar external depot:

   ```
   export HIBERNATE_JAR_DIR=<Hibernate 3rd party jars depot>
   ```

2. Download the hibernate-release-4.1.0.Final.zip file from http://sourceforge.net/projects/hibernate/files/hibernate4/.
3. Click the “4.1.0.Final” link to download the zip file.
4. Extract the contents of the archive file:

   ```
   unzip hibernate-release-4.1.0.Final.zip
   ```

   > **Note**: You must have Java JDK installed on the machine to use the jar command. Make sure you install the JDK supported for your platform.

5. Copy the jar files to your Hibernate jar directory ($HIBERNATE_JAR_DIR) using the following commands:

   ```
   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/ ehcache-
   core-2.5.2.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/optional/ehcache/hibernate-
   ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-commons-
   annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-core-
   4.1.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/hibernate-jpa-2.0-
   api-1.0.1.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/javassist-3.15.0-
   GA.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-logging-
   3.3.0.Final.jar $HIBERNATE_JAR_DIR

   cp hibernate-release-4.1.0.Final/lib/required/jboss-transaction-
   api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
   ```

Oracle WebLogic 12c (12.2.1.4) 64-bit

Oracle WebLogic software can be downloaded from the Oracle website. This application server will run as a 64-bit application.

- Download and install 64-bit Java (as documented above) before installing WebLogic.
- Download and install WebLogic Fusion Middleware Infrastructure Installer.

Oracle Service Bus 12.2.1.4

Oracle Service Bus is required for implementations that plan to use middleware implementations of adapters or the generic adapter to process meter reading or device event data.

Oracle Service Bus is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle Service Bus 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle Service Bus must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle Service Bus can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Oracle SOA Suite 12.2.1.4

Oracle SOA Suite, specifically BPEL Process Manager, is required for implementations that plan to use middleware implementations of adapters or the generic adapter to implement two-way communications for processing meter commands.

SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

> **Note:** Oracle SOA Suite 12.2.1.4 requires Oracle WebLogic Server 12.2.1.4.

Oracle SOA Suite must be installed prior to the installation of Oracle Utilities Smart Grid Gateway. Oracle SOA Suite can be downloaded from the Oracle Fusion Middleware Software Downloads portal.

Additional Prerequisite Software Information

This section outlines additional information related to installing the prerequisite software, including:

- Setting Up and Using the Additional JAR Directory
- Special Note to Upgrade from a WebLogic 12.1.3.x Environment

Setting Up and Using the Additional JAR Directory

The additional JAR directory must be populated if the Web Application Server Home directory is not set.

For example: The environment is for batch only and the server has no WebLogic installed. In this scenario, the Additional JAR Directory must be created prior to the installation and the following list of WebLogic JARs should be copied to that directory (full path from the actual WebLogic location which must be installed in the web server).

```
<Web Application Server Home Directory>/server/lib/
wlthint3client.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.codehaus.woodstox.stax2-api.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.core.jersey-client.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.core.jersey-common.jar
```

```
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.bundles.repackaged.jersey-guava.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.core.jersey-server.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.media.jersey-media-jaxb.jar
<Web Application Server Home Directory>/../oracle_common/modules/
org.glassfish.jersey.media.jersey-media-multipart.jar
if WebLocic 12.2.1.[0-2].0:
<Web Application Server Home Directory>/../oracle_common/modules/
org.codehaus.woodstox.woodstox-core-asl.jar
if WebLocic is not 12.2.1.[0-2].0:
<Web Application Server Home Directory>/../oracle_common/modules/
com.fasterxml.woodstox.woodstox-core.jar
```

If the Additional JAR directory is configured, the initialSetup process will pull those JARs from that directory. If it is not configured, the initialSetup process will pull those JARs from the Web Application Server Home directory.

Special Note to Upgrade from a WebLogic 12.1.3.x Environment

If you are upgrading from an environment which is using WebLogic 12.1.3.x, make sure to follow the steps below prior to the installation:

1. Install Oracle WebLogic Server (Fusion Middleware Infrastructure) 12.2.1.4.
2. Install Oracle Java SE Development Kit 1.8.0_261 (if not installed yet).
3. Shutdown the application server environment.
4. Take a full backup of the application:

   ```
   $SPLEBASE
   ```

5. Set the environment:

   ```
   splenviron.sh -e <ENV NAME>
   ```

6. Reconfigure the environment to point to the new WebLogic and Java (if upgraded Java as well):

   ```
   Execute: configureEnv.sh -i
   Update: "Web Java Home Directory" and "Web Application Server Home
   Directory"
   Type <P> to process (no need to rerun initialSetup.sh).
   ```

7. Set the environment again.

   ```
   splenviron.sh -e <ENV NAME>
   ```

8. Upgrade the Oracle Utilities Application Framework to V4.4.0.3.0.

   ```
   install.sh -u
   ```

Readiness Checklist

The following checklist guides you through the installation process of Oracle Utilities Smart Grid Gateway. The details for each step are presented in subsequent chapters.

1. Confirm that the recommended hardware is ready. Refer to Chapter 2: Operating Systems and Application Servers for more details.
2. Install prerequisite software. Refer to the Installing Prerequisite Software section for more details.
3. Ensure that you have downloaded the Oracle Utilities Smart Grid Gateway V2.4.0.0.0 components.
4. Go through the Appendix B: Installation and Configuration Worksheets to understand the configuration menu.
5. Determine the type of the installation:
   - **Initial Installation** - For initial installation follow the instructions mentioned in the Chapter 4: Installing Oracle Utilities Smart Grid Gateway—Initial Installation.
   - **Demo Installation** - For demo installation follow the instructions mentioned in the chapter Chapter 5: Installing Oracle Utilities Smart Grid Gateway—Demo Installation.
   - **Upgrade Installation** - For upgrade installation follow the instructions mentioned in the chapter Chapter 6: Installing Oracle Utilities Smart Grid Gateway—Upgrade Installation.
6. Perform post-installation tasks.

Chapter 4

Installing Oracle Utilities Smart Grid Gateway—Initial Installation

This chapter provides instructions to install Oracle Utilities Smart Grid Gateway for the first time or from scratch. It includes the following sections:

- Before You Install
- Initial Installation Procedure
- After the Installation
- Operating the Application

Before You Install

Refer to My Oracle Support for up-to-date additional information on Oracle Utilities Smart Grid Gateway.

Initial Installation Procedure

The initial installation procedure consists of:

- Installing the Database Component
- Installing Application Components

Installing the Database Component

The Oracle Utilities Smart Grid Gateway database component installation must be complete before you can proceed with the following sections.

Refer to the **Initial Install** section in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for instructions to install the database component.

> **Note**: When implementing Oracle Utilities Smart Grid Gateway with Oracle Utilities Meter Data Management, both the Smart Grid Gateway and Meter Data Management database components should be installed in the same database.

Installing Application Components

A successful installation consists of the following steps:

- Installing the Oracle Utilities Application Framework V4.4.0.3.0 Application Component
- Installing Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component
- Installing the Oracle Utilities Smart Grid Gateway V2.4.0.0.0 SOA Suite Application Components

> **Note**: As of release v2.2.0.3, Oracle Utilities Smart Grid Gateway is installed with Oracle Utilities Meter Data Management. Refer to the **Application Flattening** section in the *Oracle Utilities Smart Grid Gateway Release Notes* for more information.

Installing the Oracle Utilities Application Framework V4.4.0.3.0 Application Component

This section describes how to install the application component of Oracle Utilities Application Framework, including:

- Copying and Decompressing Install Media
- Setting Permissions for the cistab file in UNIX
- Installing the Application Component

Copying and Decompressing Install Media

The Oracle Utilities Application Framework V4.4.0.3 installation file is delivered in jar format for both UNIX and Windows platforms. If you are planning to install multiple Oracle Utilities Application Framework V4.4.0.3 environments operated by different Oracle Utilities administrator user ids, you must complete each of the following installation steps for each administrator userid.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.4.0.3.0 Multiplatform from Oracle Software Delivery Cloud.
3. Create a temporary directory, such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>.)

   Note: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.

4. Copy the file FW-V4.4.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. Make sure to use the BINARY option for FTP transfer.
5. Decompress the file.

   ```
   cd <TEMPDIR>
   jar -xvf FW-V4.4.0.3.0-MultiPlatform.jar
   ```

   Note: In order to be able to execute the "jar" command you need to have the Java JDK installed.

A sub-directory named FW-V4.4.0.3.0 is created. It contains the installation software for the Oracle Utilities Framework Application server.

Setting Permissions for the cistab file in UNIX

Every Oracle Utilities Application Framework environment installed on a server must be registered in the /etc/cistab file located on that server. On UNIX servers, generally only the root user ID has write permissions to the /etc directory. Since the installation process is run by the Oracle administrator user ID (cissys), this user ID may not be able to write to /etc/cistab table.

The install utility checks permissions and if it identifies a lack of the necessary permissions, it generates a script in the ../App/FW.V4.4.0.3.0 directory named cistab_<SPLENVIRON>.sh. Run the generated script using the root account before continuing with the installation process. The script initializes the cistab file in /etc directory (if it is the first Oracle Utilities Framework application environment on the server) and registers a new environment.

The generated script also changes the owner of /etc/cistab file to the Oracle Utilities Framework administrator user ID, so that the next time a new environment is created by the same Oracle Utilities Framework administrator user ID, you do not need to run the generated script with the root user ID. Instead the install utility itself proceeds with the registration.

If you are reinstalling an existing environment, only the validation of /etc/cistab entry is done by the install utility, no new registration occurs. The install utility interactively instructs you about every step that needs to occur in each specific case.

If you are planning to upgrade an existing environment it is your responsibility to take a backup prior to the installation process. The installation utility does not create a backup of existing environment.

Installing the Application Component

This section outlines the steps for installing the application component of Oracle Utilities Application Framework 4.4.0.3.0.

1. Login to the Application Server host as administrator (the default is cissys on UNIX) or as a user with Administrator privileges (on Windows).
2. Change directory to <TEMPDIR>/App/FW.V4.4.0.3.0.
3. Set the ORACLE_CLIENT_HOME and PATH variables as Oracle Client Perl is required to run the installer.

   UNIX:

   ```
   export ORACLE_CLIENT_HOME=<ORACLE CLIENT INSTALL LOCATION>
   export PERL_HOME=${ORACLE_CLIENT_HOME}/perl
   export PATH=${PERL_HOME}/bin:$PATH
   export PERL5LIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
                          Installer Decompressed location/bin/perlib>
   export PERLLIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
                          Installer Decompressed location/bin/perlib>
   export LD_LIBRARY_PATH=${ORACLE_CLIENT_HOME}/lib:$LD_LIBRARY_PATH
   ```

   Windows:

   ```
   set ORACLE_CLIENT_HOME=<ORACLE CLIENT INSTALL LOCATION>
   set PERL_HOME=%ORACLE_CLIENT_HOME%\perl
   set PATH=%PERL_HOME%\bin;%PATH%
   ```

4. Start the application installation utility by executing the appropriate script:

   UNIX:

   ```
   ksh ./install.sh
   ```

   Windows:

   ```
   install.cmd
   ```

   The Oracle Utilities Application Framework specific menu appears.

5. Follow the messages and instructions that are produced by the application installation utility.
6. Select each menu item to configure the values. For detailed description of the values, refer to Appendix B: Installation and Configuration Worksheets.
7. Below are the mandatory list of configurable items along with descriptions for a few items. Where you see <Mandatory>, enter values suitable to your environment. You can assign default values to the rest of the menu items.

   ```
   ************************************
   * Environment Installation Options *
   ************************************
   1. Environment ID, Roles, Third Party Software Configuration

       Environment ID                                        <Default>

       Server Roles                                      batch, online
   ```

```
    Oracle Client Home Directory   <Mandatory for Initial Install>
    Web Java Home Directory        <Mandatory for Initial Install>
    Hibernate JAR Directory        <Mandatory for Initial Install>
    ONS JAR Directory                                   <Optional>
    Web Application Server Home    <Mandatory for Initial Install>
    Directory
    Additional JAR Directory                            <Optional>

2. Keystore Options
    Import Keystore Directory                            <Default>

50. Environment Installation Options
    Environment Mount Point                            <Mandatory>
    Log Files Mount Point                              <Mandatory>
    Environment Name                                   <Mandatory>
    Install Application Viewer Module                         true
    Install Sample CM Source Code                             true

Each item in the above list should be configured for a successful
install.

Choose option (1,2,50, <P> Process, <X> Exit):

Once you enter 'P' after entering mandatory input values in the
above menu, the system populates another configuration menu.

***********************************************************
* Environment Configuration *
***********************************************************
 1. Environment Description
    Environment Description                            <Mandatory>

 2. Business Application Server Configuration
    Business Server Host                 <Mandatory> - Hostname on
                                           which application being
                                                         installed
    Business Server Application Name                    SPLService

 3. Web Application Server Configuration
    Web Server Host                                    <Mandatory>
    WebLogic SSL Port Number                           <Mandatory>
    WebLogic Console Port Number                       <Mandatory>
    Web Context Root                                          ouaf
```

```
        WebLogic JNDI User ID                              <Mandatory>
        WebLogic JNDI Password                             <Mandatory>
        WebLogic Server Name                                  myserver
        Web Server Application Name                             SPLWeb
        Deploy Application Viewer Module                          true
        Enable The Unsecured Health Check Service                false
        MDB RunAs User ID                                  <Mandatory>
        Super User IDs                                     <Mandatory>

    4. Database Configuration
        Application Server Database User ID                <Mandatory>
        Application Server Database Password               <Mandatory>
        XAI Database User ID                               <Mandatory>
        XAI Database Password                              <Mandatory>
        Batch Database User ID                             <Mandatory>
        Batch Database Password                            <Mandatory>
        Web JDBC DataSource Name                            <Optional>
        Database Name                                      <Mandatory>
        Database Server                                    <Mandatory>
        Database Port                                             1521
        ONS Server Configuration                            <Optional>
        Database Override Connection String                 <Optional>
        Character Based Database                                 false
        Oracle Client Character                  AMERICAN_AMERICA.AL32
        Set NLS_LANG                                              UTF8

   5. General Configuration Options
        Batch RMI Port                                     <mandatory>
        RMI Port number for JMX Business                    <optional>
        RMI Port number for JMX Web                         <optional>
        JMX Enablement System User ID                       <optional>
        JMX Enablement System Password                      <optional>
        Coherence Cluster Name                             <mandatory>
        Coherence Cluster Address                          <mandatory>
        Coherence Cluster Port                             <Mandatory>
        Coherence Cluster Mode                         prod<Mandatory>
```

```
 6. OUAF TrustStore Options
      Import TrustStore Directory                <Mandatory> for Prod


Each item in the above list should be configured for a successful
install.

Choose option (1,2,3,4,5,6 <P> Process, <X> Exit):
```

10. When the parameter setup is complete, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.

11. Once the install or upgrade has finished, the installation log location is displayed on the screen. If the log does not list any error messages, the installation of the application component of Oracle Utilities Application Framework is complete.

Installing Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component

This section describes how to install the Oracle Utilities Meter Data Management, including:

- Copying and Decompressing the Install Media
- Installing the Oracle Utilities Meter Data Management Application Component

To proceed with the Oracle Utilities Meter Data Management installation you need to be connected to the target Oracle Utilities Application Framework environment.

You must initialize the Oracle Utilities Application Framework environment. For detailed instructions, refer to the Installing the Oracle Utilities Application Framework V4.4.0.3.0 Application Component section.

Copying and Decompressing the Install Media

The Oracle Utilities Meter Data Management installation file is delivered in jar format for both UNIX and Windows platforms.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip from Oracle Software Delivery Cloud.
3. Create a temporary directory such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>)

   Note: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.

4. Unzip Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip to get the file MDM_V2.4.0.0.0.zip from the delivered package and copy to the <TEMPDIR>. To use FTP to transfer this file, use the BINARY option.
5. Decompress the file:

```
cd <TEMPDIR>
unzip MDM_V2.4.0.0.0.zip
cd App
```

For UNIX and Windows platforms, a sub-directory named MDM.V2.4.0.0.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installing the Oracle Utilities Meter Data Management Application Component

To install the Oracle Utilities Meter Data Management application component:

1. Log in to the application server host as Oracle Utilities Application Framework Administrator (default cissys).
2. Change directory:

   ```
   cd <install_dir>/bin
   ```

   where <install_dir> is the location where the Oracle Utilities Application Framework application component is installed.
3. Initialize the environment by running the appropriate command:

   UNIX

   ```
   ./splenviron.sh -e <ENV NAME>
   ```

   Windows

   ```
   splenviron.cmd -e <ENV NAME>
   ```

4. Navigate to <TEMPDIR>/MDM.V2.4.0.0.0 directory.
5. Run the install script.

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   UNIX

   ```
   ksh ./install.sh
   ```

   Windows

   ```
   install.cmd
   ```

6. Choose option P to proceed with the installation.

   > **Note:** The rest of the menu items can be ignored if you are installing only MDM.

The Oracle Utilities Meter Data Management installation is complete if no errors occurred during the installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management

This section applies to an Oracle Utilities Smart Grid Gateway configuration in which Oracle Service Bus (OSB) or Oracle SOA Suite is installed on a separate host from the Oracle Utilities Application Framework's host. In this configuration, the Oracle Utilities installation scripts must have access to the libraries in the OSB and SOA servers' directories to deploy OSB projects and SOA composites successfully.

Follow these procedures to configure access to a remote OSB server:

- Create a network share to the osb folder within the Middleware Home on the remote OSB server.
- Provide the following values for Menu Item 8 (OSB Configuration) during the installation for Oracle Utilities Meter Data Management:

  Note: Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets for more information.

  - **OSB Home** is the location of the osb folder, accessed by way of network share.
  - **OSB Host Server** is the host name of the OSB server.
  - **OSB Port Number** is the port of the OSB admin server.
  - **OSB SSL Port Number** is the port of the OSB SSL admin server.
  - **OSB Managed Server Port Number** is the port of the OSB managed server.
  - **OSB Managed Server SSL Port Number** is the port of the OSB SSL managed server.

Follow these procedures to configure access to a remote SOA Suite server:

- Create a network share to the soa folder within the Middleware Home on the remote SOA Suite server.
- Provide the following values for Menu Item 9 (SOA Configuration) during the installation for Oracle Utilities Meter Data Management.

Note: Use the completed SOA configuration worksheet to assist you in this step. Refer to the Appendix B: Installation and Configuration Worksheets.

  - **SOA Home** is the location of the soa folder, accessed by way of network share.
  - **SOA Host Server** is the host name of the SOA managed server.
  - **SOA Port Number** is the port of the SOA managed server.
  - **SOA SSL Port Number** is the port of the SOA SSL managed server.

Installing the Oracle Utilities Smart Grid Gateway V2.4.0.0.0 SOA Suite Application Components

This section describes how to install the SOA Suite application components of Oracle Utilities Smart Grid Gateway, including:

- Installing the MV90 Adapter for Itron
- Installing the Adapter Development Kit

- Installing the Adapter for Networked Energy Services
- Installing the Adapter for Itron OpenWay
- Installing the Adapter for Landis+Gyr
- Installing the Adapter for Sensus RNI
- Installing the Adapter Silver Spring Networks

Note: SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

Installing the MV90 Adapter for Itron

This section describes the installation of the MV90 Adapter for Itron, including:

- Pre-installation Tasks for the MV90 Adapter
- Installing the MV90 Adapter

Pre-installation Tasks for the MV90 Adapter

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway MV90 Adapter, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Chapter 2: Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also refer to the Installing Prerequisite Software section in Chapter 3: Planning the Installation for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Meter Data Management environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

3. Stop the environment if running.

Installing the MV90 Adapter

To install the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B**:** Installation and Configuration Worksheets.

3. Choose option P to proceed with the installation.

4. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute the post-installation steps described in Configuration Tasks for the MV90 Adapter.

Installing the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Pre-installation Tasks for the Adapter Development Kit
- Installation Tasks for the Adapter Development Kit

Pre-installation Tasks for the Adapter Development Kit

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Supported Platforms and Hardware Requirements section for versions and installation details regarding the database and operating system. Also refer to the Installing Prerequisite Software section for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Initializing the Oracle Utilities Application Framework Environment
- Installing the Adapter Development Kit

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter Development Kit

To install the Oracle Utilities Smart Grid Gateway Adapter Development Kit:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The Configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 21 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.
7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute the post-installation steps described in Configuration Tasks for the Adapter Development Kit.

Installing the Adapter for Networked Energy Services

This section describes the installation of the Adapter for Networked Energy Services, including:

- Pre-installation Tasks for the Adapter for Networked Energy Services
- Installing the Adapter for Networked Energy Services

Pre-installation Tasks for the Adapter for Networked Energy Services

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Networked Energy Services

To install the Oracle Utilities Smart Grid Gateway Adapter for Networked Energy Services:

1. Run the following install script:

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 17 to configure the URI for the NES head-end system web services.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute postinstallation steps described in Configuration Tasks for the Adapter for Networked Energy Services.

Installing the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Pre-installation Tasks for the Adapter for Itron OpenWay
- Installation Tasks for the Adapter for Itron OpenWay

Pre-installation Tasks for the Adapter for Itron OpenWay

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and log into the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Initializing the Oracle Utiliies Application Framework Environment
- Installing the Adapter for Itron OpenWay

Initializing the Oracle Utiliies Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).

2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Itron OpenWay

To install the Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 22 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Itron OpenWay.

Installing the Adapter for Landis+Gyr

This section describes the installation of the Adapter for Landis+Gyr, including:

- Pre-installation Tasks for the Adapter for Landis+Gyr
- Installing the Adapter for Landis+Gyr

Pre-installation Tasks for the Adapter for Landis+Gyr

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Operating Systems and Application Servers section for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Landis+Gyr

To install the Oracle Utilities Smart Grid Gateway Adapter for Landis+Gyr:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh. The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 16 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option P to proceed with the installation.
7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Landis+Gyr.

Installing the Adapter for Sensus RNI

This section describes the installation of the Adapter for Sensus RNI, including:

- Pre-installation Tasks for the Adapter for Sensus RNI
- Installing the Adapter for Sensus RNI

Pre-installation Tasks for the Adapter for Sensus RNI

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and log into the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Sensus RNI

To install the Oracle Utilities Smart Grid Gateway Adapter for Sensus RNI:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 18 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Sensus RNI.

Installing the Adapter Silver Spring Networks

This section describes the installation of the Adapter for Silver Spring Networks, including:

- Pre-installation Tasks for the Adapter for Silver Spring Networks
- Installing the Adapter for Silver Spring Networks

Pre-installation Tasks for the Adapter for Silver Spring Networks

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Supported Platforms and Hardware Requirements chapter for versions and installation details regarding the database and operating system. Also refer to the Installing Prerequisite Software section for prerequisite third-party software installation instructions.

Download the installation package and log into the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Silver Spring Networks

To install the Oracle Utilities Smart Grid Gateway Adapter for Silver Spring Networks:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 19 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. Select menu item 20 to configure the JMS source destination bridge.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

7. Select menu item 70 to configure the test harness.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

8. When you are done setting up the parameters, choose option P to proceed with the installation.
9. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Silver Spring Networks.

After the Installation

After completing the installation, verify the following:

1. Verify installation logs created under decompressed installer location for any errors.
2. Confirm installation logs do not contain any errors.
3. Confirm all the configurations are correct. Refer to Appendix B: Installation and Configuration Worksheets for details.
4. Confirm that the database is ready.
5. Start the application server. For instructions, refer to Appendix B: Installation and Configuration Worksheets.
6. To operate the application, refer to the Operating the Application section.

Operating the Application

At this point your installation and custom integration process is complete. Be sure to read the *Server Administration Guide* (included in this release) for more information on further configuring and operating the system.

Chapter 5

Installing Oracle Utilities Smart Grid Gateway—Demo Installation

This chapter provides instructions to set up a demo application of Oracle Utilities Smart Grid Gateway for demonstration or training purposes. It includes the following sections:

- Before You Install
- Demo Installation Procedure
- After the Installation

Before You Install

Refer to My Oracle Support for up-to-date additional information on Oracle Utilities Smart Grid Gateway.

Demo Installation Procedure

The initial installation procedure consists of:

- Database Component Installation
- Application Components Installation

Database Component Installation

Installation of the database component of Oracle Utilities Smart Grid Gateway must be complete before you can proceed with the following sections.

For instructions to install the database component, refer to the **Demo Install** section in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide*.

> **Note**: When implementing Oracle Utilities Smart Grid Gateway with Oracle Utilities Meter Data Management, both the Smart Grid Gateway and Meter Data Management database components should be installed in the same database.

Application Components Installation

A successful installation consists of the following steps:

- Installing the Oracle Utilities Application Framework Application V4.4.0.3.0
- Installing Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component
- Installing the Oracle Utilities Smart Grid Gateway V2.4.0.0.0 SOA Suite Application Components

Installing the Oracle Utilities Application Framework Application V4.4.0.3.0

This section describes how to install the application component of Oracle Utilities Application Framework, including:

- Copying and Decompressing Install Media
- Setting Permissions for the cistab file in UNIX
- Installing the Application Component

Copying and Decompressing Install Media

The Oracle Utilities Application Framework installation file is delivered in jar format for both UNIX and Windows platforms. If you are planning to install multiple Oracle Utilities Application Framework environments operated by different Oracle Utilities administrator user IDs, you must complete each of the following installation steps for each administrator userid.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.4.0.3.0 Multiplatform from Oracle Software Delivery Cloud.
3. Create a temporary directory, such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>.)

   Note: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.
4. Copy the file FW-V4.4.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. Make sure to use the BINARY option for FTP transfer.
5. Decompress the file.

   ```
   cd <TEMPDIR>
   jar -xvf FW-V4.4.0.3.0-MultiPlatform.jar
   ```

   Note: In order to be able to execute the “jar” command you need to have the Java JDK installed.

A sub-directory named FW-V4.4.0.3.0 is created. It contains the installation software for the Oracle Utilities Framework Application server.

Setting Permissions for the cistab file in UNIX

Every Oracle Utilities Application Framework environment installed on a server must be registered in the /etc/cistab file located on that server. On UNIX servers, generally only the root user ID has write permissions to the /etc directory. Since the installation process is run by the Oracle administrator user ID (cissys), this user ID may not be able to write to /etc/cistab table.

The install utility checks permissions and if it identifies a lack of the necessary permissions, it generates a script in the ../App/FW.V4.4.0.3.0 directory named cistab_<SPLENVIRON>.sh. Run the generated script using the root account before continuing with the installation process. The script initializes the cistab file in /etc directory (if it is the first Oracle Utilities Framework application environment on the server) and registers a new environment.

The generated script also changes the owner of /etc/cistab file to the Oracle Utilities Framework administrator user ID, so that the next time a new environment is created by the same Oracle Utilities Framework administrator user ID, you do not need to run the generated script with the root user ID. Instead the install utility itself proceeds with the registration.

If you are reinstalling an existing environment, only the validation of /etc/cistab entry is done by the install utility, no new registration occurs. The install utility interactively instructs you about every step that needs to occur in each specific case.

If you are planning to upgrade an existing environment it is your responsibility to take a backup prior to the installation process. The installation utility does not create a backup of existing environment.

Installing the Application Component

This section outlines the steps for installing the application component of Oracle Utilities Application Framework V4.4.0.3.0.

1. Login to the Application Server host as administrator (the default is cissys on UNIX) or as a user with Administrator privileges (on Windows).
2. Change directory to <TEMPDIR>/App/FW.V4.4.0.3.0.
3. Set the ORACLE_CLIENT_HOME and PATH variables as Oracle Client Perl is required to run the installer.

   UNIX

   ```
   export ORACLE_CLIENT_HOME=<ORACLE CLIENT INSTALL LOCATION>
   export PERL_HOME=${ORACLE_CLIENT_HOME}/perl
   export PATH=${PERL_HOME}/bin:$PATH
   export PERL5LIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
                         Installer Decompressed location/bin/perlib>
   export PERLLIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
                         Installer Decompressed location/bin/perlib>
   export LD_LIBRARY_PATH=${ORACLE_CLIENT_HOME}/lib:$LD_LIBRARY_PATH
   ```

   Windows

   ```
   set ORACLE_CLIENT_HOME=<ORACLE CLIENT INSTALL LOCATION>
   set PERL_HOME=%ORACLE_CLIENT_HOME%\perl
   set PATH=%PERL_HOME%\bin;%PATH%
   ```

4. Start the application installation utility by running the appropriate script.

   UNIX

   ```
   ksh ./install.sh
   ```

   Windows

   ```
   install.cmd
   ```

   The Oracle Utilities Application Framework specific menu appears.

5. Follow the messages and instructions that are produced by the application installation utility.
6. Select each menu item to configure the values. For detailed description of the values, refer to Appendix B: Installation and Configuration Worksheets.
7. Below are the mandatory list of configurable items along with descriptions for a few items. Where you see <Mandatory>, enter values suitable to your environment. You can assign default values to the rest of the menu items.

   ```
   ************************************
   * Environment Installation Options *
   ************************************
   1. Environment ID, Roles, Third Party Software Configuration

       Environment ID                                          <Default>

       Server Roles                                        batch, online
   ```

```
    Oracle Client Home Directory    <Mandatory for Initial Install>
    Web Java Home Directory         <Mandatory for Initial Install>
    Hibernate JAR Directory         <Mandatory for Initial Install>
    ONS JAR Directory                                    <Optional>
    Web Application Server Home     <Mandatory for Initial Install>
    Directory
    Additional JAR Directory                             <Optional>

2. Keystore Options
     Import Keystore Directory                            <Default>

50. Environment Installation Options
     Environment Mount Point                            <Mandatory>
     Log Files Mount Point                              <Mandatory>
     Environment Name                                   <Mandatory>
     Install Application Viewer Module                         true
     Install Sample CM Source Code                             true

Each item in the above list should be configured for a successful
install.

Choose option (1,2,50, <P> Process, <X> Exit):
```

Once you enter 'P' after entering mandatory input values in the above menu, the system populates another configuration menu.

```
***********************************************************
* Environment Configuration *
***********************************************************
 1. Environment Description
     Environment Description                            <Mandatory>


 2. Business Application Server Configuration
     Business Server Host                <Mandatory> - Hostname on
                                            which application being
                                                          installed
     Business Server Application Name                    SPLService


 3. Web Application Server Configuration
     Web Server Host                                    <Mandatory>
     WebLogic SSL Port Number                           <Mandatory>
     WebLogic Console Port Number                       <Mandatory>
     Web Context Root                                          ouaf
```

```
    WebLogic JNDI User ID                               <Mandatory>
    WebLogic JNDI Password                              <Mandatory>
    WebLogic Server Name                                   myserver
    Web Server Application Name                              SPLWeb
    Deploy Application Viewer Module                           true
    Enable The Unsecured Health Check Service                 false
    MDB RunAs User ID                                   <Mandatory>
    Super User IDs                                      <Mandatory>

 4. Database Configuration
    Application Server Database User ID                 <Mandatory>
    Application Server Database Password                <Mandatory>
    XAI Database User ID                                <Mandatory>
    XAI Database Password                               <Mandatory>
    Batch Database User ID                              <Mandatory>
    Batch Database Password                             <Mandatory>
    Web JDBC DataSource Name                             <Optional>
    Database Name                                       <Mandatory>
    Database Server                                     <Mandatory>
    Database Port                                              1521
    ONS Server Configuration                             <Optional>
    Database Override Connection String                  <Optional>
    Character Based Database                                  false
    Oracle Client Character                   AMERICAN_AMERICA.AL32
    Set NLS_LANG                                               UTF8

5. General Configuration Options
    Batch RMI Port                                      <mandatory>
    RMI Port number for JMX Business                     <optional>
    RMI Port number for JMX Web                          <optional>
    JMX Enablement System User ID                        <optional>
    JMX Enablement System Password                       <optional>
    Coherence Cluster Name                              <mandatory>
    Coherence Cluster Address                           <mandatory>
    Coherence Cluster Port                              <Mandatory>
    Coherence Cluster Mode                          prod<Mandatory>
 6. OUAF TrustStore Options

    Import TrustStore Directory                <Mandatory> for Prod


Each item in the above list should be configured for a successful
install.

Choose option (1,2,3,4,5,6 <P> Process, <X> Exit):
```

10. When the parameter setup is complete, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.

11. Once the install or upgrade has finished, the installation log location is displayed on the screen. If the log does not list any error messages, the installation of the application component of Oracle Utilities Application Framework is complete.

Installing Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component

This section describes how to install the Oracle Utilities Meter Data Management, including:

- Copying and Decompressing the Install Media
- Installing the Oracle Utilities Meter Data Management Application Component

To proceed with the Oracle Utilities Meter Data Management installation you need to be connected to the target Oracle Utilities Application Framework environment.

You must initialize the Oracle Utilities Application Framework environment. For detailed instructions, refer to the Installing the Oracle Utilities Application Framework V4.4.0.3.0 Application Component section.

Copying and Decompressing the Install Media

The Oracle Utilities Meter Data Management installation file is delivered in jar format for both UNIX and Windows platforms.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip from Oracle Software Delivery Cloud.
3. Create a temporary directory such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>)

   Note: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.

4. Unzip Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip to get the file MDM_V2.4.0.0.0.zip from the delivered package and copy to the <TEMPDIR>. To use FTP to transfer this file, use the BINARY option.
5. Decompress the file:

```
cd <TEMPDIR>
unzip MDM_V2.4.0.0.0.zip
cd App
```

For UNIX and Windows platforms, a sub-directory named MDM.V2.4.0.0.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installing the Oracle Utilities Meter Data Management Application Component

To install the Oracle Utilities Meter Data Management application component:

1. Log in to the application server host as Oracle Utilities Application Framework Administrator (default cissys).
2. Change directory:

   ```
   cd <install_dir>/bin
   ```

   where <install_dir> is the location where the Oracle Utilities Application Framework application component is installed.
3. Initialize the environment by running the appropriate command:

   UNIX
   ```
   ./splenviron.sh -e <ENV NAME>
   ```

   Windows
   ```
   splenviron.cmd -e <ENV NAME>
   ```
4. Navigate to <TEMPDIR>/MDM.V2.4.0.0.0 directory.
5. Run the install script.

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   UNIX
   ```
   ksh ./install.sh
   ```

   Windows
   ```
   install.cmd
   ```
6. Choose option P to proceed with the installation.

   > **Note:** The rest of the menu items can be ignored if you are installing only MDM.

The Oracle Utilities Meter Data Management installation is complete if no errors occurred during the installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management

This section applies to an Oracle Utilities Smart Grid Gateway configuration in which Oracle Service Bus (OSB) or Oracle SOA Suite is installed on a separate host from the Oracle Utilities Application Framework's host. In this configuration, the Oracle Utilities installation scripts must have access to the libraries in the OSB and SOA servers' directories to deploy OSB projects and SOA composites successfully.

Follow these procedures to configure access to a remote OSB server:

- Create a network share to the osb folder within the Middleware Home on the remote OSB server.
- Provide the following values for Menu Item 8 (OSB Configuration) during the installation for Oracle Utilities Meter Data Management:

  Note: Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

  - **OSB Home** is the location of the osb folder, accessed by way of network share.
  - **OSB Host Server** is the host name of the OSB server.
  - **OSB Port Number** is the port of the OSB admin server.
  - **OSB SSL Port Number** is the port of the OSB SSL admin server.
  - **OSB Managed Server Port Number** is the port of the OSB Managed Server.
  - **OSB Managed Server SSL Port Number** is the port of the OSB SSL Managed Server

Follow these procedures to configure access to a remote SOA Suite server:

- Create a network share to the soa folder within the Middleware Home on the remote SOA Suite server.
- Provide the following values for Menu Item 9 (SOA Configuration) during the installation for Oracle Utilities Meter Data Management.

  Note: Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

  - **SOA Home** is the location of the soa folder, accessed by way of network share.
  - **SOA Host Server** is the host name of the SOA managed server.
  - **SOA Port Number** is the port of the SOA managed server.
  - **SOA SSL Port Number** is the port of the SOA SSL managed server.

Installing the Oracle Utilities Smart Grid Gateway V2.4.0.0.0 SOA Suite Application Components

This section describes how to install the SOA Suite application components of Oracle Utilities Smart Grid Gateway, including:

- Installing the MV90 Adapter for Itron
- Installing the Adapter Development Kit

- Installing the Adapter for Networked Energy Services
- Installing the Adapter for Itron OpenWay
- Installing the Adapter for Landis+Gyr
- Installing the Adapter for Sensus RNI
- Installing the Adapter Silver Spring Networks

Note: SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

Installing the MV90 Adapter for Itron

This section describes the installation of the MV90 Adapter for Itron, including:

- Pre-installation Tasks for the MV90 Adapter
- Installing the MV90 Adapter

Pre-installation Tasks for the MV90 Adapter

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway MV90 Adapter, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Meter Data Management environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

3. Stop the environment if running.

Installing the MV90 Adapter

To install the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Run the install script:

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Choose option P to proceed with the installation.
4. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute the post-installation steps described in Configuration Tasks for the MV90 Adapter.

Installing the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Pre-installation Tasks for the Adapter Development Kit
- Installation Tasks for the Adapter Development Kit

Pre-installation Tasks for the Adapter Development Kit

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. See Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Initializing the Oracle Utilities Application Framework Environment
- Installing the Adapter Development Kit

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter Development Kit

To install the Oracle Utilities Smart Grid Gateway Adapter Development Kit:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, make sure that you have the proper execute permission on install.sh.

   The Configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 21 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described Configuration Tasks for the Adapter Development Kit.

Installing the Adapter for Networked Energy Services

This section describes the installation of the Adapter for Networked Energy Services, including:

- Pre-installation Tasks for the Adapter for Networked Energy Services
- Installing the Adapter for Networked Energy Services

Pre-installation Tasks for the Adapter for Networked Energy Services

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Serversfor versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities SApplication Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).

2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Networked Energy Services

To install the Oracle Utilities Smart Grid Gateway Adapter for Networked Energy Services:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 17 to configure the URI for the NES head-end system web services.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute postinstallation steps described in Configuration Tasks for the Adapter for Networked Energy Services.

Installing the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Pre-installation Tasks for the Adapter for Itron OpenWay
- Installation Tasks for the Adapter for Itron OpenWay

Pre-installation Tasks for the Adapter for Itron OpenWay

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Initializing the Oracle Utiliies Application Framework Environment
- Installing the Adapter for Itron OpenWay

Initializing the Oracle Utiliies Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Itron OpenWay

To install the Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 22 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

   Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Itron OpenWay.

Installing the Adapter for Landis+Gyr

This section describes the installation of the Adapter for Landis+Gyr, including:

- Pre-installation Tasks for the Adapter for Landis+Gyr
- Installing the Adapter for Landis+Gyr

Pre-installation Tasks for the Adapter for Landis+Gyr

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Landis+Gyr

To install the Oracle Utilities Smart Grid Gateway Adapter for Landis+Gyr:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh. The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 16 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option P to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

Windows

```
%SPLEBASE%\bin\ initialSetup.cmd
```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Landis+Gyr.

Installing the Adapter for Sensus RNI

This section describes the installation of the Adapter for Sensus RNI, including:

- Pre-installation Tasks for the Adapter for Sensus RNI
- Installing the Adapter for Sensus RNI

Pre-installation Tasks for the Adapter for Sensus RNI

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Sensus RNI

To install the Oracle Utilities Smart Grid Gateway Adapter for Sensus RNI:

1. Make sure the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

Windows

```
configureEnv.cmd
```

> **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 18 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Sensus RNI.

Installing the Adapter Silver Spring Networks

This section describes the installation of the Adapter for Silver Spring Networks, including:

- Pre-installation Tasks for the Adapter for Silver Spring Networks
- Installing the Adapter for Silver Spring Networks

Pre-installation Tasks for the Adapter for Silver Spring Networks

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also refer to Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Installing the Adapter for Silver Spring Networks

To install the Oracle Utilities Smart Grid Gateway Adapter for Silver Spring Networks:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 19 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. Select menu item 20 to configure the JMS source destination bridge.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B**:** Installation and Configuration Worksheets.

7. Select menu item 70 to configure the test harness.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B**:** Installation and Configuration Worksheets.

8. When you are done setting up the parameters, choose option P to proceed with the installation.

9. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Silver Spring Networks.

After the Installation

After completing the installation, verify the following:

1. Verify installation logs created under decompressed installer location for any errors.
2. Confirm installation logs do not contain any errors.
3. Confirm all the configurations are correct. Refer to Appendix B: Installation and Configuration Worksheets for details.
4. Confirm that the database is ready.
5. Start the application server. For instructions, refer to Appendix B: Installation and Configuration Worksheets.
6. To operate the application, refer to the respective section.

Chapter 6

Installing Oracle Utilities Smart Grid Gateway—Upgrade Installation

This chapter provides instructions to upgrade Oracle Utilities Smart Grid Gateway from V2.3.0.2.0 to V2.4.0.0.0.

> **Note**: If you have a version prior to 2.3.0.2.0, you must upgrade to V2.3.0.2.0 before upgrading to V2.4.0.0.0.

This chapter includes:

- Before You Upgrade
- Upgrade Procedure
- Operating the Application

Before You Upgrade

Review the list of operating system, application server and database server combinations that this version of Oracle Utilities Smart Grid Gateway is certified to operate on. The list is provided in the Supported Platforms and Hardware Requirements chapter.

For further assistance, contact My Oracle Support before you upgrade.

> **Note:** If you are upgrading a previously installed application server, it is recommended that you make a backup before you start the upgrade procedure. The upgrade installation will remove your existing environment including your configurations.

Upgrade Procedure

The upgrade installation procedure consists of:

- Database Component Upgrade
- Application Components Upgrade

Database Component Upgrade

Upgrading the Oracle Utilities Smart Grid Gateway database component must be complete before proceeding with the following sections.

Refer to the **Upgrade Install** section in the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for instructions to upgrade the database component.

> **Note**: When implementing Oracle Utilities Smart Grid Gateway with Oracle Utilities Meter Data Management, both the Smart Grid Gateway and Meter Data Management database components should be installed in the same database.

Application Components Upgrade

A successful upgrade consists of the following steps:

- Upgrading the Oracle Utilities Application Framework Application Component to V4.4.0.3.0
- Upgrading Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component
- Upgrading the Oracle Utilities Smart Grid Gateway V2.2.0.3 SOA Suite Application Components

Upgrading the Oracle Utilities Application Framework Application Component to V4.4.0.3.0

This section describes how to upgrade the application component of Oracle Utilities Application Framework, including:

- Copying and Decompressing Install Media

- Setting Permissions for the cistab file in UNIX
- Upgrading the Application Component Over Oracle Utilities Smart Grid GatewayV2.4.0.0.0

Copying and Decompressing Install Media

The Oracle Utilities Application Framework installation file is delivered in jar format for both UNIX and Windows platforms. If you are planning to install multiple Oracle Utilities Application Framework environments operated by different Oracle Utilities administrator user ids, you must complete each of the following installation steps for each administrator userid.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.4.0.3.0 Multiplatform from Oracle Software Delivery Cloud.
3. Create a temporary directory, such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>.)

   > **Note**: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.

4. Copy the file FW-V4.4.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. Make sure to use the BINARY option for FTP transfer.
5. Decompress the file.

   ```
   cd <TEMPDIR>
   jar -xvf FW-V4.4.0.3.0-MultiPlatform.jar
   ```

   > **Note**: In order to be able to execute the “jar” command you need to have the Java JDK installed.

A sub-directory named FW-V4.4.0.3.0 is created. It contains the installation software for the Oracle Utilities Framework Application server.

Setting Permissions for the cistab file in UNIX

Every Oracle Utilities Application Framework environment installed on a server must be registered in the /etc/cistab file located on that server. On UNIX servers, generally only the root user ID has write permissions to the /etc directory. Since the installation process is run by the Oracle administrator user ID (cissys), this user ID may not be able to write to /etc/cistab table.

The install utility checks permissions and if it identifies a lack of the necessary permissions, it generates a script in the <TEMPDIR>/App/FW.V4.4.0.3.0 directory named cistab_<SPLENVIRON>.sh. Run the generated script using the root account before continuing with the installation process. The script initializes the cistab file in /etc directory (if it is the first Oracle Utilities Framework application environment on the server) and registers a new environment.

The generated script also changes the owner of /etc/cistab file to the Oracle Utilities Framework administrator user ID, so that the next time a new environment is created by the same Oracle Utilities Framework administrator user ID, you do not need to run the generated script with the root user ID. Instead the install utility itself proceeds with the registration.

If you are reinstalling an existing environment, only the validation of /etc/cistab entry is done by the install utility, no new registration occurs. The install utility interactively instructs you about every step that needs to occur in each specific case.

If you are planning to upgrade an existing environment it is your responsibility to take a backup prior to the installation process. The installation utility does not create a backup of existing environment.

Upgrading the Application Component Over Oracle Utilities Smart Grid GatewayV2.4.0.0.0

This section outlines the steps for upgrading the application component of Oracle Utilities Application Framework over Oracle Utilities Smart Grid Gateway 2.4.0.0.0.

> **Note:** Customers who have a version prior to 2.3.0.2.0 must install 2.3.0.2.0 before upgrading to 2.4.0.0.0.

1. Login to the Application Server host as administrator (the default is cissys on UNIX) or as a user with Administrator privileges (on Windows).

2. Change directory to the bin folder.

   ```
   cd <install_dir>/bin
   ```

   where <install_dir> is the location where the Oracle Utilities Meter Data Management Base application component is installed.

3. Initialize the environment.

   UNIX

   ```
   ./splenviron.sh -e <ENV NAME>
   ```

   Windows

   ```
   splenviron.cmd -e <ENV NAME>
   ```

4. Stop the environment, if running (for 2.2.0.3.0 versions).

   UNIX

   ```
   $SPLEBASE/bin/spl.sh stop
   ```

   Windows

   ```
   %SPLEBASE%\bin\spl.cmd stop
   ```

5. Change the directory to <TEMPDIR>/App/FW.V4.4.0.3.0.

   > **NOTE**: While installing the FW V4.4.0.3 from the previous environment to V2.4.0.0.0, the install utility removes the existing environment and re-creates the environment. Make a backup before you proceed with installing FW V4.4.0.3 to retain any configurations for future reference.

6. Start the application installation utility.

   UNIX

   ```
   ksh ./install.sh
   ```

Windows

```
install.cmd
```

The Oracle Utilities Application Framework specific menu appears.

7. Follow the messages and instructions that are produced by the application installation utility.
8. Select each menu item to configure the values. For detailed description of the values, refer to the Installation and Configuration Worksheets.
9. Below is the mandatory list of configurable items along with descriptions for a few items. Where you see <Mandatory>, enter values suitable to your environment. You can assign default values to the rest of the menu items.

```
***********************************
* Environment Installation Options *
***********************************
1. Environment ID, Roles, Third Party Software Configuration

    Environment ID                                      <Default>

    Server Roles                                   batch, online

    Oracle Client Home Directory    <Mandatory for Initial Install>

    Web Java Home Directory         <Mandatory for Initial Install>

    Hibernate JAR Directory         <Mandatory for Initial Install>

    ONS JAR Directory                                  <Optional>

    Web Application Server Home     <Mandatory for Initial Install>
    Directory

    Additional JAR Directory                           <Optional>


2. Keystore Options

     Import Keystore Directory                          <Default>


50. Environment Installation Options

     Environment Mount Point                          <Mandatory>

     Log Files Mount Point                            <Mandatory>

     Environment Name                                 <Mandatory>

     Install Application Viewer Module                      true

     Install Sample CM Source Code                          true


Each item in the above list should be configured for a successful
install.

Choose option (1,2,50, <P> Process, <X> Exit):

Once you enter 'P' after entering mandatory input values in the
above menu, the system populates another configuration menu.
```

```
**********************************************************
* Environment Configuration *
**********************************************************
 1. Environment Description

    Environment Description                            <Mandatory>


 2. Business Application Server Configuration

    Business Server Host                 <Mandatory> - Hostname on
                                           which application being
                                                         installed

    Business Server Application Name                    SPLService


 3. Web Application Server Configuration

    Web Server Host                                    <Mandatory>

    WebLogic SSL Port Number                           <Mandatory>

    WebLogic Console Port Number                       <Mandatory>

    Web Context Root                                          ouaf

    WebLogic JNDI User ID                              <Mandatory>

    WebLogic JNDI Password                             <Mandatory>

    WebLogic Server Name                                  myserver

    Web Server Application Name                             SPLWeb

    Deploy Application Viewer Module                          true

    Enable The Unsecured Health Check Service                false

    MDB RunAs User ID                                  <Mandatory>

    Super User IDs                                     <Mandatory>


 4. Database Configuration

    Application Server Database User ID                <Mandatory>

    Application Server Database Password               <Mandatory>

    XAI Database User ID                               <Mandatory>

    XAI Database Password                              <Mandatory>

    Batch Database User ID                             <Mandatory>

    Batch Database Password                            <Mandatory>

    Web JDBC DataSource Name                            <Optional>

    Database Name                                      <Mandatory>

    Database Server                                    <Mandatory>

    Database Port                                             1521

    ONS Server Configuration                            <Optional>

    Database Override Connection String                 <Optional>
    Character Based Database                                 false

    Oracle Client Character                    AMERICAN_AMERICA.AL32
    Set NLS_LANG                                              UTF8


5. General Configuration Options

    Batch RMI Port                                     <mandatory>

    RMI Port number for JMX Business                    <optional>

    RMI Port number for JMX Web                         <optional>

    JMX Enablement System User ID                       <optional>

    JMX Enablement System Password                      <optional>

    Coherence Cluster Name                             <mandatory>

    Coherence Cluster Address                          <mandatory>

    Coherence Cluster Port                             <Mandatory>

    Coherence Cluster Mode                         prod<Mandatory>


 6. OUAF TrustStore Options

    Import TrustStore Directory              <Mandatory> for Prod


Each item in the above list should be configured for a successful
install.

Choose option (1,2,3,4,5,6 <P> Process, <X> Exit):
```

10. When the parameter setup is complete, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.

11. Once the install or upgrade has finished, the installation log location is displayed on the screen. If the log does not list any error messages, the installation of the application component of Oracle Utilities Application Framework is complete.

Upgrading Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component

This section describes how to install the Oracle Utilities Meter Data Management, including:

- Copying and Decompressing the Install Media
- Installing the Oracle Utilities Meter Data Management Application Component

To proceed with the Oracle Utilities Meter Data Management installation you need to be connected to the target Oracle Utilities Application Framework environment.

You must initialize the Oracle Utilities Application Framework environment. For detailed instructions, refer to the Installing the Oracle Utilities Application Framework V4.4.0.3.0 Application Component section.

Copying and Decompressing the Install Media

The Oracle Utilities Meter Data Management installation file is delivered in jar format for both UNIX and Windows platforms.

To copy and decompress the install media:

1. Login to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip from Oracle Software Delivery Cloud.
3. Create a temporary directory such as c:\ouaf\temp or /ouaf/temp. (Referred to below as <TEMPDIR>)

   > **Note**: This directory must be located outside any current or other working Oracle Utilities application environment. All files that are placed in this directory as a part of the installation can be deleted after completing a successful installation.

4. Unzip Oracle Utilities Meter Data Management V2.4.0.0.0 Multiplatform.zip to get the file MDM_V2.4.0.0.0.zip from the delivered package and copy to the <TEMPDIR>. To use FTP to transfer this file, use the BINARY option.
5. Decompress the file:

   ```
   cd <TEMPDIR>
   unzip MDM_V2.4.0.0.0.zip
   cd App
   ```

For UNIX and Windows platforms, a sub-directory named MDM.V2.4.0.0.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installing the Oracle Utilities Meter Data Management Application Component

To install the Oracle Utilities Meter Data Management application component:

1. Log in to the application server host as Oracle Utilities Application Framework Administrator (default cissys).
2. Change directory:

   ```
   cd <install_dir>/bin
   ```

   where <install_dir> is the location where the Oracle Utilities Application Framework application component is installed.

3. Initialize the environment by running the appropriate command:

   UNIX

   ```
   ./splenviron.sh -e <ENV NAME>
   ```

   Windows

   ```
   splenviron.cmd -e <ENV NAME>
   ```

4. Navigate to <TEMPDIR>/MDM.V2.4.0.0.0 directory.
5. Run the install script.

Note: On UNIX, ensure that you have the proper execute permission on install.sh.

UNIX

```
ksh ./install.sh
```

Windows

```
install.cmd
```

6. Choose option P to proceed with the installation.

   Note: The rest of the menu items can be ignored if you are installing only MDM.

The Oracle Utilities Meter Data Management installation is complete if no errors occurred during the installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management

This section applies to an Oracle Utilities Smart Grid Gateway configuration in which Oracle Service Bus (OSB) or Oracle SOA Suite is installed on a separate host from the Oracle Utilities Application Framework's host. In this configuration, the Oracle Utilities installation scripts must have access to the libraries in the OSB and SOA servers' directories to deploy OSB projects and SOA composites successfully.

Follow these procedures to configure access to a remote OSB server:

- Create a network share to the osb folder within the Middleware Home on the remote OSB server.
- Provide the following values for Menu Item 8 (OSB Configuration) during the installation for Oracle Utilities Meter Data Management:

  Note: Use the completed OSB configuration worksheet to assist you in this step. See the Installation and Configuration Worksheets.

  - **OSB Home** is the location of the osb folder, accessed by way of network share.
  - **OSB Host Server** is the host name of the OSB server.
  - **OSB Port Number** is the port of the OSB admin server.
  - **OSB SSL Port Number** is the port of the OSB SSL admin server.
  - **OSB Managed Server Port Number** is the port of the OSB Managed Server.
  - **OSB Managed Server SSL Port Number** is the port of the OSB SSL Managed Server

Follow these procedures to configure access to a remote SOA Suite server:

- Create a network share to the soa folder within the Middleware Home on the remote SOA Suite server.
- Provide the following values for Menu Item 9 (SOA Configuration) during the installation for Oracle Utilities Meter Data Management.

Note: Use the completed SOA configuration worksheet to assist you in this step. See the Installation and Configuration Worksheets.

- **SOA Home** is the location of the soa folder, accessed by way of network share.
- **SOA Host Server** is the host name of the SOA managed server.
- **SOA Port Number** is the port of the SOA managed server.
- **SOA SSL Port Number** is the port of the SOA SSL managed server.

Upgrading the Oracle Utilities Smart Grid Gateway V2.2.0.3 SOA Suite Application Components

This section describes how to upgrade the SOA Suite application components of Oracle Utilities Smart Grid Gateway, including:

- Upgrading the MV90 Adapter for Itron
- Upgrading the Adapter Development Kit
- Upgrading the Adapter for Networked Energy Services
- Upgrading the Adapter for Itron OpenWay
- Upgrading the Adapter for Landis+Gyr
- Upgrading the Adapter for Sensus RNI
- Upgrading the Adapter Silver Spring Networks

Note: SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

Upgrading the MV90 Adapter for Itron

This section describes the installation of the MV90 Adapter for Itron, including:

- Before You Upgrade
- Upgrading the MV90 Adapter

Pre-installation Tasks for the MV90 Adapter

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway MV90 Adapter, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also, see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Meter Data Management environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

3. Stop the environment if running.

Upgrading the MV90 Adapter

To install the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Choose option P to proceed with the installation.
4. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute the post-installation steps described in Configuration Tasks for the MV90 Adapter.

Upgrading the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Pre-installation Tasks for the Adapter Development Kit
- Installation Tasks for the Adapter Development Kit

Pre-installation Tasks for the Adapter Development Kit

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also, see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter Development Kit

This section describes the installation of the Adapter Development Kit, including:

- Initializing the Oracle Utilities Application Framework Environment
- Upgrading the Adapter Development Kit

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Upgrading the Adapter Development Kit

To install the Oracle Utilities Smart Grid Gateway Adapter Development Kit:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The Configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 21 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described Configuration Tasks for the Adapter Development Kit.

Upgrading the Adapter for Networked Energy Services

This section describes the installation of the Adapter for Networked Energy Services, including:

- Pre-installation Tasks for the Adapter for Networked Energy Services
- Upgrading the Adapter for Networked Energy Services

Pre-installation Tasks for the Adapter for Networked Energy Services

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Serversfor versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities SApplication Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Upgrading the Adapter for Networked Energy Services

To install the Oracle Utilities Smart Grid Gateway Adapter for Networked Energy Services:

1. Run the following install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 17 to configure the URI for the NES head-end system web services.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

UNIX

```
$SPLEBASE/bin/initialSetup.sh
```

Windows

```
%SPLEBASE%\bin\ initialSetup.cmd
```

Once the install has finished successfully, execute postinstallation steps described in Configuration Tasks for the Adapter for Networked Energy Services.

Upgrading the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Pre-installation Tasks for the Adapter for Itron OpenWay
- Installation Tasks for the Adapter for Itron OpenWay

Pre-installation Tasks for the Adapter for Itron OpenWay

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Installation Tasks for the Adapter for Itron OpenWay

This section describes the installation of the Adapter for Itron OpenWay, including:

- Initializing the Oracle Utiliies Application Framework Environment
- Upgrading the Adapter for Itron OpenWay

Initializing the Oracle Utiliies Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Upgrading the Adapter for Itron OpenWay

To install the Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 22 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Itron OpenWay.

Upgrading the Adapter for Landis+Gyr

This section describes the installation of the Adapter for Landis+Gyr, including:

- Pre-installation Tasks for the Adapter for Landis+Gyr
- Upgrading the Adapter for Landis+Gyr

Pre-installation Tasks for the Adapter for Landis+Gyr

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media

- Initializing the Oracle Utilities Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework Environment

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Upgrading the Adapter for Landis+Gyr

To install the Oracle Utilities Smart Grid Gateway Adapter for Landis+Gyr:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh. The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 16 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option P to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Landis+Gyr.

Upgrading the Adapter for Sensus RNI

This section describes the installation of the Adapter for Sensus RNI, including:

- Pre-installation Tasks for the Adapter for Sensus RNI
- Upgrading the Adapter for Sensus RNI

Pre-installation Tasks for the Adapter for Sensus RNI

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utiliies Application Framework Environment

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Please refer to the Operating Systems and Application Servers for versions and installation details regarding the database and operating system. Also see Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).

2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

Windows

```
%SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
```

Upgrading the Adapter for Sensus RNI

To install the Oracle Utilities Smart Grid Gateway Adapter for Sensus RNI:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 18 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. When you are done setting up the parameters, choose option **P** to proceed with the installation.

7. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Sensus RNI.

Upgrading the Adapter Silver Spring Networks

This section describes the installation of the Adapter for Silver Spring Networks, including:

- Pre-installation Tasks for the Adapter for Silver Spring Networks
- Upgrading the Adapter for Silver Spring Networks

Pre-installation Tasks for the Adapter for Silver Spring Networks

This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- Copying and Decompressing the Installation Media
- Initializing the Oracle Utilities Application Framework

Copying and Decompressing the Installation Media

The installation file is delivered in jar format for both UNIX and Windows platforms.

Oracle Utilities Smart Grid Gateway is delivered as part of the Oracle Utilities Meter Data Management installation package. Refer to the Supported Platforms and Hardware Requirements for versions and installation details regarding the database and operating system. See Installing Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Login to the host server as the Oracle Utilities Application Framework administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Application Framework.

Initializing the Oracle Utilities Application Framework

1. Login as Oracle Utilities Application Framework Administrator (default cissys).
2. Initialize the Oracle Utilities Application Framework environment that you want to install the product into.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh  -e $SPLENVIRON
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   ```

Upgrading the Adapter for Silver Spring Networks

To install the Oracle Utilities Smart Grid Gateway Adapter for Silver Spring Networks:

1. Run the install script.

   UNIX

   ```
   ksh ./configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   > **Note:** On UNIX, ensure that you have the proper execute permission on install.sh.

   The configuration menu for Oracle Utilities Smart Grid Gateway appears.

2. Select menu item 8 to configure OSB.

   Use the completed OSB configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

3. Select menu item 9 to configure SOA.

Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

4. Select menu item 10 to configure the SOA Configuration Plan.

   Use the completed SOA Configuration Plan (MDM) worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

5. Select menu item 19 to configure the URI of the head-end system.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

6. Select menu item 20 to configure the JMS source destination bridge.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

7. Select menu item 70 to configure the test harness.

   Use the completed SOA configuration worksheet to assist you in this step. Refer to Appendix B: Installation and Configuration Worksheets.

8. When you are done setting up the parameters, choose option P to proceed with the installation.

9. Run initialSetup.sh.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd
   ```

Once the install has finished successfully, execute post-installation steps described in Configuration Tasks for the Adapter for Silver Spring Networks.

Operating the Application

At this point your installation and custom integration process is complete. Be sure to read the *Server Administration Guide* (included in this release) for more information on further configuring and operating the system.

Chapter 7

Configuring the Oracle Utilities Smart Grid Gateway Adapters

This chapter describes configuration tasks such as deploying OSB and SOA adapters for the Oracle Utilities Smart Grid Gateway adapters. It includes:

Note: SOA Suite is NOT required with native implementations of Smart Grid Gateway adapters. See **Smart Grid Gateway Implementations** in the *Oracle Utilities Meter Solution Administrative User Guide* for more information.

Configuration Tasks for the MV90 Adapter

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway MV90 Adapter, including:

- Deploying the OSB Adapter for the MV90
- Starting the Application

Deploying the OSB Adapter for the MV90

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance. To deploy the OSB adapter, use the following procedures.

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>.

```
mv90-usage
mv90-usage-arch
mv90-usage-error
```

2. Start the example OSB WebLogic instance.
   Refer to the section Creation of Example Weblogic Domains.

   UNIX

```
cd $SPLEBASE/osbapp
./startWebLogic.sh
```

   Windows

```
cd %SPLEBASE%\osbapp
startWebLogic.cmd
```

3. Create JMS queues and target them to the OSB admin server.
   a. Create a JMS server “OSB-JMSServer” and target it to admin server.
   b. Create a JMS module “MV90-SystemModule”.
   c. Under “MV90-SystemModule” create a sub-deployment “MV90-JMSFAServer” and target it to “OSB-JMSServer”.
   d. Create the following JMS queues:

Queue Name: DestinationQueue-D5

JNDI Name: DestinationQueue-D5

Sub-deployment: MV90-JMSFAServer

Targets: OSB-JMSServer

Queue Name: NotificationQueue-D5

JNDI Name: NotificationQueue-D5

Sub-deployment: MV90-JMSFAServer

Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.

   For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

   UNIX

   ```
   ccd $SPLEBASE/osbapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile
   deploy-osb_MV90.xml -Dadmin.user=<ADMIN_USER> -
   Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
   Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
   Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
   Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
   ```

   > **Note:** Use the following command if this is an upgrade from a previous version:

   ```
   cd $SPLEBASE/osbapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile
   deploy-osb_MV90.xml
   update_osb -Dadmin.user=<ADMIN_USER> -
   Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
   Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
   Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
   Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
   ```

   This will not override any OSB custom changes.

   Windows

   ```
   cd %SPLEBASE%\osbapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-osb_MV90.xml -Dadmin.user=<ADMIN_USER> -
   Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
   Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
   Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
   Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
   ```

   > **Note:** Use the following command if this is an upgrade from a previous version:

   ```
   update_osb -Dadmin.user=<ADMIN_USER> -
   Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
   Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
   Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
   Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
   ```

   This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “MV90-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D5" and accept the default targets.

3. Under the Foreign Server, navigate to the **General** tab and configure the following:
   a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
   b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
   c. JNDI Properties Credential: Credentials for user with access to OSB server
   d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
   e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
   - Name: DestinationQueue-D5
     Local JNDI Name: ForegnDestinationQueue-D5
     Remote JNDI Name: DestinationQueue-D5
   - Name: IMDDestinationQueue-D5
     Local JNDI Name: ForegnIMDDestinationQueue-D5
     Remote JNDI Name: IMDDestinationQueue-D5
   - Name: NotificationQueue-D5
     Local JNDI Name: ForegnNotificationQueue-D5
     Remote JNDI Name: NotificationQueue-D5
5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-D5
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D5
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D5
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D5
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D5
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D5
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

See Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

To deploy on a separate WebLogic instance:

1. Create the following directories under <OSB_LOG_DIR>.

```
mv90-usage
mv90-usage-arch
mv90-usage-error
```

2. Copy the following jars to the lib folder under the WebLogic domain directory.

```
spl-d1-osb-2.4.0.0.0.jar
```

   This jar is present under the following location:

   UNIX: $SPLEBASE/etc/lib

Windows: %SPLEBASE%\etc\lib

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server:
   - Create a JMS server “OSB-JMSServer” and target it to admin server.
   - Create a JMS module “MV90-SystemModule”.
   - Under “MV90-SystemModule” create a sub-deployment “MV90-JMSFAServer” and target it to “OSB-JMSServer”.
   - Create the following JMS queues:

     Queue Name: DestinationQueue-D5

     JNDI Name: DestinationQueue-D5

     Sub-deployment: MV90-JMSFAServer

     Targets: OSB-JMSServer

     Queue Name: NotificationQueue-D5

     JNDI Name: NotificationQueue-D5

     Sub-deployment: MV90-JMSFAServer

     Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance.
   For SSL deployment please refer to the section Deploying OSB adapter on SSL.

   UNIX

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile
    deploy-osb_MV90.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile
deploy-osb_MV90.xml -Dadmin.user=<ADMIN_USER> -
```

```
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile
deploy-osb_MV90.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “MV90-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D5" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D5
      Local JNDI Name: ForegnDestinationQueue-D5
      Remote JNDI Name: DestinationQueue-D5
    - Name: IMDDestinationQueue-D5
      Local JNDI Name: ForegnIMDDestinationQueue-D5
      Remote JNDI Name: IMDDestinationQueue-D5
    - Name: NotificationQueue-D5
      Local JNDI Name: ForegnNotificationQueue-D5
      Remote JNDI Name: NotificationQueue-D5
5. Under **Connection Factories**, create the following foreign connection factories:
    - Name: DestinationQueueConnectionFactory-D5
      Local JNDI Name: ForegnDestinationQueueConnectionFactory-D5
      Remote JNDI Name: weblogic.jms.XAConnectionFactory

- Name: IMDDestinationQueueConnectionFactory-D5
  Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D5
  Remote JNDI Name: weblogic.jms.XAConnectionFactory
- Name: NotificationQueueConnectionFactory-D5
  Local JNDI Name: ForegnNotificationQueueConnectionFactory-D5
  Remote JNDI Name: weblogic.jms.XAConnectionFactory

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) document on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role.
>
> The WebLogic console application can be accessed from the following URL: http://<hostname>:<portname>/ console

Configuration Tasks for the Adapter Development Kit

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway Adapter Development Kit, including:

- Deploying the OSB Adapter for the Adapter Development Kit
- Deploying the SOA Adapter for the Adapter Development Kit
- Configuring Security for the SOA System
- Starting the Application

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for the Adapter Development Kit

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server. To deploy the OSB adapter, use the following procedures:

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>:

   ```
   dg-csv-error
   dg-csv
   dg-xml-error
   dg-xml-arch
   dg-xml
   dg-csv-arch
   dg-seeder-error
   dg-seeder-arch
   dg-seeder
   ```

2. Start the example OSB WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/osbapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\osbapp
   startWebLogic.cmd
   ```

3. Create JMS queues and target them to the OSB admin server:

   - Create a JMS server "OSB-JMSServer" and target it to admin server.
   - Create a JMS module "DG-SystemModule"
   - Under "DG-SystemModule" create a sub-deployment "DG-JMSFAServer" and target it to "OSB-JMSServer"
   - Create the following JMS queues:

     Queue Name: DestinationQueue-DG

     JNDI Name: DestinationQueue-DG

     Sub-deployment: DG-JMSFAServer

     Targets: OSB-JMSServer

     Queue Name: IMDDestinationQueue-DG

     JNDI Name: IMDDestinationQueue-DG

     Sub-deployment: DG-JMSFAServer

     Targets: OSB-JMSServer

     Queue Name: NotificationQueue-DG

     JNDI Name: NotificationQueue-DG

     Sub-deployment: DG-JMSFAServer

     Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.
   For SSL deployment please refer to the section Deploying OSB adapter on SSL.

UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_DG.xml -
Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

> **Note**: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile
deploy-osb_DG.xml update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_DG.xml
- Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

> **Note:** Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_DG.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “DG-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-DG" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server

   d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential

   e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>

4. Under **Destinations**, create the following foreign destinations:

   - Name: DestinationQueue-DG
     Local JNDI Name: ForegnDestinationQueue-DG
     Remote JNDI Name: DestinationQueue-DG

   - Name: IMDDestinationQueue-DG
     Local JNDI Name: ForegnIMDDestinationQueue-DG
     Remote JNDI Name: IMDDestinationQueue-DG

   - Name: NotificationQueue-DG
     Local JNDI Name: ForegnNotificationQueue-DG
     Remote JNDI Name: NotificationQueue-DG

5. Under **Connection Factories**, create the following foreign connection factories:

   - Name: DestinationQueueConnectionFactory-DG
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: IMDDestinationQueueConnectionFactory-DG
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: NotificationQueueConnectionFactory-DG
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

To deploy on a separate WebLogic instance:

1. Create the following directories under <OSB_LOG_DIR>.

```
dg-csv-error
dg-csv
dg-xml-error
dg-xml-arch
dg-xml
dg-csv-arch
dg-seeder-error
dg-seeder-arch
dg-seeder
```

2. Copy the following jars to the lib folder under the WebLogic's domain directory:

```
spl-d1-osb-2.4.0.0.0.jar
```

   These jars are present under the following location:

   UNIX

```
$SPLEBASE/etc/lib
```

Windows

```
%SPLEBASE%\etc\lib
```

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server.
    - Create a JMS server "OSB-JMSServer" and target it to admin server.
    - Create a JMS module "DG-SystemModule"
    - Under "DG-SystemModule" create a sub-deployment "DG-JMSFAServer" and target it to "OSB-JMSServer"
    - Create the following JMS queues:

    Queue Name: DestinationQueue-DG

    JNDI Name: DestinationQueue-DG

    Sub-deployment:: DG-JMSFAServer

    Targets: OSB-JMSServer

    Queue Name: IMDDestinationQueue-DG

    JNDI Name: IMDDestinationQueue-DG

    Sub-deployment: DG-JMSFAServer

    Targets: OSB-JMSServer

    Queue Name: NotificationQueue-DG

    JNDI Name: NotificationQueue-DG

    Sub-deployment: DG-JMSFAServer

    Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance.
   For SSL deployment please refer to the section Deploying OSB adapter on SSL.

   Note:- Modify the OSB Host Server,OSB Port Number according to Standalone domain using "OSB Configuration Menu item 8".

UNIX

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_DG.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_DG.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_DG.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>

%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_DG.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “DG-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-DG" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-DG
      Local JNDI Name: ForegnDestinationQueue-DG
      Remote JNDI Name: DestinationQueue-DG
    - Name: IMDDestinationQueue-DG
      Local JNDI Name: ForegnIMDDestinationQueue-DG
      Remote JNDI Name: IMDDestinationQueue-DG

- Name: NotificationQueue-DG
  Local JNDI Name: ForegnNotificationQueue-DG
  Remote JNDI Name: NotificationQueue-DG

5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-DG
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-DG
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-DG
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-DG
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for the Adapter Development Kit

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To deploy the SOA adapter, use the following procedures:

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at the locations below for JAVA_OPTIONS:

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   startWebLogic.cmd
   ```

2. Add “-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>” to the JAVA_OPTIONS.

3. Start the example SOA WebLogic instance:

   UNIX

   ```
   cd $SPLEBASE/soaapp

   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

4. Deploy the SOA adapter on the example WebLogic instance.
   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
    %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_DG.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

5. Deploy the TestHarness SOA composites on example WebLogic instance.
   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   > **Note:** Open the command prompt as Administrative mode and then select the environment to deploy SOA.

   ```
   cd %SPLEBASE%/soaapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_DG.xml deployTestHarness  -Dserver.password=<SOA_USER>
   -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

6. Import the Policy Templates and Policies.

   a. First, import the policy template jar using Enterprise Manager.

      Linux

      ```
      cd $SPLEBASE/soaapp
      $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
      policy.xml -Dproduct=d1
      ```

      Windows

      ```
      cd %SPLEBASE%/soaapp
      $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
      policy.xml -Dproduct=d1
      ```

    a. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
    b. Right-click the domain and navigate to **Web Services, WSM Policies.**
    c. Click **Web Services Assertion Templates** at the top of the page.
    d. Click **Import** and import the sgg-d1-policy.jar file.

    This file is located in the following directory:

    UNIX: $SPLEBASE/soaapp/policies/jars

    Windows: %SPLEBASE%\soaapp\policies\jars

b. For SOA 12c version, perform the following steps to import policies:

    a. Import the “sgg_dg_cfs_multispeak_header_client_policy” policy file ($SPLEBASE/soaapp) using Enterprise Manager.
    b. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
    c. Create a "META-INF\policies\oracle" folder structure and copy the policy under oracle folder and zip the entire folder as “sgg_dg_cfs_multispeak_header_client_policy.zip”.
    d. Right-click the domain and navigate to **Web Services, WSM Policies.**
    e. Click **Import** and import sgg_dg_cfs_multispeak_header_client_policy.zip.

    This file is located in the following directory:

    UNIX: $SPLEBASE/soaapp

    Windows: %SPLEBASE%\soaapp

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Create WebLogic SOA Domain and select Enterprise Manager option.
2. Copy the following jar file to the lib folder under the WebLogic domain directory, spl-d1-soa- security.jar

    This jar is present under the following location:

    UNIX: $SPLEBASE/etc/lib

    Windows: %SOA_HOME%\etc\lib
3. Add system permissions for Smart Grid Gateway security policies as follows:
    a. Log on to Oracle Enterprise Manager as an administrative user.
    b. Select **WebLogic Domain**, then **Security**, then **System Policies**.

    The **System Policies** page opens.
    c. Search for an existing permission for the Smart Grid Gateway security jar as follows:

a. Select “Codebase” from the **Type** drop-down list (you should not have to change this).

b. Select “Includes” from the **Name** drop-down list.

c. Enter “spl-d1-soa-security.jar” into the search field.

d. Click the arrow button.

e. No policies should be found:

d. Click **Create**.

The **Create System Grant** page opens.

e. Select "Codebase" from the **Grant To** drop-down list.

f. Enter the complete path to the security jar in the **Codebase** field.

```
"file:${domain.home}/lib/spl-d1-soa-security.jar"
```

g. Click **Add** (under **Permissions**).

The **Add Permission** window opens.

h. Select the "**Select here to enter details for a new permission** checkbox.

The following fields appear:

- Permission Class
- Resource Name
- Permission Actions

i. Enter the following details into the three fields:

Field	Value
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission
Resource Name	context=SYSTEM,mapName=*,keyName=*
Permission Actions	*

j. Click **OK** to close the **Add Permission** window.

k. Click **OK** (on the **Create System Grant** page) to save the system grant.

l. Repeat the search from step 2 to confirm the new system policy exists:

This search should return the system policy you just added.

4. Copy the SGGLogin.config file from below location to the config directory of Weblogic SOA domain and edit the startWeblogic script located of Weblogic SOA domain-> bin for JAVA_OPTIONS:

a. This SGGLogin.config is present under the following location:

UNIX: $SPLEBASE/soaapp/config

Windows: %SOA_HOME%\soaapp\config

b. Copy the file.

UNIX: <Weblogic_SOA_domain>/config

Windows: <Weblogic_SOA_domain>\config

c. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS to

   UNIX: <Weblogic_SOA_domain>/bin/startWeblogic.sh

   Windows: <Weblogic_SOA_domain>\bin\startWeblogic.cmd

5. Start the separate WebLogic instance.

6. Before SOA composites deployment, import the Policy Templates and Policies.

   a. Import the policy template jar using Enterprise Manager.

   Linux

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d1
```

   Windows

```
cd %SPLEBASE%/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d1
```

      a. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

      b. Right-click the domain and navigate to **Web Services, WSM Policies.**

      c. Click **Web Services Assertion Templates** at the top of the page.

      d. Click **Import** and import the sgg-d1-policy.jar zip.

      This file is located in the following directory:

      UNIX: $SPLEBASE/soaapp/policies/jars

      Windows: %SPLEBASE%\soaapp\policies\jars

   b. For SOA 12c version, perform the following steps to import policies:

      a. Import the "sgg_dg_cfs_multispeak_header_client_policy" policy file ($SPLEBASE/soaapp) using Enterprise Manager.

      b. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

      c. Create a "META-INF\policies\oracle" folder structure, copy the policy under oracle folder and zip the entire folder as "sgg_dg_cfs_multispeak_header_client_policy.zip".

      d. Right-click the domain and navigate to **Web Services, WSM Policies.**

      e. Click **Import** and import the sgg_dg_cfs_multispeak_header_client_policy.zip file.

      This file is located in the following directory:

      UNIX: $SPLEBASE/soaapp

      Windows: %SPLEBASE%\soaapp

7. Deploy the SOA cartridge on the separate WebLogic instance.

   Note: Modify the SOA Host Server, SOA Port Number, SOA WebLogic User Name, SOA WebLogic User Password and Endpoint URLs menu items according to separate domain using “SOA Configuration Menu item 9”.

   For SSL deployment, refer to Deploying SOA Composites on SSL.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
   soa_MDF.xml -Dserver.user=<ADMIN_USER> -
   Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant
   -buildfile deploy-soa_DG.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties
   ```

8. Deploy the TestHarness SOA composites on the separate WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
   deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_DG.xml deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

Configuring Security for the SOA System

Security is managed through policies attached to the input and output points of each composite. More information on policies and their configuration can be found in **Chapter 10: Configuring Policies** in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*.

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework
- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server.
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click the domain, and choose **Security**, **Credentials**.
2. On the **Credentials** page, click **Create Map**.
3. In the **Create Map** dialog, name the map **oracle.wsm.security**, then click **OK**.
4. Click **Create Key** and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.dg.credentials
    - **Type:** Password
    - **Username:** A valid WebLogic user name
    - **Password:** A valid WebLogic password
5. Click **OK**.
6. Click **Create Key** again and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** **s**gg.dg.ouaf.credentials
    - **Type:** Password
    - **Username:** A valid OUAF user name
    - **Password:** A valid OUAF password
7. Click **OK**.

Configuring Security for the SOA System to Communicate with the Head-End System

The ADK Test Harness is a frequently-used substitute for a real head-end System. Some specific settings highlighted below will facilitate connecting to and using the Test Harness.

- Creating Security Credentials
- Creating the Web Service Policy for the Security Credentials

Creating Security Credentials

Configuring security for the SOA system involves creating the security credentials in Oracle Enterprise Manager.

To create the security credential in the Credential File Store (CFS):

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. In the WebLogic Domain menu, navigate to **Security**, **Credentials**.
3. Click **Create Map** to set up a new credentials store.
4. In the **Create Map** dialog box, enter a unique value in the **Map Name** field.
5. Click **OK**.
6. Select the new map in the **Credentials** list and click **Create Key**.
7. In the **Create Key** dialog box, enter the appropriate values in the fields. In the **Type** field, select **Password**.
8. Click **OK**.

   By default, the sgg_dg_cfs_multispeak_header_client_policy policy imported previously uses a Credential Map named “dg.security” and a Credential Key called “dg.credentials.” Use these values unless making changes to the template values.

   Test Harness Note: By default, the Test Harness expects a user name of “MultiSpeakUserID” and a password of “MultiSpeakPwd.”

Creating the Web Service Policy for the Security Credentials

To create a web service policy for the security credentials:

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. In the WebLogic Domain menu, navigate to **Web Services, Policies**.
3. Select the policy oracle/wss_http_token_client_policy.
4. Click **Create Like.**
   - Give the policy a unique name and an appropriate description.
   - Under Assertions, remove the Log Message and the HTTP Security policies.
   - Click **Add.**
   - Enter a name for the new assertion.
   - In the Assertion Template field, select sgg/d1_csf_access_client_xpath_template.

- Click **OK.**

5. In the Assertion Content field, edit property values in the XML according to the example below. The following table lists the property values that should be edited:

Field	Default Value	Description
csf-map		Required. The credential store map to use. This value is specified in the task **Creating Security Credentials** on page 7-20.
csf-key		Required. The key in the credential store map that will resolve to a username-password pair. This value is specified in the task **Creating Security Credentials** on page 7-20.
namespaceDefinitions		Prefix-namespace definitions used in the xpath fields below. Each should be in the form prefix=namespace. Multiple definitions should be separated by spaces. Default namespaces cannot be set.
soapElement	Header	The context node for xpath searches, either the SOAP header or the SOAP body. Legal values are "header" and "body."
userid.xpath		The xpath to the location to inject the username in the SOAP element. The statement must resolve to an attribute or element that already exists.
password.xpath		The xpath to the location to inject the password in the SOAP element. The statement must resolve to an attribute or element that already exists.
isDebuggingActive	false	Reserved for internal use.

```
<orasp:SGGCredentialStoreInsertionXPath xmlns:orawsp="http://
schemas.oracle.com/ws/2006/01/policy" orawsp:Silent="true"
orawsp:name="CSF_DG" orawsp:description="Properties to add CSF
credentials to a SOAP message" orawsp:Enforced="true"
orawsp:category="security/authentication" xmlns:orasp="http://
schemas.oracle.com/ws/2006/01/securitypolicy">
    <orawsp:bindings>

<orawsp:Implementation>com.splwg.d1.sgg.soa.common.security.policy.Cre
dentialStorageFacilityAccessAssertationExecutor</
orawsp:Implementation>
        <orawsp:Config orawsp:name="CSFKeyInsertionConfig"
orawsp:configType="declarative">
            <orawsp:PropertySet orawsp:name="CSFKeyProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-map">
                    <orawsp:Description>Which CSF map to use</
orawsp:Description>
```

```
                    <orawsp:Value>CSF_map_name</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-key">
                    <orawsp:Description>Which key in the map to use</
orawsp:Description>
                    <orawsp:Value>CSF_Key</orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="XPathProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="soapElement">
                  <orawsp:Description>The segment of the soap message
to which to write.  Legal Values are "header" &amp; "body"</
orawsp:Description>
                    <orawsp:Value>header</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="optional" orawsp:name="namespaceDefinitions">
                    <orawsp:Description>A space-separated list of
prefix-namespace pairs.  For example: ns1=http://myurl.com/ns1
ns2=http://oracle.com xsd=http://www.w3.org/2001/XMLSchema</
orawsp:Description>
                    <orawsp:Value>ns1=http://www.multispeak.org/
Version_4.1_Release</orawsp:Value/>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="userid.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the user id.</
orawsp:Description>
                    <orawsp:Value>./ns1:MultiSpeakMsgHeader/@UserID</
orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="password.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the password.</
orawsp:Description>
                    <orawsp:Value>./ns1:MultiSpeakMsgHeader/@Pwd</
orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="DebugProperties">
                <orawsp:Property orawsp:type="boolean"
orawsp:contentType="optional" orawsp:name="isDebuggingActive">
                    <orawsp:Description>controls debugging output</
orawsp:Description>
                    <orawsp:Value>false</orawsp:Value>
                    <orawsp:DefaultValue>false</orawsp:DefaultValue>
                </orawsp:Property>
            </orawsp:PropertySet>
        </orawsp:Config>
    </orawsp:bindings>
</orasp:SGGCredentialStoreInsertionXPath>
```

6. Save the policy.
7. Attach the policy to the MR_Server reference on the Common composite.
    a. In Oracle Enterprise Manager, navigate to the **DG/Common** composite.
    b. Navigate to the Policies tab.

   c. From the **Attach To/Detach From** menu, select **MR_Server**.
   d. In the Attached Policies window, select the oracle/wss_http_token_client_policy.
   e. Click **Detach** to remove the default security policy.
   f. In the Available Policies window, select the policy that you just created.
   g. Click **Attach** to attach the policy to the MR_Server reference.

8. Attach the policy to the CD_Server reference on the Common composite.
   a. Navigate to the **DG/Common** composite.
   b. Navigate to the **Policies** tab.
   c. In the **Attach To/Detach From** menu, select **CD_Server**.
   d. In the **Attached Policies** window, select oracle/wss_http_token_client_policy.
   e. Click **Detach** to remove the default security policy.
   f. In the **Available Policies** window, select the policy that you just created.
   g. Click **Attach** to attach the policy to the CD_Server reference.
9. Attach the policy to the OD_Server reference on the Common composite.
   a. Navigate to the **DG/Common** composite.
   b. Navigate to the **Policies** tab.
   c. From the **Attach To/Detach From** menu, select **OD_Server**.
   d. In the **Attached Policies** window, select oracle/wss_http_token_client_policy.
   e. Click **Detach** to remove the default security policy.
   f. In the **Available Policies** window, select the policy that you just created.
   g. Click **Attach** to attach the policy to the OD_Server reference.

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) document on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Configuration Tasks for the Adapter for Networked Energy Services

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway Adapter for Networked Energy Services, including:

- Deploying the OSB Adapter for Networked Energy Services
- Deploying the SOA Adapter for Networked Energy Services
- Deploying the Test Harness
- Configuring the Networked Energy Services Head-End System to Report Events
- Configuring Security for the SOA System
- Starting the Application

Note: Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for Networked Energy Services

This section describes how to deploy the OSB Adapter.

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>:

```
d4-event
d4-event-arch
d4-event-error
d4-usage
d4-usage-arch
d4-usage-error
```

2. Start the example OSB WebLogic instance.

UNIX

```
cd $SPLEBASE/osbapp
./startWebLogic.sh
```

Windows

```
cd %SPLEBASE%\osbapp
startWebLogic.cmd
```

3. Create JMS queues and target them to the OSB admin server:

   a. Create a JMS server “OSB-JMSServer” and target it to the admin server.

   b. Create a JMS module “D4-SystemModule”

   c. Under “D4-SystemModule” create a sub-deployment “D4-JMSFAServer” and target it to “OSB-JMSServer”

   d. Create the following JMS queues:

      Queue Name: DestinationQueue-D4

JNDI Name: DestinationQueue-D4

Sub-deployment: D4-JMSFAServer

Targets: OSB-JMSServer

Queue Name: IMDDestinationQueue-D4

JNDI Name: IMDDestinationQueue-D4

Sub-deployment: D4-JMSFAServer

Targets: OSB-JMSServer

Queue Name: NotificationQueue-D4

JNDI Name: NotificationQueue-D4

Sub-deployment: D4-JMSFAServer

Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.
   For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

   UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
 update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D4.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
```

```
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D4-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D4" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D4
      Local JNDI Name: ForegnDestinationQueue-D4
      Remote JNDI Name: DestinationQueue-D4
    - Name: IMDDestinationQueue-D4
      Local JNDI Name: ForegnIMDDestinationQueue-D4
      Remote JNDI Name: IMDDestinationQueue-D4
    - Name: NotificationQueue-D4
      Local JNDI Name: ForegnNotificationQueue-D4
      Remote JNDI Name: NotificationQueue-D4
5. Under **Connection Factories**, create the following foreign connection factories:
    - Name: DestinationQueueConnectionFactory-D4
      Local JNDI Name: ForegnDestinationQueueConnectionFactory-D4
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: IMDDestinationQueueConnectionFactory-D4
      Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D4
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: NotificationQueueConnectionFactory-D4
      Local JNDI Name: ForegnNotificationQueueConnectionFactory-D4
      Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

1. Create the following directories under <OSB_LOG_DIR>.

   ```
   d4-event
   d4-event-arch
   d4-event-error
   d4-usage
   d4-usage-arch
   d4-usage-error
   ```

2. Copy the following jars to the lib folder under the WebLogic's domain directory.

   ```
   spl-d1-osb-2.4.0.0.0.jar
   ```

   This jar is present under the following location:

   UNIX: `$SPLEBASE/etc/lib`

   Windows: `%SPLEBASE%\etc\lib`

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server:
   - Create a JMS server "OSB-JMSServer" and target it to the admin server
   - Create a JMS module "D4-SystemModule"
   - Under "D4-SystemModule" create a sub-deployment "D4-JMSFAServer" and target it to "OSB-JMSServer"
   - Create the following JMS queues:

     Queue Name: DestinationQueue-D4

     JNDI Name: DestinationQueue-D4

     Sub-deployment: D4-JMSFAServer

     Targets: OSB-JMSServer

     Queue Name: IMDDestinationQueue-D4

     JNDI Name: IMDDestinationQueue-D4

     Sub-deployment: D4-JMSFAServer

     Targets: OSB-JMSServer

     Queue Name: NotificationQueue-D4

     JNDI Name: NotificationQueue-D4

     Sub-deployment: D4-JMSFAServer

     Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance by running the following command from the Oracle Utilities application server:

   For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

   UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

   This will not override any OSB custom changes

   Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D4.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D4.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

   This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D4-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D4" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
   a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory

b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)

c. JNDI Properties Credential: Credentials for user with access to OSB server

d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential

e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>

4. Under **Destinations**, create the following foreign destinations:
   - Name: DestinationQueue-D4
     Local JNDI Name: ForegnDestinationQueue-D4
     Remote JNDI Name: DestinationQueue-D4
   - Name: IMDDestinationQueue-D4
     Local JNDI Name: ForegnIMDDestinationQueue-D4
     Remote JNDI Name: IMDDestinationQueue-D4
   - Name: NotificationQueue-D4
     Local JNDI Name: ForegnNotificationQueue-D4
     Remote JNDI Name: NotificationQueue-D4
5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-D4
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D4
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D4
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D4
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D4
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D4
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for Networked Energy Services

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To deploy the SOA adapter, use the following procedures.

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at below locations for JAVA_OPTIONS:

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

2. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS
3. Start the example SOA WebLogic instance:

   UNIX
   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows
   ```
    cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

4. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX
   ```
   cd $SPLEBASE/soaapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>> -
   DsysPropFile=soa.properties
   ```

   Windows
   ```
   cd %SPLEBASE%\soaapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D4.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Copy the following jar file to the lib folder under the WebLogic domain directory:

   ```
   spl-d1-soa-security.jar
   ```

   This jar is present under the following location:

   UNIX: `$SPLEBASE/etc/lib`

   Windows: `%SPLEBASE%\etc\lib`

2. Copy the SGGLogin.config file from below location to the config directory of WebLogic SOA domain and edit the startWeblogic script located of WebLogic SOA domain-> bin for JAVA_OPTIONS:

a. This SGGLogin.config is present under the following location:

   UNIX: `$SPLEBASE/soaapp/config`

   Windows: `%SOA_HOME%\soaapp\config`

b. Copy the file.

   UNIX: `<Weblogic_SOA_domain>/config`

   Windows: `<Weblogic_SOA_domain>\config`

3. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/ SGGLogin.config - Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS to

   UNIX: `<Weblogic_SOA_domain>/bin/startWeblogic.sh`

   Windows: `<Weblogic_SOA_domain>\bin\startWeblogic.cmd`

4. Start the separate WebLogic instance.

5. Deploy the SOA adapter on the separate WebLogic instance by running the following command from the Oracle Utilities application server:

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

UNIX
For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties
```

Windows

```
cd %SPLEBASE%\soaapp
```

For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties

%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D4.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties
```

Deploying the Test Harness

The test harness is a set of mock web services that can be used to test the SOA configuration setup and functionality in the absence of an actual physical head-end system. This is an optional task.

> **Note:** The test harness is not a supported feature of the application.

Use the following procedures to deploy the test harness SOA adapter:

To Deploy on the Example WebLogic Instance

1. Deploy the test harness on the example WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   Note: Open the command prompt as Administrative mode and then select the environment to deploy SOA.

   ```
   cd %SPLEBASE%/soaapp
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_D4.xml deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

1. Deploy the SOA adapter on the separate WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
   deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D4.xml
    deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

Configuring the Networked Energy Services Head-End System to Report Events

This section describes how to configure the Networked Energy Services head-end system to report events to the Networked Energy Services. Configuring the head-end system requires using the NES Diagnostic Tool to specify the following system properties:

- Event Delivery Type

- Event Receiver URL
- Event Receiver Namespace
- API Key Timeout Period

Configuring the Event Delivery Type

To configure the event delivery type:

1. In the NES Diagnostic Tool navigation tree, navigate to **NES System Data, Event Configuration.**
2. In the tree, select the **Add Device Failure** event to view its properties.
3. Set the DELIVERYTYPEID property to **EventDeliveryType.SOAP.**

Repeat this task for each of the following events:

- Add Device Failure
- Add Device Success
- Connect Device Load Command Complete
- Disconnect Device Load Command Complete
- Move Device Success
- Move Device Failure
- Read Device Load Profile On-Demand Command Complete
- Read Device Full Load Profile Command Complete
- Read Device Load Status Command Complete
- Read Device Billing Data On-Demand Command Complete
- Set Device ATM Configuration Command Complete

Configuring the Event Receiver URL

To configure the event receiver URL:

1. In the NES Diagnostic Tool navigation tree, navigate to **NES System Data, Settings, Solution Settings.**
2. Select **Event Receiver URL** to view its properties.
3. Set the VALUE property to the URL that is specified for the web service ReceivePanoramixEvents. For example:

   ```
   http://<NES_HOST>:<PORT_NUMBER>/soa-infra/services/Echelon_NES/
    HandleReceiveEvents/ReceivePanoramixEvents
   ```

4. Restart the application server that hosts the Networked Energy Services head-end system. (The World Wide Web and Networked Energy Services Local Task Manager services).

Configuring the Event Receiver Namespace

To configure the event receiver namespace:

1. In the NES Diagnostic Tool navigation tree, navigate to **NES System Data, Settings, Solution Settings.**

2. Select **Event Receiver Namespace.**
3. Set the VALUE property to **http://tempuri.org.** This is the namespace for the Networked Energy Services Adapter web service that will receive the events.

Configuring the API Key Timeout Period

> **Note:** This task is optional. By default the API Key Timeout Period is set to 60 minutes.

To configure the API Key Timeout Period:

1. In the NES Diagnostic Tool navigation tree, navigate to NES System Data, Settings, Solution Settings.
2. In the tree, select the API Key Timeout Period to view its properties.
3. Change the VALUE property to set the timeout period for the API key.

Restart the application server that hosts the Networked Energy Services head-end system.

Configuring Security for the SOA System

Security is managed through policies attached to the input and output points of each composite. More information on policies and their configuration can be found in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*, Chapter 10: Configuring Policies.

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework
- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server.
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click on the domain, and choose **Security, Credentials**.
2. On the **Credentials** page, click **Create Map.**
3. In the **Create Map** dialog, name the map **oracle.wsm.security**, then click **OK**.
4. Click **Create Key** and enter the following values:
   - **Select Map:** oracle.wsm.security
   - **Key:** sgg.d4.credentials

- **Type:** Password
- **Username:** A valid WebLogic user name
- **Password:** A valid WebLogic password

5. Click **OK.**
6. Click **Create Key** again and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.d4.ouaf.credentials
    - **Type:** Password
    - **Username:** A valid OUAF user name
    - **Password:** A valid OUAF password
7. Click **OK.**

Configuring Security for the SOA System to Communicate with the Head-End System

Configuring security for the SOA system involves creating the security credentials in Oracle Enterprise Manager, and then creating a web service policy that uses the credentials to communicate with the head-end system. These configuration tasks are described in the following sections:

- Creating the Security Credentials
- Importing the Policy Templates
- Creating the Web Service Policy for the Security Credentials

Creating the Security Credentials

To create the security credential in the Credential File Store (CFS):

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. Right-click the domain and navigate to **Security, Credentials.**
3. Click **Create Map** to set up a new credentials store.
4. In the **Create Map** dialog box, enter a unique value in the **Map Name** field.

    For example, nes.credentials.
5. Click **OK.**
6. Select the new map in the **Credentials** list and click **Create Key.**

    For example, nes-key.
7. In the **Create Key** dialog box, enter the appropriate values in the fields.
8. In the **Type** field, select **Password.**
9. Click **OK.**

Importing the Policy Templates

To import the policy assertion templates:

1. Import the policy template jar using Enterprise Manager.

a. **For Linux**:

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d1
```

For **Windows:**

```
cd %SPLEBASE%/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile  package-soa-
policy.xml -Dproduct=d1
```

b. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

c. Right-click the domain and navigate to **Web Services, WSM Policies.**

d. Click **Web Services Assertion Templates** at the top of the page.

e. Click **Import** and import the sgg-d1-policy.jar zip.

This file is located in the following directory:

UNIX: $SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

2. Import the policy template jar using Enterprise Manager.

a. **Linux**:

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d4
```

Windows

```
cd %SPLEBASE%/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d4
```

b. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

c. Right-click the domain and navigate to **Web Services, WSM Policies.**

d. Click **Web Services Assertion Templates** at the top of the page.

e. Click **Import** and import the sgg-d4-policy.jar zip.

This file is located in the following directory:

UNIX: $SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

Creating the Web Service Policy for the Security Credentials

To create a web service policy for the security credentials:

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. Right-click the domain and navigate to **Web Services, Policies.**
3. In the **Applies To** field, select either **All** or **Service Clients.**

4. Select the policy oracle/wss_http_token_client_policy.
5. Click **Create Like.**
    a. Give the policy a unique name and an appropriate description.
    b. Under **Assertions**, remove the Log Message and the HTTP Security policies.
    c. Click **Add.**
    d. Enter a name for the new assertion.
    e. In the **Assertion Template** field, select sgg/ d1_csf_access_client_xpath_template and click **Save**.
    f. Click **OK.**
6. In the **Assertion Content** field, edit property values in the XML according to the example below. The following table lists the property values that should be edited:

Field	**Default Value**	**Description**
csf-map		Required. The credential store map to use. This value is specified in the task **Creating the Security Credentials** on page 7-35.
csf-key		Required. The key in the credential store map that will resolve to a username-password pair. This value is specified in the task **Creating the Security Credentials** on page 7-35.
namespaceDefinitions		Prefix-namespace definitions used in the xpath fields below. Each should be in the form prefix=namespace. Multiple definitions should be separated by spaces. Default namespaces cannot be set.
soapElement	Body	The context node for xpath searches, either the SOAP header or the SOAP body. Legal values are "header" and "body."
userid.xpath		The xpath to the location to inject the username in the SOAP element. The statement must resolve to an attribute or element that already exists.
password.xpath		The xpath to the location to inject the password in the SOAP element. The statement must resolve to an attribute or element that already exists.
isDebuggingActive	false	Reserved for internal use.

```
<orasp:SGGCredentialStoreInsertionXPath xmlns:orawsp="http://
schemas.oracle.com/ws/2006/01/policy" orawsp:Silent="true"
orawsp:name="CSF_Echelon" orawsp:description="Properties to add CSF
credentials to a SOAP message" orawsp:Enforced="true"
orawsp:category="security/authentication" xmlns:orasp="http://
schemas.oracle.com/ws/2006/01/securitypolicy">
    <orawsp:bindings>

<orawsp:Implementation>com.splwg.d1.sgg.soa.common.security.policy.Cre
dentialStorageFacilityAccessAssertationExecutor</
orawsp:Implementation>
        <orawsp:Config orawsp:name="CSFKeyInsertionConfig"
orawsp:configType="declarative">
            <orawsp:PropertySet orawsp:name="CSFKeyProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-map">
                    <orawsp:Description>Which CSF map to use</
orawsp:Description>
                    <orawsp:Value>CSF_map_name</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-key">
                    <orawsp:Description>Which key in the map to use</
orawsp:Description>
                    <orawsp:Value>CSF_Key</orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="XPathProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="soapElement">
                  <orawsp:Description>The segment of the soap message
to which to write.  Legal Values are "header" &amp; "body"</
orawsp:Description>
                    <orawsp:Value>body</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="optional" orawsp:name="namespaceDefinitions">
                    <orawsp:Description>A space-separated list of
prefix-namespace pairs.  For example: ns1=http://myurl.com/ns1
ns2=http://oracle.com xsd=http://www.w3.org/2001/XMLSchema</
orawsp:Description>
                    <orawsp:Value/>    <!-- NOTE: nothing entered in
this space -->
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="userid.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the user id.</
orawsp:Description>
                    <orawsp:Value>./sUserLogin</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="password.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the password.</
orawsp:Description>
                    <orawsp:Value>./sPassword</orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="DebugProperties">
                <orawsp:Property orawsp:type="boolean"
orawsp:contentType="optional" orawsp:name="isDebuggingActive">
```

```
                    <orawsp:Description>controls debugging output</
orawsp:Description>
                    <orawsp:Value>false</orawsp:Value>
                    <orawsp:DefaultValue>false</orawsp:DefaultValue>
                </orawsp:Property>
            </orawsp:PropertySet>
        </orawsp:Config>
    </orawsp:bindings>
</orasp:SGGCredentialStoreInsertionXPath>
```

7. Save the policy.
8. Attach the policy to the User Manger reference.
    a. In Oracle Enterprise Manager, Navigate to the **AuthenticationMgr** composite. The full path is **SOA/soa-infra/Echelon/AuthenticationMgr.**
    b. On the **Policies** tab, from the **Attach To/Detach From** menu, select **UserManager**.
    c. In the **Available Policies** window, select the policy that you just created.
    d. Click **Attach** to attach the policy to the UserManager reference.

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) document on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

Note: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Configuration Tasks for the Adapter for Itron OpenWay

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay, including:

- Deploying the OSB Adapter for the Itron OpenWay
- Deploying the SOA Adapter for the Itron OpenWay
- Configuring Security for the SOA System
- Starting the Application

Note: Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for the Itron OpenWay

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance. To deploy the OSB adapter, use the following procedures:

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>:

```
itronxml
itronxml-arch
itronxml-error
itronexcpetion
itronexception-arch
itronexception-error
```

2. Start the example OSB WebLogic instance.

   UNIX

```
cd $SPLEBASE/osbapp
./startWebLogic.sh
```

   Windows

```
cd %SPLEBASE%\osbapp  startWebLogic.cmd
```

3. Create JMS queues and target them to the OSB admin server.
   a. Create a JMS server “OSB-JMSServer” and target it to admin server.
   b. Create a JMS module “D8-SystemModule”.
   c. Under “D8-SystemModule” create a sub-deployment “D8-JMSFAServer” and target it to “OSB-JMSServer”.
4. Create the following JMS queues.

   Queue Name: DestinationQueue-D8

   JNDI Name: DestinationQueue-D8

   Sub-deployment: D8-JMSFAServer

   Targets: OSB-JMSServer

   Queue Name: IMDDestinationQueue-D8

   JNDI Name: IMDDestinationQueue-D8

   Sub-deployment: D8-JMSFAServer

   Targets: OSB-JMSServer

   Queue Name: NotificationQueue-D8

JNDI Name: NotificationQueue-D8

Sub-deployment: D8-JMSFAServer

Targets: OSB-JMSServer

5. Deploy the OSB adapter on the example WebLogic instance.
For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy- osb_D8.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D8.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D8.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version.

```
cd %SPLEBASE%\osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D8.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D8-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D8" and accept the default targets.

3. Under the Foreign Server, navigate to the **General** tab and configure the following:

   a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory

   b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)

   c. JNDI Properties Credential: Credentials for user with access to OSB server

   d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential

   e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>

4. Under **Destinations**, create the following foreign destinations:

   - Name: DestinationQueue-D8
     Local JNDI Name: ForegnDestinationQueue-D8
     Remote JNDI Name: DestinationQueue-D8

   - Name: IMDDestinationQueue-D8
     Local JNDI Name: ForegnIMDDestinationQueue-D8
     Remote JNDI Name: IMDDestinationQueue-D8

   - Name: NotificationQueue-D8
     Local JNDI Name: ForegnNotificationQueue-D8
     Remote JNDI Name: NotificationQueue-D8

5. Under **Connection Factories**, create the following foreign connection factories:

   - Name: DestinationQueueConnectionFactory-D8
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: IMDDestinationQueueConnectionFactory-D8
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: NotificationQueueConnectionFactory-D8
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

1. Create the following directories under <OSB_LOG_DIR>.

```
itronxml
itronxml-arch
itronxml-error
itronexception
itronexception-arch
itronexception-error
```

2. Copy the following jars to the lib folder under the WebLogic's domain directory.

```
spl-d1-osb-2.4.0.0.0.jar
```

   This jar is present under the following location:

   UNIX: $SPLEBASE/etc/lib

Windows: %SPLEBASE%\etc\lib

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server.
    a. Create a JMS server "OSB-JMSServer" and target it to admin server. Create a JMS module "D8-SystemModule".
    b. Under "D8-SystemModule" create a sub-deployment "D8-JMSFAServer" and target it to "OSB-JMSServer"
    c. Create the following JMS queues.

    Queue Name: DestinationQueue-D8

    JNDI Name: DestinationQueue-D8

    Sub-deployment: D8-JMSFAServer

    Targets: OSB-JMSServer

    Queue Name: IMDDestinationQueue-D8

    JNDI Name: IMDDestinationQueue-D8

    Sub-deployment: D8-JMSFAServer

    Targets: OSB-JMSServer

    Queue Name: NotificationQueue-D8

    JNDI Name: NotificationQueue-D8

    Sub-deployment: D8-JMSFAServer

    Targets: OSB-JMSServer
5. Deploy the OSB adapter on the separate WebLogic instance.
For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

    Note: Modify the OSB Host Server,OSB Port Number according to Standalone domain using "OSB Configuration Menu item 8".

UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D8.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D8.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D8.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D8.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D8-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D8" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
   a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
   b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
   c. JNDI Properties Credential: Credentials for user with access to OSB server
   d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
   e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
   - Name: DestinationQueue-D8
     Local JNDI Name: ForegnDestinationQueue-D8
     Remote JNDI Name: DestinationQueue-D8
   - Name: IMDDestinationQueue-D8
     Local JNDI Name: ForegnIMDDestinationQueue-D8
     Remote JNDI Name: IMDDestinationQueue-D8
   - Name: NotificationQueue-D8
     Local JNDI Name: ForegnNotificationQueue-D8
     Remote JNDI Name: NotificationQueue-D8

5. Under **Connection Factories**, create the following foreign connection factories:

   - Name: DestinationQueueConnectionFactory-D8
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D8
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D8
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D8
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for the Itron OpenWay

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at below locations for JAVA_OPTIONS.

   UNIX

   cd $SPLEBASE/soaapp

   ./startWebLogic.sh

   Windows

   cd %SPLEBASE%\soaapp startWebLogic.cmd

2. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/ SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS

3. Start the example SOA WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

4. Create JMS queues and target them to the SOA admin server.

   a. Create the "SGGJMSServer" JMS server and target it to the SOA server.

   b. Create an "SGGJMSModule" JMS module.

   c. Under "SGGJMSModule" create a sub-deployment "SGGSubDeployment" and target it to "SGGJMSServer".

5. Create a Connection Factory “D8-TestHarnessConnectionFactory” with the JNDI name “sgg/jms/D8-TestHarnessConnFactory”.

6. Create the following JMS queue.

   Queue Name: D8-TestHarnessAsyncOpQueue

   JNDI Name: sgg/jms/D8-TestHarnessAsyncOpQueue

   Sub-deployment: SGGSubDeployment

   Targets: SGGJMSServer

7. Deploy the SOA adapter on the example WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/soaapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D8.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

8. Deploy the TestHarness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   > **Note:** Open the command prompt as Administrative mode and then select the environment to deploy SOA.

   ```
   cd %SPLEBASE%/soaapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_D8.xml deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Create WebLogic SOA Domain and select Enterprise Manager option also.
2. Copy the following jar file to the lib folder under the WebLogic domain directory, spl-d1-soa- security.jar.

   This jar is present under the following location.

   UNIX

   ```
    $SPLEBASE/etc/lib
   ```

   Windows

   ```
   %SPLEBASE%\etc\lib
   ```

3. Add system permissions for Smart Grid Gateway security policies.
   1. Log on to Oracle Enterprise Manager as an administrative user.
   2. Select **WebLogic Domain**, then **Security**, then **System Policies**.

      The **System Policies** page opens.
   3. Search for an existing permission for the Smart Grid Gateway security jar as follows:
      1. Select "Codebase" from the **Type** drop-down list (you should not have to change this).
      2. Select "Includes" from the **Name** drop-down list.
      3. Enter "spl-d1-soa-security.jar" into the search field.
      4. Click the arrow button.
      5. No policies should be found:
   4. Click **Create**.

      The **Create System Grant** page opens.
   5. Select "Codebase" from the **Grant To** drop-down list.
   6. Enter the complete path to the security jar in the **Codebase** field as follows:

      ```
      "file:${domain.home}/lib/spl-d1-soa-security.jar"
      ```

   7. Click **Add** (under **Permissions**).

      The **Add Permission** window opens.
   8. Select the "**Select here to enter details for a new permission** checkbox.

      The following fields appear:
      - Permission Class
      - Resource Name
      - Permission Actions

i. Enter the following details into the three fields:

Field	Value
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission
Resource Name	context=SYSTEM,mapName=*,keyName=*
Permission Actions	*

j. Click **OK** to close the **Add Permission** window.

k. Click **OK** (on the **Create System Grant** page) to save the system grant.

l. Repeat the search from step 2 to confirm the new system policy exists:

This search should return the system policy you just added.

4. Copy the SGGLogin.config file from below location to the config directory of WebLogic SOA domain and edit the startWeblogic script located of WebLogic SOA domain-> bin for JAVA_OPTIONS.

   This SGGLogin.config is present under the following location.

   UNIX: $SPLEBASE/soaapp/config

   Windows: %SOA_HOME%\soaapp\config

   a. Copy the file.

   Unix :<Weblogic_SOA_domain>/config

   Windows: <Weblogic_SOA_domain>\config

   b. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/ SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS to:

   Unix: <Weblogic_SOA_domain>/bin/startWeblogic.sh

   Windows:<Weblogic_SOA_domain>\bin\startWeblogic.cmd

5. Start the separate SOA WebLogic instance.

   a. Create JMS queues and target them to the SOA admin server.

   b. Create a JMS server "SGGJMSServer" and target it to the SOA server.

   c. Create a JMS module "SGGJMSModule".

   d. Under "SGGJMSModule" create a sub-deployment "SGGSubDeployment" and target it to "SGGJMSServer".

6. Create a Connection Factory "D8-TestHarnessConnectionFactory" with JNDI name "sgg/jms/D8-TestHarnessConnFactory".

7. Create the following JMS queue.

   Queue Name: D8-TestHarnessAsyncOpQueue

   JNDI Name: sgg/jms/D8-TestHarnessAsyncOpQueue

   Sub-deployment: SGGSubDeployment

   Targets: SGGJMSServer

8. Deploy the SOA cartridge on the separate WebLogic instance.

   > **Note:** Modify the SOA Host Server, SOA Port Number, SOA WebLogic User Name, SOA WebLogic User Password and Endpoint URLs menu items according to separate domain using "SOA Configuration Menu item 9".

   The steps to deploy SSL are described in the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant
   -buildfile deploy-soa_D8.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties
   ```

9. Deploy the TestHarness SOA composites on the separate WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
   deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D8.xml
   deployTestHarness -Dserver.user=<ADMIN_USER>
   -Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
   ```

Configuring Security for the SOA System

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework
- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click the domain, and choose **Security**, **Credentials**.
2. On the **Credentials** page click **Create Map**.
3. In the **Create Map** dialog, name the map **oracle.wsm.security** and click **OK**.
4. Click **Create Key** and enter the following values:
    - **Select Map**: oracle.wsm.security
    - **Key**: sgg.d8.credentials
    - **Type**: Password
    - **Username**: A valid WebLogic user name
    - **Password**: A valid WebLogic password
5. Click **OK**.
6. Click **Create Key** again and enter the following values:
    - **Select Map**: oracle.wsm.security
    - **Key**: sgg.d8.ouaf.credentials
    - **Type:** Password
    - **Username**: A valid OUAF user name
    - **Password**: A valid OUAF password
7. Click **OK**.

Configuring Security for the SOA System to Communicate with the Head-End System

According to the Itron OpenWay Web Service Reference Guide, the head end system can accommodate many different types of security schemes including Basic HTTP, HTTPS, and X.509. Oracle SOA Server supports these, as well. By default, Basic HTTP is enabled, but as always users should evaluate the most appropriate type of security for their environment. Please refer to the Oracle SOA Server product documentation for detailed instructions on securing web services.

Importing the Policy Templates and Policies.

Follow the procedure below to import the policy templates and policies:

1. Import the policy template jar using Enterprise Manager.

   a. For **Linux**:

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfileant package-soa-
   policy.xml -Dproduct=d1
   ```

   For **Windows**

   ```
   cd %SPLEBASE%/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d1
   ```

   b. In Oracle Enterprise Manager, navigate to WebLogic Domain and select the required SOA domain.

   c. Right-click the domain and navigate to **Web Services**, **WSM Policies**.

   d. Click **Web Services Assertion Templates** at the top of the page.

   e. Click **Import** and import the sgg-d1-policy.jar zip.

   This file is located in the following directory:

   UNIX: $SPLEBASE/soaapp/policies/jars

   Windows: %SPLEBASE%\soaapp\policies\jars

2. Import the policy template jar using Enterprise Manager.

   a. For **Linux**

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d8
   ```

   For **Windows**

   ```
   cd %SPLEBASE%/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d8
   ```

   b. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

   c. Right-click the domain and navigate to **Web Services**, **WSM Policies**.

   d. Click **Import** and import the sgg-d8-policy.jar zip.

   This file is located in the following directory:

   UNIX: $SPLEBASE/soaapp/policies/jars

   Windows: %SPLEBASE%\soaapp\policies\jars

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) document on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Configuration Tasks for the Adapter for Landis+Gyr

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway Adapter for Landis+Gyr, including:

- Deploying the OSB Adapter for Landis+Gyr
- Deploying the SOA Adapter for Landis+Gyr
- Configuring Security for the SOA System
- Starting the Application

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for Landis+Gyr

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance. To deploy the OSB adapter, use the following procedures:

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>:

```
lg-cim-event
lg-cim-event-arch
lg-cim-event-error
lg-event
lg-event-arch
lg-event-error
lg-usage
```

```
lg-usage-arch
lg-usage-error
```

2. Start the example OSB WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/osbapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\osbapp
   startWebLogic.cmd
   ```

3. Create JMS queues and target them to the OSB admin server.

   a. Create a JMS server “OSB-JMSServer” and target it to admin server.

   b. Create a JMS module “D3-SystemModule”.

   c. Under “D3-SystemModule” create a sub-deployment “D3-JMSFAServer” and target it to “OSB-JMSServer”.

   d. Create the following JMS queues.

      Queue Name: DestinationQueue-D3

      JNDI Name: DestinationQueue-D3

      Sub-deployment: D3-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: IMDDestinationQueue-D3

      JNDI Name: IMDDestinationQueue-D3

      Sub-deployment: D3-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: NotificationQueue-D3

      JNDI Name: NotificationQueue-D3

      Sub-deployment: D3-JMSFAServer

      Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/osbapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
   -Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
   Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
   Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
   Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
   Douaf.filter.password=<JMS_PASSWORD>
   ```

   Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
update_osb -Dadmin.user=<ADMIN_USER> --Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy- osb_LG.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “LG-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D3
      Local JNDI Name: ForegnDestinationQueue-D3
      Remote JNDI Name: DestinationQueue-D3

- Name: IMDDestinationQueue-D3
  Local JNDI Name: ForegnIMDDestinationQueue-D3
  Remote JNDI Name: IMDDestinationQueue-D3
- Name: NotificationQueue-D3
  Local JNDI Name: ForegnNotificationQueue-D3
  Remote JNDI Name: NotificationQueue-D3

5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-D3
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D3
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D3
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

1. Create the following directories under <OSB_LOG_DIR>.

```
lg-cim-event
lg-cim-event-arch
lg-cim-event-error
lg-event
lg-event-arch
lg-event-error
lg-usage
lg-usage-arch
lg-usage-error
```

2. Copy the following jars to the lib folder under the WebLogic's domain directory.

```
spl-d1-osb-2.4.0.0.0.jar
```

   This jar is present under the following location:

   UNIX: $SPLEBASE/etc/lib

   Windows: %SPLEBASE%\etc\lib

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server.
   - Create a JMS server “OSB-JMSServer” and target it to admin server.
   - Create a JMS module “D3-SystemModule”.
   - Under “D3-SystemModule” create a sub-deployment “D3-JMSFAServer” and target it to “OSB-JMSServer”.
   - Create the following JMS queues:

     Queue Name: DestinationQueue-D3

JNDI Name: DestinationQueue-D3

Sub-deployment: D3-JMSFAServer

Targets: OSB-JMSServer

Queue Name: IMDDestinationQueue-D3

JNDI Name: IMDDestinationQueue-D3

Sub-deployment:: D3-JMSFAServer

Targets: OSB-JMSServer

Queue Name: NotificationQueue-D3

JNDI Name: NotificationQueue-D3

Sub-deployment: D3-JMSFAServer

Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance.

   For SSL deployment, refer to the Deploying OSB adapter on SSL section.

   UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

   This will not override any OSB custom changes.

   Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_LG.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_LG.xml
update_osb -Dadmin.user=<ADMIN_USER> -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “LG-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
   a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
   b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
   c. JNDI Properties Credential: Credentials for user with access to OSB server
   d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
   e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
   - Name: DestinationQueue-D3
     Local JNDI Name: ForegnDestinationQueue-D3
     Remote JNDI Name: DestinationQueue-D3
   - Name: IMDDestinationQueue-D3
     Local JNDI Name: ForegnIMDDestinationQueue-D3
     Remote JNDI Name: IMDDestinationQueue-D3
   - Name: NotificationQueue-D3
     Local JNDI Name: ForegnNotificationQueue-D3
     Remote JNDI Name: NotificationQueue-D3
5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-D3
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D3
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D3
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D3
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for Landis+Gyr

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To deploy the SOA adapter, follow the procedures below.

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at below locations for JAVA_OPTIONS:

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   startWebLogic.cmd
   ```

   Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS

2. Start the example SOA WebLogic instance:

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

3. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_LG.xml
   ```

```
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>  -
DsysPropFile=soa.properties
```

4. Deploy the TestHarness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   > **Note:** Open the command prompt as Administrative mode and then select the environment to deploy SOA.

   ```
   cd %SPLEBASE%/soaapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_LG.xml deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD>  -DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Create WebLogic SOA Domain and select Enterprise Manager option also.
2. Copy the following jar file to the lib folder under the WebLogic domain directory, spl-d1-soa- security.jar.

   This jar is present under the following location:

   UNIX

   ```
   $SPLEBASE/etc/lib
   ```

   Windows

   ```
   %SPLEBASE%\etc\lib
   Append the following XML snippet to
   <MIDDLEWARE_HOME>\user_projects\domains\<SOA
   Domain>\config\fmwconfig\system-jazn-data.xml:
          <grant>
   <grantee>
   <codesource>
   <url>file:${domain.home}/lib/spl-d1-soa-security.jar</url>
   </codesource>
   </grantee>
   <permissions>
   <permission>
   <class>oracle.security.jps.service.credstore.CredentialAccessPermi
   ssion</class>
   <name>context=SYSTEM,mapName=*,keyName=*</name>
   <actions>*</actions>
   </permission>
   </permissions>
   <permission-set-refs>
   </permission-set-refs>
   ```

```
</grant>
```

3. Copy the SGGLogin.config file from below location to the config directory of Weblogic SOA domain and edit the startWeblogic script located of Weblogic SOA domain-> bin for JAVA_OPTIONS:

   This SGGLogin.config is present under the following location:

   UNIX: $SPLEBASE/soaapp/config

   Windows: %SOA_HOME%\soaapp\config

   a. Copy the file.

      UNIX: <Weblogic_SOA_domain>/config

      Windows: <Weblogic_SOA_domain>\config

   b. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS to

      UNIX: <Weblogic_SOA_domain>/bin/startWeblogic.sh

      Windows: <Weblogic_SOA_domain>\bin\startWeblogic.cmd

4. Start the separate WebLogic instance.
5. Deploy the SOA adapter on the separate WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ```

   For WebLogic 12c:

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   ```

   For WebLogic 12c:

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant
   -buildfile deploy-soa_LG.xml
   -Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
   DsysPropFile=soa.properties
   ```

6. Deploy the TestHarness SOA composites on the separate WebLogic instance.

   For the SSL deployment procedure, refer to the section Deploying SOA Composites on SSL.

   UNIX

   For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
 deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
```

   Windows

```
cd %SPLEBASE%\soaapp
```

   For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_LG.xml
deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD>  -DsysPropFile=soa.properties
```

Configuring Security for the SOA System

Security is managed through policies attached to the input and output points of each composite. More information on policies and their configuration can be found in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*, Chapter 10: Configuring Policies.

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework
- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click the domain, and choose **Security, Credentials**.
2. On the **Credentials** page, click **Create Map.**
3. In the **Create Map** dialog, name the map oracle.wsm.security and click **OK**.

4. Click **Create Key** and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.d3.credentials
    - **Type:** Password
    - **Username:** A valid WebLogic user name
    - **Password:** A valid WebLogic password
5. Click **OK**.
6. Click **Create Key** again and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key: s**gg.d3.ouaf.credentials
    - **Type:** Password
    - **Username:** A valid OUAF user name
    - **Password:** A valid OUAF password
7. Click **OK**.

Configuring Security for the SOA System to Communicate with the Head-End System

Configuring security for the SOA system involves creating the security credentials in Oracle Enterprise Manager, and then creating a web service policy that uses the credentials to communicate with the head-end system. These configuration tasks are described in the following sections:

- Creating the Security Credentials
- Importing the Policy Templates and Policies
- Creating the Web Service Policy for the Security Credentials

Creating the Security Credentials

To create the security credential in the Credential File Store (CFS):

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. In the **WebLogic Domain** menu, navigate to **Security, Credentials**.
3. Click **Create Map** to set up a new credentials store.
4. In the **Create Map** dialog box, enter a unique value in the **Map Name** field.
5. Click **OK.**
6. Select the new map in the Credentials list and click **Create Key**.
7. In the **Create Key** dialog box, enter the appropriate values in the fields.
8. In the **Type** field, select **Password**.
9. Click **OK**.

Importing the Policy Templates and Policies

Follow the procedure below to import policy templates and policies.

1. Import the policy template jar using Enterprise Manager.

   Linux

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d1
   ```

   Windows

   ```
   cd %SPLEBASE%/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d1
   ```

   a. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

   b. Right-click the domain and navigate to **Web Services, WSM Policies**.

   c. Click **Web Services Assertion Templates** at the top of the page.

   d. Click **Import** and import the sgg-d1-policy.jar file.

   This file is located in the following directory:

   UNIX: $SPLEBASE/soaapp/policies/jars

   Windows: %SPLEBASE%\soaapp\policies\jars

2. Import the policy template jar using Enterprise Manager.

   Linux

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d3
   ```

   Windows

   ```
   cd %SPLEBASE%/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
   policy.xml -Dproduct=d3
   ```

   a. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

   b. Right-click the domain and navigate to **Web Services, WSM Policies.**

   c. Click **Web Services Assertion Templates** at the top of the page.

   d. Click **Import** and import the sgg-d3-policy.jar file.

   This file is located in the following directory:

   UNIX: $SPLEBASE/soaapp/policies/jars

   Windows: %SPLEBASE%\soaapp\policies\jars

Creating the Web Service Policy for the Security Credentials

To create a web service policy for the security credentials:

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

2. In the **WebLogic Domain** menu, navigate to **Web Services, Policies**.
3. Select the policy oracle/wss_http_token_client_policy.
4. Click **Create Like.**
    a. Give the policy a unique name and an appropriate description.
    b. Under **Assertions**, remove the Log Message and the HTTP Security policies.
    c. Click **Add.**
    d. Enter a name for the new assertion.
    e. In the Assertion Template field, select sgg/d1_csf_access_client_xpath_template.
    f. Click **OK.**
5. In the **Assertion Content** field, edit property values in the XML according to the example below. The following table lists the property values that should be edited:

Field	Default Value	Description
csf-map		Required. The credential store map to use. This value is specified in the task Creating the Security Credentials.
csf-key		Required. The key in the credential store map that will resolve to a username-password pair. This value is specified in the task Creating the Security Credentials.
namespaceDefinitions		Prefix-namespace definitions used in the xpath fields below. Each should be in the form prefix=namespace. Multiple definitions should be separated by spaces. Default namespaces cannot be set.
soapElement	Header	The context node for xpath searches, either the SOAP header or the SOAP body. Legal values are "header" and "body."
userid.xpath		The xpath to the location to inject the username in the SOAP element. The statement must resolve to an attribute or element that already exists.
password.xpath		The xpath to the location to inject the password in the SOAP element. The statement must resolve to an attribute or element that already exists.
isDebuggingActive	false	Reserved for internal use.

```
<orasp:SGGCredentialStoreInsertionXPath xmlns:orawsp="http://
schemas.oracle.com/ws/2006/01/policy" orawsp:Silent="true"
orawsp:name="CSF_CIM_L+G" orawsp:description="Properties to add CSF
credentials to a SOAP message" orawsp:Enforced="true"
orawsp:category="security/authentication" xmlns:orasp="http://
schemas.oracle.com/ws/2006/01/securitypolicy">
    <orawsp:bindings>
```

```
<orawsp:Implementation>com.splwg.d1.sgg.soa.common.security.policy.Cre
dentialStorageFacilityAccessAssertionExecutor</
orawsp:Implementation>
        <orawsp:Config orawsp:name="CSFKeyInsertionConfig"
orawsp:configType="declarative">
            <orawsp:PropertySet orawsp:name="CSFKeyProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-map">
                    <orawsp:Description>Which CSF map to use</
orawsp:Description>
                    <orawsp:Value>CSF_map_name</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="csf-key">
                    <orawsp:Description>Which key in the map to use</
orawsp:Description>
                    <orawsp:Value>CSF_CIM_Key</orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="XPathProperties">
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="soapElement">
                  <orawsp:Description>The segment of the soap message
to which to write. Legal Values are "header" &amp; "body"</
orawsp:Description>
                    <orawsp:Value>header</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="optional" orawsp:name="namespaceDefinitions">
                    <orawsp:Description>A space-separated list of
prefix-namespace pairs. For example: ns1=http://myurl.com/ns1
ns2=http://oracle.com xsd=http://www.w3.org/2001/XMLSchema</
orawsp:Description>
                  <orawsp:Value>ns1=http://www.landisgyr.com/iec61968/
2010/03</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="userid.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the user id.</
orawsp:Description>
                    <orawsp:Value>./UserName</orawsp:Value>
                </orawsp:Property>
                <orawsp:Property orawsp:type="string"
orawsp:contentType="required" orawsp:name="password.xpath">
                    <orawsp:Description>The xpath relative to the
soapElement property at which to insert the password.</
orawsp:Description>
                    <orawsp:Value>./Password</orawsp:Value>
                </orawsp:Property>
            </orawsp:PropertySet>
            <orawsp:PropertySet orawsp:name="DebugProperties">
                <orawsp:Property orawsp:type="boolean"
orawsp:contentType="optional" orawsp:name="isDebuggingActive">
                    <orawsp:Description>controls debugging output</
orawsp:Description>
                    <orawsp:Value>false</orawsp:Value>
                    <orawsp:DefaultValue>false</orawsp:DefaultValue>
                </orawsp:Property>
            </orawsp:PropertySet>
        </orawsp:Config>
```

```
    </orawsp:bindings>
</orasp:SGGCredentialStoreInsertionXPath>
```

6. Save the policy.
7. Attach the policy to the MR_CB reference on the CommissionDecommission composite.
    a. In Oracle Enterprise Manager, navigate to the **CommissionDecommission** composite.
    b. From the **Attach To/Detach From** menu, select **MR_CB.**
    c. In the **Available Policies** window, select the policy that you just created.
    d. Click **Attach** to attach the policy to the MR_CB reference.
8. Attach the policy to the CD_CB reference on the ConnectDisconnect composite
    a. Navigate to the **ConnectDisconnect** composite.
    b. From the **Attach To/Detach From** menu, select **CD_CB**.
    c. In the **Available Policies** window, select the policy that you just created.
    d. Click **Attach** to attach the policy to the CD_CB reference.
9. Attach the policy to the MR_CB reference on the OnDemandRead composite.
    a. Navigate to the **OnDemandRead** composite.
    b. From the **Attach To/Detach From** menu, select **MR_CB.**
    c. In the **Available Policies** window, select the policy that you just created.
    d. Click **Attach** to attach the policy to the MR_CB reference.

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) document on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Configuration Tasks for the Adapter for Sensus RNI

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway, including:

- Deploying the OSB Adapter for Sensus RNI
- Deploying the SOA Adapter for Sensus RNI
- Configuring Security for the SOA System
- Starting the Application

Note: Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for Sensus RNI

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance. To deploy the OSB adapter, use the following procedures.

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>:

```
d6-usage
d6-usage-arch
d6-usage-error
d6-event
d6-event-arch
d6-event-error
```

2. Start the example OSB WebLogic instance.

UNIX

```
cd $SPLEBASE/osbapp
./startWebLogic.sh
```

Windows

```
cd %SPLEBASE%\osbapp
startWebLogic.cmd
```

3. Create JMS queues and target them to the OSB admin server.

   a. Create a JMS server “OSB-JMSServer” and target it to admin server.

   b. Create a JMS module “D6-SystemModule”.

   c. Under “D6-SystemModule” create a sub-deployment “D6-JMSFAServer” and target it to “OSB-JMSServer”.

   d. Create the following JMS queues.

   Queue Name: DestinationQueue-D6

   JNDI Name: DestinationQueue-D6

   Sub-deployment: D6-JMSFAServer

Targets: OSB-JMSServer

Queue Name: IMDDestinationQueue-D6

JNDI Name: IMDDestinationQueue-D6

Sub-deployment: D6-JMSFAServer

Targets: OSB-JMSServer

Queue Name: NotificationQueue-D6

JNDI Name: NotificationQueue-D6

Sub-deployment: D6-JMSFAServer

Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.
   For SSL deployment, please refer to the Deploying OSB Adapter on SSL section.

   UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D6.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D6.xml
update_osb -Dadmin.user=<ADMIN_USER>
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   This will not override any OSB custom changes.

   Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D6.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D6.xml
update_osb -Dadmin.user=<ADMIN_USER>
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
```

```
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D6-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D6
      Local JNDI Name: ForegnDestinationQueue-D6
      Remote JNDI Name: DestinationQueue-D6
    - Name: IMDDestinationQueue-D6
      Local JNDI Name: ForegnIMDDestinationQueue-D6
      Remote JNDI Name: IMDDestinationQueue-D6
    - Name: NotificationQueue-D6
      Local JNDI Name: ForegnNotificationQueue-D6
      Remote JNDI Name: NotificationQueue-D6
5. Under **Connection Factories**, create the following foreign connection factories:
    - Name: DestinationQueueConnectionFactory-D6
      Local JNDI Name: ForegnDestinationQueueConnectionFactory-D6
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: IMDDestinationQueueConnectionFactory-D6
      Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D6
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: NotificationQueueConnectionFactory-D6
      Local JNDI Name: ForegnNotificationQueueConnectionFactory-D6
      Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Note: Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

1. Create the following directories under <OSB_LOG_DIR>.

   ```
   d6-usage
   d6-usage-arch
   d6-usage-error
   d6-event
   d6-event-arch
   d6-event-error
   ```

2. Copy the following jars to the lib folder under the WebLogic's domain directory.

   ```
   spl-d1-osb-2.4.0.0.0.jar
   ```

   This jar is present under the following location:

   UNIX: $SPLEBASE/etc/lib

   Windows: %SPLEBASE%\etc\lib

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server.
   a. Create a JMS server “OSB-JMSServer” and target it to admin server.
   b. Create a JMS module “D6-SystemModule”.
   c. Under “D6-SystemModule” create a sub-deployment “D6-JMSFAServer” and target it to “OSB-JMSServer”.
   d. Create the following JMS queues:

      Queue Name: DestinationQueue-D6

      JNDI Name: DestinationQueue-D6

      Sub-deployment: D6-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: IMDDestinationQueue-D6

      JNDI Name: IMDDestinationQueue-D6

      Sub-deployment: D6-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: NotificationQueue-D6

      JNDI Name: NotificationQueue-D6

      Sub-deployment: D6-JMSFAServer

      Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance.
   For SSL deployment, please refer to the section Deploying OSB adapter on SSL.

   UNIX

   ```
   cd $SPLEBASE/osbapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D6.xml
   ```

```
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D6.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D6.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D6.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D6-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential

e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>

4. Under **Destinations**, create the following foreign destinations:

   - Name: DestinationQueue-D6
     Local JNDI Name: ForegnDestinationQueue-D6
     Remote JNDI Name: DestinationQueue-D6

   - Name: IMDDestinationQueue-D6
     Local JNDI Name: ForegnIMDDestinationQueue-D6
     Remote JNDI Name: IMDDestinationQueue-D6

   - Name: NotificationQueue-D6
     Local JNDI Name: ForegnNotificationQueue-D6
     Remote JNDI Name: NotificationQueue-D6

5. Under **Connection Factories**, create the following foreign connection factories:

   - Name: DestinationQueueConnectionFactory-D6
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D6
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: IMDDestinationQueueConnectionFactory-D6
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D6
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

   - Name: NotificationQueueConnectionFactory-D6
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D6
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for Sensus RNI

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To deploy the SOA adapter, follow the procedures below.

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at below locations for JAVA_OPTIONS:

   UNIX

   ```
   $SPLEBASE/soaapp/bin/startWebLogic.sh
   ```

   Windows

   ```
   %SPLEBASE%\soaapp\bin\startWebLogic.cmd
   ```

   Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/SGGLogin.config

   -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS

2. Start the example SOA WebLogic instance:

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   startWebLogic.cmd
   ```

3. Import the Policy Templates and Policies.

   a. Import the policy template jar using Enterprise Manager.

      Linux

      ```
      cd $SPLEBASE/soaapp
      -DsysPropFile=soa.properties package-soa-policy.xml -
      Dproduct=d1
      ```

      Windows

      ```
      cd %SPLEBASE%/soaapp
      -DsysPropFile=soa.properties package-soa-policy.xml -
      Dproduct=d1
      ```

      In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

      a. Right-click on the domain and navigate to **Web Services, WSM Policies**.

      b. Click **Web Services Assertion Templates** at the top of the page.

      c. Click **Import** and import the sgg-d1-policy.jar file.

      This file is located in the following directory:

      UNIX: $SPLEBASE/soaapp/policies/jars

      Windows: %SPLEBASE%\soaapp\policies\jars

   b. Next, import the policy template jar using Enterprise Manager.

      Linux

      ```
      cd $SPLEBASE/soaapp
      -DsysPropFile=soa.properties package-soa-policy.xml -
      Dproduct=d6
      ```

      Windows

      ```
      cd %SPLEBASE%/soaapp
      -DsysPropFile=soa.properties package-soa-policy.xml -
      Dproduct=d6
      ```

      In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

      a. Right click on the domain and navigate to **Web Services, WSM Policies**.

      b. Click **Web Services Assertion Templates** at the top of the page.

      c. Click **Import** and import the sgg-d6-policy.jar zip.

This file is located in the following directory.

UNIX: $SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

4. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D6.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

5. Deploy the Test Harness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   Note: Open the command prompt as Administrative mode and then select the environment to deploy soa

   ```
   cd %SPLEBASE%/soaapp
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_D6.xml deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Create WebLogic SOA Domain and select Enterprise Manager option.

2. Copy the following jar file to the lib folder under the WebLogic domain directory, spl-d1-soa- security.jar.

   This jar is present under the following location:

   UNIX: $SPLEBASE/etc/lib

   Windows: %SPLEBASE%\etc\lib

3. Add system permissions for Smart Grid Gateway security policies as follows.

   a. Log on to Oracle Enterprise Manager as an administrative user.

   b. Select **WebLogic Domain**, then **Security**, then **System Policies**.

      The **System Policies** page opens.

   c. Search for an existing permission for the Smart Grid Gateway security jar as follows:

      d. Select "Codebase" from the **Type** drop-down list (you should not have to change this).

      e. Select "Includes" from the **Name** drop-down list.

      f. Enter "spl-d1-soa-security.jar" into the search field.

      g. Click the arrow button.

      h. No policies should be found:

   d. Click **Create**.

      The **Create System Grant** page opens.

   e. Select "Codebase" from the **Grant To** drop-down list.

   f. Enter the complete path to the security jar in the **Codebase** field as follows:

      ```
      "file:${domain.home}/lib/spl-d1-soa-security.jar"
      ```

   g. Click **Add** (under **Permissions**).

      The **Add Permission** window opens.

   h. Select the "**Select here to enter details for a new permission** checkbox.

      The following fields appear:

      - Permission Class
      - Resource Name
      - Permission Actions

   i. Enter the following details into the three fields:

Field	**Value**
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission
Resource Name	context=SYSTEM,mapName=*,keyName=*
Permission Actions	*

   j. Click OK to close the **Add Permission** window.

   k. Click **OK** (on the **Create System Grant** page) to save the system grant.

l. Repeat the search from step 2 to confirm the new system policy exists:

   This search should return the system policy you just added.

4. Copy the SGGLogin.config file from below location to the config directory of Weblogic SOA domain and edit the startWeblogic script located of Weblogic SOA domain-> bin for JAVA_OPTIONS.

   a. This SGGLogin.config is present under the following location:

      UNIX: $SPLEBASE/soaapp/config

      Windows: %SOA_HOME%\soaapp\config

   b. Copy the file.

      Unix :<Weblogic_SOA_domain>/config

      Windows :<Weblogic_SOA_domain>\config

   c. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/
      SGGLogin.config
      -Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS to

      Unix :<Weblogic_SOA_domain>/bin/startWeblogic.sh

      Windows :<Weblogic_SOA_domain>\bin\startWeblogic.cmd

5. Start the separate WebLogic instance.

6. Before SOA composites deployment, import the Policy Templates and Policies.

   a. First, import the policy template jar using Enterprise Manager.

      Linux

      ```
      cd $SPLEBASE/soaapp
      $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
      policy.xml -Dproduct=d1
      ```

      Windows

      ```
      cd %SPLEBASE%/soaapp
      $SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
      policy.xml -Dproduct=d1
      ```

      i. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

      ii. Right-click the domain and navigate to **Web Services > WSM Policies.**

      iii. Click **Web Services Assertion Templates** at the top of the page.

      iv. Click **Import From File** and import the **sgg-d1-policy.jar** zip.

         This file is located in the following directory:

         UNIX: $SPLEBASE/soaapp/policies/jars

         Windows: %SPLEBASE%\soaapp\policies\jars

   b. First, import the policy template jar using Enterprise Manager.
      Linux

      ```
      cd $SPLEBASE/soaapp
      ```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d6
```

Windows

```
cd %SPLEBASE%/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d6
```

a. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

b. Right-click the domain and navigate to **Web Services, WSM Policies.**

c. Click on **Web Services Assertion Templates** at the top of the page.

d. Click on **Import From File** and import the sgg-d6-policy.jar file.

This file is located in the following directory:

UNIX: $SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

7. Deploy the SOA cartridge on the separate WebLogic instance.

Note: Modify the SOA Host Server, SOA Port Number, SOA WebLogic User Name, SOA WebLogic User Password and Endpoint URLs menu items according to separate domain using "SOA Configuration Menu item 9".

UNIX

```
cd $SPLEBASE/soaapp
```

For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties
```

Windows

```
cd %SPLEBASE%\soaapp
```

For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
 -soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties

%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D6.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD> -
DsysPropFile=soa.properties
```

8. Deploy the Test Harness SOA composites on the separate WebLogic instance.

UNIX

```
cd $SPLEBASE/soaapp
```

For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
```

Windows

```
cd %SPLEBASE%\soaapp
```

For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D6.xml
 deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
```

Configuring Security for the SOA System

Security is managed through policies attached to the input and output points of each composite. More information on policies and their configuration can be found in the **Configuring Policies** chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite.*

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework
- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click the domain, and select **Security** > **Credentials**.
2. On the **Credentials** page, click **Create Map.**
3. In the **Create Map** dialog, name the map **oracle.wsm.security**, then click **OK.**
4. Click **Create Key** and enter the following values**:**
   - **Select Map:** oracle.wsm.security
   - **Key:** sgg.d6.credentials
   - **Type:** Password

- **Username:** A valid WebLogic user name with acces to the SOA Suite server
- **Password:** A valid WebLogic password

5. Click **OK.**
6. Click **Create Key** again and enter the following values:
   - **Select Map:** oracle.wsm.security
   - **Key:** sgg.d6.ouaf.credentials
   - **Type:** Password
   - **Username:** A valid OUAF user name
   - **Password:** A valid OUAF password
7. Click **OK.**

Configuring Security for the SOA System to Communicate with the Head-End System

Configuring security for the SOA system involves creating the security credentials in Oracle Enterprise Manager, and then creating a web service policy that uses the credentials to communicate with the head-end system. These configuration tasks are described in the following sections:

- Creating the Security Credentials

Creating the Security Credentials

To create the security credential in the Credential File Store (CFS):

1. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
2. In the WebLogic Domain menu, navigate to **Security > Credentials.**
3. Click **Create Map** to set up a new credentials store.
4. In the **Create Map** dialog box, enter “rni.security” in the **Map Name** field.
5. Click **OK.**
6. Select the new map in the **Credentials** list and click **Create Key.**
7. In the **Create Key** dialog box, enter the appropriate values in the fields. In the **Key** field, enter “rni.credentials”. In the **Type** field, select **Password.**
8. Click **OK.**

   By default, the sgg_d6_cfs_multispeak_header_client_policy policy imported previously uses a Credential Map named "rni.security" and a Credential Key called “rni.credentials." Use these values unless making changes to the template values.

   Test Harness Note: The test harness is equipped with service policies that authenticate users with credentials in the MultiSpeakMsgHeader. That means the credentials configured in the map and key above should be valid WebLogic users.

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) white paper on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Configuration Tasks for the Adapter for Silver Spring Networks

This section describes the tasks that should be taken after installing Oracle Utilities Smart Grid Gateway, including:

- Deploying the OSB Adapter for Silver Spring Networks
- Deploying the SOA Adapter for Silver Spring Networks
- Configuring Security for the SOA System
- Starting the Application

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

Deploying the OSB Adapter for Silver Spring Networks

The OSB adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance. To deploy the OSB adapter, use the following procedures:

To Deploy on the Example WebLogic Instance

1. Create the following directories under <OSB_LOG_DIR>.

```
d7-csv
d7-csv-arch
d7-csv-error
d7-ssnxml
```

```
d7-ssnxml-arch
d7-ssnxml-error
```

2. Start the example OSB WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/osbapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\osbapp
   startWebLogic.cmd
   ```

3. Create JMS queues and target them to the OSB admin server.

   a. Create a JMS server OSB-JMSServer” and target it to admin server.

   b. Create a JMS module D7-SystemModule.

   c. Under D7-SystemModule create a sub-deployment D7-JMSFAServer and target it to OSB-JMSServer.

   d. Create the following JMS queues.

      Queue Name: DestinationQueue-D7

      JNDI Name: DestinationQueue-D7

      Sub-deployment: D7-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: IMDDestinationQueue-D7

      JNDI Name: IMDDestinationQueue-D7

      Sub-deployment: D7-JMSFAServer

      Targets: OSB-JMSServer

      Queue Name: NotificationQueue-D7

      JNDI Name: NotificationQueue-D7

      Sub-deployment: D7-JMSFAServer

      Targets: OSB-JMSServer

4. Deploy the OSB adapter on the example WebLogic instance.
   For SSL deployment, please refer to Deploying OSB Adapter on SSL.

   UNIX

   ```
   cd $SPLEBASE/osbapp

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml
   -Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
   Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
   Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
   Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
   Douaf.filter.password=<JMS_PASSWORD>
   ```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml -
Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D7.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D7-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D7
      Local JNDI Name: ForegnDestinationQueue-D7
      Remote JNDI Name: DestinationQueue-D7

- Name: IMDDestinationQueue-D7
  Local JNDI Name: ForegnIMDDestinationQueue-D7
  Remote JNDI Name: IMDDestinationQueue-D7
- Name: NotificationQueue-D7
  Local JNDI Name: ForegnNotificationQueue-D7
  Remote JNDI Name: NotificationQueue-D7

5. Under **Connection Factories**, create the following foreign connection factories:
   - Name: DestinationQueueConnectionFactory-D7
     Local JNDI Name: ForegnDestinationQueueConnectionFactory-D7
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: IMDDestinationQueueConnectionFactory-D7
     Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D7
     Remote JNDI Name: weblogic.jms.XAConnectionFactory
   - Name: NotificationQueueConnectionFactory-D7
     Local JNDI Name: ForegnNotificationQueueConnectionFactory-D7
     Remote JNDI Name: weblogic.jms.XAConnectionFactory

To Deploy on a Separate WebLogic Instance

Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying OSB components on a separate WebLogic server.

1. Create the following directories under <OSB_LOG_DIR>.

   ```
   d7-csv
   d7-csv-arch
   d7-csv-error
   d7-ssnxml
   d7-ssnxml-arch
   d7-ssnxml-error
   ```

2. Copy the following jars to the lib folder under the WebLogic's domain directory.

   ```
   spl-d1-osb-2.4.0.0.0.jar
   ```

   This jar is present in the following location:

   UNIX: $SPLEBASE/etc/lib

   Windows: %SPLEBASE%\etc\lib

3. Start the separate WebLogic instance.
4. Create JMS queues and target them to the OSB admin server.
   - Create a JMS server OSB-JMSServer” and target it to admin server.
   - Create a JMS module D7-SystemModule.
   - Under D7-SystemModule create a sub-deployment D7-JMSFAServer and target it to OSB-JMSServer.
   - Create the following JMS queues.

     Queue Name: DestinationQueue-D7

     JNDI Name: DestinationQueue-D7

     Sub-deployment: D7-JMSFAServer

Targets: OSB-JMSServer

Queue Name: IMDDestinationQueue-D7

JNDI Name: IMDDestinationQueue-D7

Sub-deployment: D7-JMSFAServer

Targets: OSB-JMSServer

Queue Name: NotificationQueue-D7

JNDI Name: NotificationQueue-D7

Sub-deployment: D7-JMSFAServer

Targets: OSB-JMSServer

5. Deploy the OSB adapter on the separate WebLogic instance.
   For SSL deployment, refer to Deploying OSB Adapter on SSL.

UNIX

```
cd $SPLEBASE/osbapp
```

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml

```
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version.

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-osb_D7.xml
-Dadmin.user=<ADMIN_USER> -Dadmin.password=<OSB_ADMIN_PASSWORD> -
Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD> -
Dprocessing.archive=true  -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version. It will not override any OSB custom changes.

```
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
```

```
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Create the following JMS configuration in the Oracle Utilities Meter Data Management application Admin Server:

1. Create a JMS module “D7-SystemModule” and target it to the Managed Server where the Oracle Utilities Meter Data Management application is running.
2. Under the JMS module, create a new Foreign Server "OSBForeignServer-D3" and accept the default targets.
3. Under the Foreign Server, navigate to the **General** tab and configure the following:
    a. JNDI Initial Context Factory: weblogic.jndi.WLInitialContextFactory
    b. JNDI Connection URL: URL for OSB Sever in the format - t3://<osb hostname>:<osb port number> (Use t3s for SSL)
    c. JNDI Properties Credential: Credentials for user with access to OSB server
    d. Confirm JNDI Properties Credential: Same as JNDI Properties Credential
    e. JNDI Properties: java.naming.security.principal=<User with access to OSB server for which credentials were provided>
4. Under **Destinations**, create the following foreign destinations:
    - Name: DestinationQueue-D7
      Local JNDI Name: ForegnDestinationQueue-D7
      Remote JNDI Name: DestinationQueue-D7
    - Name: IMDDestinationQueue-D7
      Local JNDI Name: ForegnIMDDestinationQueue-D7
      Remote JNDI Name: IMDDestinationQueue-D7
    - Name: NotificationQueue-D7
      Local JNDI Name: ForegnNotificationQueue-D7
      Remote JNDI Name: NotificationQueue-D7
5. Under **Connection Factories**, create the following foreign connection factories:
    - Name: DestinationQueueConnectionFactory-D7
      Local JNDI Name: ForegnDestinationQueueConnectionFactory-D7
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: IMDDestinationQueueConnectionFactory-D7
      Local JNDI Name: ForegnIMDDestinationQueueConnectionFactory-D7
      Remote JNDI Name: weblogic.jms.XAConnectionFactory
    - Name: NotificationQueueConnectionFactory-D7
      Local JNDI Name: ForegnNotificationQueueConnectionFactory-D7
      Remote JNDI Name: weblogic.jms.XAConnectionFactory

Deploying the SOA Adapter for Silver Spring Networks

The SOA adapter can be deployed on the bundled WebLogic example server instance or on a separate WebLogic server instance.

> **Note:** Oracle Enterprise Manager may be required for some of the security setups and for monitoring SOA. If Oracle Enterprise Manager

is required, you need to extend the example SOA WebLogic domain and enable Enterprise Manager using WebLogic's configuration utility.

To deploy the SOA adapter, use the following procedures.

To Deploy on the Example WebLogic Instance

1. Edit the startWeblogic script located at below locations for JAVA_OPTIONS.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp startWebLogic.cmd
   ```

2. Add "-Djava.security.auth.login.config=${DOMAIN_HOME}/config/ SGGLogin.config -
   Djavax.net.ssl.trustStore=<<JAVA_TRUST_STORE_LOCATION>>" to the JAVA_OPTIONS
3. Start the example SOA WebLogic instance.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   ./startWebLogic.sh
   ```

   Windows

   ```
   cd %SPLEBASE%\soaapp
   startWebLogic.cmd
   ```

4. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

   Windows

   ```
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
   -soa_MDF.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties

   %SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D7.xml
   -Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
   DsysPropFile=soa.properties
   ```

5. Deploy the TestHarness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

   ```
   cd $SPLEBASE/soaapp
   $SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
   deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

   Windows

   > **Note:** Open the command prompt as Administrative mode and then select the environment to deploy SOA.

   ```
   cd %SPLEBASE%/soaapp
   %SPLEBASE%\product\apache-ant\bin\ant -buildfile
   deploy-soa_D7.xml deployTestHarness  -Dserver.password=<SOA_USER>
    -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
   ```

To Deploy on a Separate WebLogic Instance

> **Note:** Refer to Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Meter Data Management for more information about deploying SOA components on a separate WebLogic server.

1. Create WebLogic SOA Domain and select Enterprise Manager option also.
2. Copy the following jar file to the lib folder under the WebLogic domain directory, spl-d1-soa-security.jar

   This jar is present in the following location:

   UNIX: $SPLEBASE/etc/lib

   Windows: %SPLEBASE%\etc\lib
3. Add system permissions for Smart Grid Gateway security policies as follows:
   a. Log on to Oracle Enterprise Manager as an administrative user.
   b. Select **WebLogic Domain**, then **Security**, then **System Policies**.

      The **System Policies** page opens.
   c. Search for an existing permission for the Smart Grid Gateway security jar as follows:
      a. Select "Codebase" from the **Type** drop-down list (you should not have to change this).
      b. Select "Includes" from the **Name** drop-down list.
      c. Enter "spl-d1-soa-security.jar" into the search field.
      d. Click the arrow button.
      e. No policies should be found:
   d. Click **Create**.

      The **Create System Grant** page opens.
   e. Select "Codebase" from the **Grant To** drop-down list.

f. Enter the complete path to the security jar in the **Codebase** field as follows:

```
"file:${domain.home}/lib/spl-d1-soa-security.jar"
```

g. Click **Add** (under **Permissions**).

The **Add Permission** window opens.

h. Select the **"Select here to enter details for a new permission** checkbox.

The following fields appear:

- Permission Class
- Resource Name
- Permission Actions

i. Enter the following details into the three fields:

Field	Value
Permission Class	oracle.security.jps.service.credstore.CredentialAccessPermission
Resource Name	context=SYSTEM,mapName=*,keyName=*
Permission Actions	*

j. Click OK to close the **Add Permission** window.

k. Click **OK** (on the **Create System Grant** page) to save the system grant.

l. Repeat the search from step 2 to confirm the new system policy exists:

This search should return the system policy you just added.

4. Copy the SGGLogin.config file from below location to the config directory of Weblogic SOA domain and edit the startWeblogic script located of Weblogic SOA domain > bin for JAVA_OPTIONS.

   This SGGLogin.config is present under the following location:

   UNIX: $SPLEBASE/soaapp/config

   Windows: %SOA_HOME%\soaapp\config

   Copy the file.

   Unix :<Weblogic_SOA_domain>/config

   Windows: <Weblogic_SOA_domain>\config

5. Start the separate WebLogic instance.

6. Create JMS queues and target them to the SOA managed server:

   a. Create a JMS Server:

      a. Under Domain Structure, navigate to **Services** > **Messaging** > **JMS Servers.**

      b. On the **JMS Servers** page, click on **New**.

      c. On the **Create a New JMS Server** page:

      - Provide a name for your JMS Server. For example: SSN-JMSServer
      - Select a Persistent Store to SOAJMSFileStore. Click **Next.**

- On the next screen, select the SOA_Server as Target Server instance where you would like to deploy this JMS Server.
- Select the Target Server from the dropdown list and click **Finish** to complete the JMS server creation. Make sure you activate the changes.
- You should now find your new JMS Server in the JMS Servers List.

b. Create a JMS Module.

a. On the Create JMS System Module page, enter the name. For example: SSN-SystemModule (other fields can remain empty).

b. Select the SOA Server you would like to target (ideally, this would be the same server that is hosting the JMS server you created above).

For example: soa_server1

c. On the next screen, click **Finish and Activate changes**.

c. Create Queues.

a. Click on **New** in JMS Module to create the Queue.

b. Provide a name (for example: SSNTestSSNODRQ) and a JNDI name (for example, queue/SSNTestSSNODRQ).

c. Select a subdeployment (for example: SSN-JMSFAServer) if you already created or follow below steps to create a new subdeployment. (A subdeployment is a convenient way for grouping and targeting JMS module resources.)

d. Provide a name for the subdeployment (for example: SSN-JMSFAServer) and click **OK.**

- Select the target JMS Server we created (for example: SSN-JMSServer) and click **finish**.
- Click **New** in JMS Module to create the queue.
- Provide a name (for example: SSNODRQ) and a JNDI name (for example: queue/SSNODRQ).
- Select a subdeployment (for example: SSN-JMSFAServer) if you already created or follow below steps to create a New Subdeployment.(A subdeployment is a convenient way for grouping and targeting JMS module resources.)
- Provide a name for the subdeployment (for example: SSN-JMSFAServer) and click **OK**.
- Select the target JMS Server we created (for example: SSN-JMSServer) and Click **finish**.

d. Create JMS Connection Factory.

a. Click on **New** in JMS Module to create the Connection factory.

b. Give the Connection factory a name (for example, SSNTestHarnessConnectionFactory and JNDI name (for example, jms/ SSNTestHarnessConnectionFactory). Click **Next**.

c. Select **Advance Targeting** and on the next page select the subdeployment you created above (SSN-JMSFAServer). Wait for the page to refresh and click on **Finish**.

d. Click on **New** in JMS Module to create the Connection factory.

e. Give the Connection factory a name (for example, SSNConnectionFactory) and JNDI name (for example, jms/SSNConnectionFactory). Click **Next.**

f. Select **Advance Targeting** and on the next page select the subdeployment you created above (SSN-JMSFAServer). Wait for the page to refresh and click **Finish**.

e. Create a Source JMS Bridge Destination.

a. Under Domain Structure, navigate to **Services** > **Messaging** > **Bridge** > **JMS Bridge Destinations.**

b. On the **JMS Bridge Destinations** page, click **New**.

c. On the create a **New JMS Bridge Destination** page:

- Provide a name for your JMS Bridge destination SSNTestHarnessBridgeDestination.
- Select Adapter JNDI named eis.jms.WLSConnectionFactoryJNDINoTX.
- Provide Initial Context Factory as weblogic.jndi.WLInitialContextFactory.
- Provide Connection URL as t3://@SSN_UIQ_HOST@:@SSN_UIQ_PORT@.
- Provide Connection Factory JNDI name as jms/SSNTestHarnessConnectionFactory.
- Provide Destination JNDI name as queue/SSNTestSSNODRQ.
- Select Destination type as queue.
- Provide username.
- Provide password.
- Confirm the password.

Note: After creating JMS Bridge Destination, click **Services** > **Messaging** > **Bridge** > **JMS Bridge Destinations** > **SSNSOABridgeDestination**.

- On the **SSNSOABridgeDestination** page, enter the username and password values. Click **Save**.

f. Create a Target JMS Bridge Destination.

a. Under Domain Structure, navigate to **Services** > **Messaging** > **Bridge** > **JMS Bridge Destinations.**

b. On the **JMS Bridge Destinations** page, click **New**.

c. On the **Create a New JMS Bridge Destination** page:

- Provide a name for your JMS Bridge destination SSNSOABridgeDestination.

- Select Adapter JNDI name as eis.jms.WLSConnectionFactoryJNDINoTX.
- Provide Initial Context Factory as weblogic.jndi.WLInitialContextFactory.
- Provide Connection URL as t3://@SOA_HOST@:@SOA_PORT_NUMBER.
- Provide Connection Factory JNDI name as jms/SSNConnectionFactory"
- Provide Destination JNDI name as queue/SSNODRQ.
- Select Destination type as queue.

Note: After creating JMS Bridge Destination, navigate to **Services > Messaging > Bridge > JMS Bridge Destinations > SSNSOABridgeDestination**.

- On the **SSNSOABridgeDestination** page, enter username and password values, click **Save**.

g. Create a Bridge.

Under Domain Structure, navigate to **Services > Messaging > Bridges On the Bridges** page. Click **New**. On the **Create a New Bridge** page:

- Provide a name for Bridge as SSNODRQBridge.
- Select Quality of Service as At most-Once.
- Check Started.
- Click **Next.**
- Select Source Bridge Destination as SSNTestHarnessBridgeDestination.
- Select Messaging Provider as WebLogic Server 7.0 or Higher.

Note: In real time depending on SSN environment this should be changed

- Select Target Bridge Destination as SSNSOABridgeDestination.
- Select Messaging Provider as WebLogic Server 7.0 or Higher.
- Select server as soa_server1.

Note: Any web logic managed server.

- Click **Finish**.

7. Deploy the SOA adapter on the separate WebLogic instance.

Note: Modify the SOA Host Server, SOA Port Number, SOA WebLogic User Name, SOA WebLogic User Password menu items according to separate domain using SOA Configuration Menu item 9.

For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

UNIX

```
cd $SPLEBASE/soaapp
```

For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>-
DsysPropFile=soa.properties

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>-
DsysPropFile=soa.properties
```

Windows

```
cd %SPLEBASE%\soaapp
```

For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>-
DsysPropFile=soa.properties

%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D7.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>-
DsysPropFile=soa.properties
```

8. Deploy the TestHarness SOA composites on the separate WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

UNIX

```
cd $SPLEBASE/soaapp
```

For WebLogic 12c:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
 deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
```

Windows

```
cd %SPLEBASE%\soaapp
```

For WebLogic 12c:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D7.xml
 deployTestHarness -Dserver.user=<ADMIN_USER>
-Dserver.password=<ADMIN_PASSWORD> -DsysPropFile=soa.properties
```

Configuring Security for the SOA System

Security is managed through policies attached to the input and output points of each composite. More information on policies and their configuration can be found in **Chapter 10: Configuring Policies** in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite.*

This section describes how to configure security credentials for the SOA system, including:

- Configuring Security for the SOA System to Communicate with the Application Framework

- Configuring Security for the SOA System to Communicate with the Head-End System

Configuring Security for the SOA System to Communicate with the Application Framework

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server.
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click on the domain, and choose **Security, Credentials**.
2. On the **Credentials** page, click **Create Map.**
3. **In the Create Map dialog, name the map oracle.wsm.security, then click OK.**
4. Click **Create Key** and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.d7.credentials
    - **Type:** Password
    - **Username:** A valid WebLogic user name
    - **Password:** A valid WebLogic password
5. Click **OK.**
6. Click **Create Key** again and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.d7.ouaf.credentials
    - **Type:** Password
    - **Username:** A valid OUAF user name
    - **Password:** A valid OUAF password
7. Click **OK.**

Configuring Security for the SOA System to Communicate with the Head-End System

Configuring security for the SOA system involves creating the security credentials in Oracle Enterprise Manager and establishing a secure socket layer communications channel to the head end system.

These configuration tasks are described in the following sections:

- Creating the Security Credentials
- Attaching Secure Socket Layer (SSL) Policies

Creating the Security Credentials

Configuring security for the SOA system involves using Oracle Enterprise Manager to create the following security credentials:

- A Credential Map
- A Credential Key for the WebLogic Server.
- A Credential Key for the Oracle Utilities Application Framework

Use the following procedure to create the security credentials:

1. In Oracle Enterprise Manager, expand the WebLogic domain, right-click on the domain, and choose **Security, Credentials.**
2. On the **Credentials** page, click **Create Map.**
3. In the Create Map dialog, name the map **oracle.wsm.security,** then click **OK.**
4. Click **Create Key** and enter the following values:
    - **Select Map:** oracle.wsm.security
    - **Key:** sgg.d7.ssn.credentials
    - **Type:** Password
    - **Username:** A valid WebLogic user name
    - **Password:** A valid WebLogic password
5. Click OK.

Importing the Policy Templates and Policies

Follow the procedure below to import the policy templates and policies:

a. Import the policy template jar using Enterprise Manager.

For **Linux**:

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d1
```

For **Windows**
cd %SPLEBASE%/soaapp

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile package-soa-
policy.xml -Dproduct=d1
```

b. In Oracle Enterprise Manager, navigate to WebLogic Domain and select the required SOA domain.

c. Right click on the domain and navigate to **Web Services**, **WSM Policies**.

d. Click on **Web Services Assertion Templates** at the top of the page

e. Click on **Import** and import the sgg-d1-policy.jar zip.

This file is located in the following directory:

UNIX: $SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

Attaching Secure Socket Layer (SSL) Policies

Silver Springs Networks accepts SSL transmissions to secure web service calls to their head-end system. Oracle web service references communicating with the head-end system include OWSM policies that implement HTTPS over SSL. The following services are all contained in the Common composite:

- JobManager
- DeviceManager
- DataAggregation
- DeviceResults

Each of these is configured to use the credential created above that uses the “sgg.d7.ssn.credentials” key.

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

Creating WebLogic Domain

Create the WebLogic native domain and deploy the application. For instructions refer to the *Native Installation Oracle Utilities Application Framework* (Doc ID: 1544969.1) white paper on My Oracle Support.

The MDB user configured in Menu 3 during the Oracle Utilities Application Framework installation has to be created in the Oracle Utilities Application Framework application and WebLogic console, and should be part of the “cisusers” group.

> **Note**: The first time you start Oracle Utilities Meter Data Management, you need to log into the WebLogic console and give system access to cisusers role. The WebLogic console application can be accessed through the following URL: http://<hostname>:<portname>/console.

Operating the Application

At this point your installation and custom integration process is complete. Be sure to read the *Server Administration Guide* (included in this release) for more information on configuring and operating the system.

Configuring SOA Authorization Policies

This section describes how to configure SOA authorization roles and policies to allow the oracle/binding_permission_authorization_policy to determine which users or groups are authorized to access the web services to which they are applied.

Note: Much of this information is derived from Policy Authorization Examples in SOA Suite 11g.

Configuring SOA authorization includes the following:

- Creating WebLogic Server Groups
- Creating Application Roles
- Creating Application Policies

Creating WebLogic Server Groups

In the WebLogic Server Console, create a group which includes the internal and external users defined for your implementation. For example, you might create the following group:

- CustomerGroup

Creating Application Roles

To create an application role,

1. Right-click on the WebLogic domain (or click the **WebLogic Domain** drop-down list), and select **Security** and then **Application Roles**.

   The **Application Roles** page opens.

2. Select "soa-infra" from the **Application Stripe** drop-down list (in the **Search** section) and click **Create**.

   The **Create Application Role** page opens.

3. Enter a **Role Name**, **Display Name**, and **Description** for the role and click **Add** (under **Members**).

   The **Add Principals** screen opens.

4. In the **Search** section, select "Group" from the **Type** drop-down list, and enter search criteria to find the group you created earlier, and click the search icon. Select the group you created earlier from the **Searched Principals** list, and click **OK**.

   The selected group will appear in the **Members** list.

5. 5.Click **OK** (upper right corner).

   An Information panel will display indicating that your application role has been added.

Creating Application Policies

To create an application policy:

1. Right-click on the WebLogic domain(or click the **WebLogic Domain** drop-down list), and select **Security** and then **Application Policies**.

   The **Application Policies** page opens.

2. In the **Search** section, select "soa-infra" from the **Application Stripe** drop-down list, select "Application Role": from the **Principal Type** drop-down list, and click **Create**.

   The **Create Application Grants** page opens.

3. Under **Permissions**, click **Add**.

   The **Add Permission** screen opens.

4. Click **Continue**.

5. Enter the following:

   - **Permission Class**: oracle.wsm.security.WSFunctionPermission
   - **Resource Name**: *
   - **Permission Actions**: * (asterisk)

   Note: Restrictions can be added via the **Resource Name** and **Permission Actions** fields for more granular control over individual composites.

6. Click **Select**.

   The "oracle.wsm.security.WSFunctionPermission" class will appear in the **Permissions** list

7. Under **Grantee**, click **Add**.

   The **Add Principals** screen opens.

8. Select "Group" from the **Type** drop-down list, and enter search criteria to find the group you created earlier, and click the search icon. Select the group you created earlier from the **Searched Principals** list, and click **OK**.

   The selected group will appear in the **Permissions** list.

6. Click **OK** (upper right corner).

An Information panel will display indicating that new security grant has been added.

Creating an Example WebLogic Domain

This section provides the steps to create example weblogic domains of OSB and SOA which are created under osbapp and soaapp. Before executing the below scripts, Repository Creation Utility (RCU) should be used to create schemas required for the respective domains and the values of prefix & password used for creation of schemas should be specified in the configuration menu.

Oracle does recommend the usage of example domains for production use.

Creating an OSB Example Domain

Follow the procedure below to create an OSB example domain:

1. Ensure that values are set for the following menu items.
   Please refer to Appendix B - "8. OSB Configuration" for more information.
   - OSB Port Number
   - OSB SSL Port Number
   - JDBC URL for database
   - OSB Service Table Schema Name
   - OSB Service Table Schema Password
2. Run the following commands:

   Linux:

   ```
   cd $SPLEBASE/bin
   ./createDomain.sh -t OSB
   ```

   Windows

   ```
   cd %SPLEBASE%/bin
   ./createDomain.cmd -t OSB
   ```

Creating a SOA Example Domain

Follow the procedure below to create a SOA example domain:

1. Ensure that values are set for the following menu items.
   Please refer to Appendix B, "9. SOA Configuration" for more information.
   - SOA Port Number
   - SOA SSL Port Number
   - JDBC URL for database
   - SOA Service Table Schema Name
   - SOA Service Table Schema Password
2. Run the following commands:

   Linux:

   ```
   cd $SPLEBASE/bin
   ./createDomain.sh -t SOA
   ```

Windows
cd %SPLEBASE%/bin

```
./createDomain.cmd -t SOA
```

Deploying OSB Adapter on SSL

This section describes steps to deploy OSB on SSL.

1. Set the OSB SSL Port Number and configure Menu 60 should be configured appropriately. Refer to Appendix B Installation and Configuration Worksheets for detailed info.
   - Enable OSB SSL Port
   - OSB Trust Keystore Type
   - OSB Trust Keystore File Type
   - OSB Trust Keystore File
2. Run the following commands when using Custom trust store:

   Note: Replace <adapter> in the below commands with the respective adapter name i.e (LG, D4, MV90, D6, D7, D8, DG).

UNIX

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-

osb_<adapter>.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
-
Dosb.keystore.passphrase=<passphrase_of_truststore_for_osb_deploym
ent>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml

update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
- Dosb.keystore.passphrase=<passphrase_of_ truststore
_for_osb_deployment>
```

This will not override any OSB custom changes

Windows

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
```

```
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
- Dosb.keystore.passphrase=<passphrase_of_ truststore
_for_osb_deployment>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp

%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml

update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
- Dosb.keystore.passphrase=<passphrase_of_ truststore
_for_osb_deployment>
```

This will not override any OSB custom changes

3. The following commands are required when using Demo trust store:

   Note: Replace <adapter> in the below commands with the respective adapter name i.e (LG, D4, MV90, D6, D7, D8, DG).

UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER>
-Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER>
-Douaf.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp


$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml
update_osb -Dadmin.user=<ADMIN_USER>
-Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER>
-Douaf.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Windows

```
cd %SPLEBASE%\osbapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true  -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version.

```
cd %SPLEBASE%/osbapp

%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true -
Dosb.user=<OSB_USER> -Dosb.password=<OSB_PASSWORD> -
Douaf.filter.user=<JMS_USER> -Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes.

Deploying SOA Composites on SSL

This section describes steps to deploy SOA composites on SSL.

1. Set SOA SSL Port Number and Menu 64 should be configured appropriately. Refer Appendix B Installation and Configuration Worksheets for detailed info.
    - Enable SOA SSL Port
    - SOA Trust Keystore Type
    - SOA Trust Keystore File Type
    - SOA Trust Keystore File
2. Create partitions on the Enterprise Manager console.
    a. For Adapter Development Kit, create the following partitions on the EM console:
        - MDF
        - DG
        - DG_TEST

    b. For Adapter for Networked Energy Services, create the following partitions on the EM console:
        - MDF
        - Echelon
        - Echelon_Test

    c. For Adapter for Itron Openway, create the following partitions on the EM console:
        - MDF
        - Itron
        - Itron_Test

    d. For Adapter for Landis+Gyr create the following partitions on the EM console:
        - MDF
        - LG

- LG_Test

e. For Adapter for Sensus RNI, create the following partitions on the EM console:

- MDF
- Sensus
- Sensus_Test

f. For Adapter for Silver Springs Networks, create the following partitions on the EM console:

- MDF
- SSN
- SSN_Test

3. The following commands are required when using Demo trust store, <adapter> in below commands should be replaced with respective adapter name i.e (LG, D4, D6, D7, D8, DG).

4. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties
```

   Windows

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties
```

5. Deploy the TestHarness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

   UNIX

```
cd $SPLEBASE/soaapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
soa_<adapter>.xml deployTestHarness  -Dserver.password=<SOA_USER>
 -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
```

Windows

Note: Open the command prompt as Administrative mode and then select the environment to deploy SOA.

```
cd %SPLEBASE%/soaapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile
deploy-soa_<adapter>.xml deployTestHarness  -
Dserver.password=<SOA_USER>
  -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
```

6. The following commands are required when using Custom trust store. <adapter> in the commands below should be replaced with the respective adapter name (LG, D4, D6, D7, D8, DG).
7. Add the following line in the file soa.properties, located at below locations:

```
javax.net.ssl.trustStorePassword=<passphrase_of_truststore
_for_soa_deployment>
```

Linux: $SPLEBASE/soaapp

Windows: %SPLEBASE%/soapp

8. Deploy the SOA adapter on the example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

UNIX

```
cd $SPLEBASE/soaapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties
```

Windows

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties
```

9. Deploy the TestHarness SOA composites on example WebLogic instance.

   For the SSL deployment procedure, refer to the Deploying SOA Composites on SSL section.

UNIX

```
cd $SPLEBASE/soaapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
soa_<adapter>.xml deployTestHarness  -Dserver.password=<SOA_USER>
```

```
 -Dserver.password=<SOA_PASSWORD> -DsysPropFile=soa.properties
```

Windows

> **Note**: Open the command prompt as Administrative mode and then select the environment to deploy SOA.

```
cd %SPLEBASE%/soaapp
%SPLEBASE%\product\apache-ant\bin\ant -buildfile
deploy-soa_<adapter>.xml deployTestHarness -
Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD> -
DsysPropFile=soa.properties
```

Deploying OSB Adapters with DataRaker

This section describes steps to deploy OSB with Dataraker functionality.

> **Note**: Replace <adapter> in the commands below with the respective adapter name i.e (LG, D4, MV90, D6, D7, D8, DG).

1. Run the following commands:

   UNIX

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true -
Ddeploy.dataraker=true -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

> **Note**: Use the following command if this is an upgrade from a previous version:

```
cd $SPLEBASE/osbapp

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true -
Ddeploy.dataraker=true -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

   This will not override any OSB custom changes.

   Windows

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true -
Ddeploy.dataraker=true -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

Note: Use the following command if this is an upgrade from a previous version:

```
cd %SPLEBASE%/osbapp
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD> -Dprocessing.archive=true -
Ddeploy.dataraker=true -Dosb.user=<OSB_USER> -
Dosb.password=<OSB_PASSWORD> -Douaf.filter.user=<JMS_USER> -
Douaf.filter.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

2. For SSL deployment of OSB adapters with DataRaker functionality, please refer Deploying OSB adapters on SSL with argument.

   Below is an example command for Linux with Custom trust store:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_<adapter>.xml -Dadmin.user=<ADMIN_USER>
-Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER>
-Douaf.password=<JMS_PASSWORD> -
Dosb.keystore.passphrase=<passphrase_of_truststore_for_osb_deploym
ent> - Ddeploy.dataraker=true
```

3. For Dataraker messages to pass through SSL, open SB console of OSB.
4. Select the DataRakerBusinessService under each of the adapter specific CM project
5. Create an OSB session by clicking on the “**Create**” button on top-left of the screen
6. Navigate to **Transport Detail** in the **Business Service Definition.**
7. Select **Enable SSL** under **Advanced Options.**
8. Click **Save** in the **Business Service** definition tab.
9. Click **Activate.**
10. Configure a queue on the SOA server for DataRaker functionality.
11. Create the following JMS queues:

    Queue Name: DataRakerQueue

    JNDI Name: DataRakerQueue

    Sub-deployment: SOASubDeployment

    Targets: SOAJMSServer

Chapter 8

Installing Oracle Utilities Service Order Management

This chapter describes steps required for a successful Oracle Utilities Service Order Management installation.

Installation Overview

The following overview guides you through the installation process. The details for each step are presented as individual chapters in the rest of this guide.

1. Confirm that the recommended hardware is ready. Refer to Operating Systems and Application Servers for more details.
2. Install prerequisite software. Refer to the Installing Prerequisite Software section for more details.

   Note: Oracle Utilities Service Order Management only supports WebLogic 12.2.1.3+ and Oracle Service Bus/Oracle SOA Suite 12.2.1.3.
3. Ensure that you have downloaded the Oracle Utilities Service Order Management V2.4.0.0.0 components from Oracle Software Delivery Cloud.
4. Go through the Appendix B**:** Installation and Configuration Worksheets to understand the configuration menu.
5. Determine the type of the installation: initial or demo.

   Refer to the Initial Installation or Demo Installation sections for more information.
6. Integrate Oracle Utilities Customer Care and Billing (CCB) with Oracle Utilities Service Order Management (SOM) by following the instructions in the document *Oracle Utilities Customer Care and Billing Integration to Oracle Utilities Service Order Management Installation Guide* on Oracle Technology Network.
7. Integrate Oracle Utilities Service Order Management (SOM) with Oracle Utilities Mobile Workforce Management (MWM) by following the instructions in the document *Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide on* Oracle Technology Network.

Initial Installation

A successful initial installation of SOM involves the installation of the following components:

- Oracle Utilities Service Order Management Database Component

  For steps to install the database, refer to the chapter “Installing the Database for Service Order Management” in the *Oracle Utilities Smart Grid Gateway Database Administrator’s Guide*.
- Oracle Utilities Application Framework V4.4.0.3.0 Application Component
- Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component

To install all of the above components, follow the instructions mentioned in Chapter 4**:** Installing Oracle Utilities Smart Grid Gateway—Initial Installation.

Demo Installation

A successful installation of SOM involves the installation of the following components:

- Oracle Utilities Service Order Management Database Component
  For the steps to install the demo database, refer to the chapter “Installing the Database for Service Order Management” in the *Oracle Utilities Smart Grid Gateway Database Administrator’s Guide.*
- Oracle Utilities Application Framework V4.4.0.3.0 Application Component
- Oracle Utilities Meter Data Management V2.4.0.0.0 Application Component

To install all of the above components, follow the instructions mentioned in Chapter 5**:** Installing Oracle Utilities Smart Grid Gateway—Demo Installation.

Chapter 9

Additional Tasks

This section describes tasks that should be completed after installing Oracle Utilities Smart Grid Gateway, including:

- Importing Self-Signed Certificates
- Customizing Configuration Files
- Integrating Existing Customer Modifications
- Generating the Application Viewer
- Building Javadocs Indexes
- Configuring the Environment for Batch Processing
- Customizing the Logo
- Configure Node Manager Properties to allow SSL
- Database Patching

Importing Self-Signed Certificates

If you are using self-signed certificates and the Inbound Web Services (IWS) feature, then it is necessary to import these certificates into the OUAF truststore file.

Perform the following commands:

1. Start WebLogic.
2. Initialize a command shell and setup the environment.

   UNIX

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
    For example:
   /ouaf/TEST_ENVIRON1/bin/splenviron.sh -e TEST_ENVIRON1
   ```

   Windows

   ```
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
   For example:
   D:\ouaf\TEST_ENVIRON1\bin\splenviron.cmd -e TEST_ENVIRON1
   ```

3. Run the following script to generate all information.

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh -i
   ```

   Windows

   ```
   %SPLEBASE%\bin\ initialSetup.cmd -i
   ```

   > **Note**: This needs to be performed before deploying the IWS application.

Customizing Configuration Files

If you wish to make customer modifications to various configuration files, create a 'CM copy' of the template file or a user exit. This preserves your changes whenever initialSetup is executed; otherwise, your changes to the delivered template files will be lost if it is patched in the future:

For example, to customize hibernate properties of the SPLWeb web application, perform the following:

1. Locate the hibernate.properties.template in the $SPLEBASE/templates directory
2. Copy the file to cm.hibernate.properties.template.
3. Apply your changes to cm.hibernate.properties.template.
4. Update application war file with the latest changes by executing the following command:

   UNIX

   ```
   $SPLEBASE/bin/initialSetup.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\initialSetup.cmd
   ```

Refer to the Oracle Utilities Application Framework SDK documentation for more details.

Integrating Existing Customer Modifications

Existing Customer Modifications (CM) applied to an application server on an earlier release cannot be applied directly to a later version. CM code needs to be applied from an SDK version compatible with this release.

Refer to SDK documentation for more information about migrating CM code.

Generating the Application Viewer

You may extend application viewer capabilities within an environment by generating additional items. These include information about algorithm types, algorithms, maintenance objects and data dictionary information. The Javadoc indexes are also re-built.

To generate the additional items in the application viewer, perform the following:

1. Shut down the environment.
2. Initialize a command shell and setup the environment by running the following:

   UNIX
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON

   For example:

   ```
   /ouaf/TEST_ENVIRON1/bin/splenviron.sh -e TEST_ENVIRON1
   ```

   Windows
   %SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%

   For example:

   ```
   D:\ouaf\TEST_ENVIRON1\bin\splenviron.cmd -e TEST_ENVIRON1
   ```

3. Run the following script to generate all information.

   UNIX

   ```
   ksh $SPLEBASE/bin/genappvieweritems.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\genappvieweritems.cmd
   ```

4. Restart your application.

Building Javadocs Indexes

Rebuilding Javadoc indexes is already part of generating application viewer above. However, there are times when you need to run it separately. For example, this is required after customer modifications (CM) have been applied to an environment when it includes Java code.

Perform the following to rebuild the Javadoc indexes.

Windows

```
%SPLEBASE%\bin\buildJavadocsIndex.cmd
```

UNIX

```
ksh $SPLEBASE/bin/buildJavadocsIndex.sh
```

Configuring the Environment for Batch Processing

See the *Server Administration Guide* for information on configuring the environment for batch processing.

Customizing the Logo

To replace the Oracle Utilities logo on the main menu with another image, put the new image <customer_logo_file>.png file into the directory $SPLEBASE/etc/conf/root/cm and create a new "External" Navigation Key called CM_logoImage. To do that, run the Oracle Utilities application from the browser with the parameters: http://<hostname>:<port>/cis.jsp?utilities=true&tools=true.

From the Admin menu, select Navigation Key.

Add the above Navigation Key with its corresponding URL Override path.

The syntax for the URL path is:

Windows

http://<host name>:<port>/<Web Context>/cm/<customer_logo_file>.png

UNIX

http://<host name>:<port>/<Web Context>/cm/<customer_logo_file>.png

The root directory may be deployed in war file format for runtime environment (SPLApp.war). Use provided utilities to incorporate your cm directory into SPLApp.war file0

Other Tasks

Configure Node Manager Properties to allow SSL

Follow the steps below to update the nodemanager.properties with the correct Private Key Passphrase.

Under the following location: DOMAIN_HOME/nodemanager update the following properties in the nodemanager.properties file:

- CustomIdentityKeyStorePassPhrase=
- CustomIdentityPrivateKeyPassPhrase=

Set these to the value “0uaf_demo_c3rt”

> **Note**: At first when the node manager is started, the values in the file will be encrypted. These values will need to updated in production configuration with the proper values based on your configuration.

Configure setDomainEnv.sh Script

You will need to set the value of SPLEBASE with the proper value for your implementation. Under the following location, DOMAIN_HOME/bin, update the setDomainEnv.sh file and add the following

```
SPLEBASE="${SPLEBASE}"
```

> **Note**: You will need to update ${SPLEBASE} with appropriate value based on your configuration.

Update SPLEBASE

The following update in the configuration indicates if the embedded configuration is being utilized or if the environment is a native installation to WebLogic. When this item is populated in the environment, the delivered base tools will be able to identify that the starting and stopping of the environment are being done under the domain home.

1. Initialize the Environment: splenviron.sh –e <Environment_Name>
2. Execute: configureEnv.sh –a
3. Select Menu Item: 52. Advanced Web Application Configuration

==

4. 02. Configuration Option: Domain Home Location

   Current Value <ENTER>:

   The Weblogic Domain Home location, when this parameter is populated you will need to use the native Weblogic tools for maintenance (starting, stopping, deployment, and undeployment).

   Enter Value: <Enter your domain home location>

5. Once the Domain Home location has been completed, Enter <P> Process

Update setDomainEnv.sh

To update serDomainEnv.sh, follow these steps:

1. Edit setDomainEnv.sh and change antlr, serializer and xalan jar versions to the following:
   - antlr-2.7.7.jar
   - serializer-2.7.2.jar
   - xalan-2.7.2.jar

2. Update setUserOverrides.sh.
3. Edit setUserOverrides.sh and add the below to JAVA_OPTIONS. For AIX, the below parameters also need to be added to JAVA_OPTIONS.

```
-
Djavax.xml.transform.TransformerFactory=org.apache.xalan.processor
.TransformerFactoryImpl -
Djavax.xml.validation.SchemaFactory:http://www.w3.org/2001/
XMLSchema=org.apache.xerces.jaxp.validation.XMLSchemaFactory
```

Database Patching

The database patching utility is delivered under SPLEBASE and is Java-based so you are able to create a standalone package to be able to install database patches on a separate server that has Java 7 installed. You can also install database patches using the components that are delivered under SPLEBASE without the need to move the database patching utility to a different server.

The following is an overview of the process to install database patches on a separate server. You will need to create a jar file containing the utilities and supporting files to allow you to run the database patch installer on another server.

To generate the jar file:

1. Initialize a command shell:

   The scripts that are provided with the system need to be run from a shell prompt on the machine where you installed the application server. Before such scripts can be run the shell must be "initialized" by running the splenviron script provided with the system.

   UNIX
   Log on to your UNIX box as the Oracle Utilities Administrator (default cissys) and open a shell prompt.

   In the following example, replace the variables

   - $SPLEBASE with the Full directory name that you installed the application into
   - $SPLENVIRON with the name you gave to the environment at installation time

   To initialize the environment enter:

   ```
   $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
   ```
   For example:

   ```
   /ouaf/DEMO/bin/splenviron.sh -e DEMO
   ```

   Windows
   The command window should be opened on the Windows server that you installed the application on.

   In the below example you should replace the following variables:

   - %SPLEBASE%: The Full directory name that you installed the application into
   - %SPLENVIRON%: The name you gave to the environment at installation time

To initialize the environment, type the following in your command prompt:

```
%SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
```

For example:

```
D:\ouaf\DEMO\bin\splenviron.cmd -e DEMO
```

2. Execute the following script to generate the jar file.

   UNIX

   ```
   ksh $SPLEBASE/bin/createDBStandlone.sh
   ```

   Windows

   ```
   %SPLEBASE%\bin\createDBStandlone.cmd
   ```

   > **Note**: By default, the output jar db_patch_standalone.jar is created in SPLEBASE/tools/dbstandalone. You can use the –l option to change the default directory.

3. Transfer the generated jar (db_patch_standalone.jar) to the Windows/Unix machine where you want to run the database patching utility.
4. Extract the contents of the archive file:

   ```
   jar xvf db_patch_standalone.jar
   ```

   > **Note**: You must have Java 7 JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

Overview of Database Patching Application

The database patching utility requires you have Java 7 JDK installed on the machine to execute the database patch application process.

The patch application process will perform following items to account for executing patch application under SPLEBASE or on a standalone server.

The database patch application utility will look do the following when it is executed:

- Checks to see if the environment variable $SPLEBASE is set.

  If the $SPLEBASE variable is set, the utility uses the libraries under $SPLEBASE to apply the patch.

- When the $SPLEBASE is not set, the utility checks to see if the TOOLSBIN environment variable is set.

  If the TOOLSBIN is set, the utility uses the libraries under the TOOLSBIN location.

- When both SPLEBASE and TOOLSBIN environment are not set, the utility prompts for the location of the TOOLSBIN.

The TOOLSBIN is the location of the of the application scripts ouafDatabasePatch.sh[cmd].

Unix Example:

The TOOLSBIN location would be set to /ouaf/dbpatch/bin

```
export TOOLSBIN=/ouaf/dbpatch/bin
```

Unix Sample - Database Patch Application (ouafDatabasePatch.sh)

> **Note**: The default permissions (ouafDatabasePatch.sh), may need to be adjusted to be executed by your user and group, when applying database fixes.

- Sample Execution – Passing a Password

```
./ouafDatabasePatch.sh -x ouafadm -p "-t O -d
CISADM_Z1_12C_44030_BLD001,slc04lds:1522:Z143Q12C"
```

- Sample Execution – Prompting for a Password

```
./ouafDatabasePatch.sh  -p "-t O -d
CISADM_Z1_12C_44030_BLD001,slc04lds:1522:Z143Q12C"
```

- Sample Execution - passing in the tools bin location

```
/ouafDatabasePatch.sh -u
ouafDatabasePatch.sh [-h] [-u] [-v] [-x] [-t tools dir] [-p
ouafparms]
     -h   displays help of ouafpatch
     -u   displays usage of ouafDatabasePatch.sh
     -v   displays version of ouafpatch
     -x   password to be passed to ouafpatch
     -b   location of the tools bin directory
     -p   parameters directly passed to ouafpatch
          must be the last parameter passed and
          be enclosed with quotes
```

WINDOWS Example:
The TOOLSBIN location would be set to c:\ouaf\dbpatch\bin.

```
SET TOOLSBIN=c:\ouaf\dbpatch\bin
```

Windows Sample - Database Patch Application (ouafDatabasePatch.cmd)

- Sample Execution – Passing a Password

```
ouafDatabasePatch.cmd -x password -p "-t O -d
SCHEMA_NAME,DBSERVER:DBPORT:DBSID"
```

- Sample Execution – Prompting for a Password

```
ouafDatabasePatch.cmd -p “-t O -d
SCHEMA_NAME,DBSERVER:DBPORT:DBSID C”
```

- Sample Execution - passing in the tools bin location

```
ouafDatabasePatch.cmd -b "C:\temp\db_patch_standalone\bin" -p
"-t O -d SCHEMA_NAME,DBSERVER:DBPORT:DBSID -c
C:\temp\dbrollup\CDXPatch2\CDXPatch.ini"
```

Windows Sample Usage

```
ouafDatabasePatch.cmd -u
USAGE:
USAGE:ouafDatabasePatch.cmd[-h] [-u] [-v] [-x] [-b tools dir] [-
p ouafparms]
USAGE:          -h   displays help of ouafpatch
USAGE:          -u   displays usage of ouafDatabasePatch.cmd
USAGE:          -v   displays version of ouafpatch
USAGE:          -x   password to be passed to ouafpatch
```

```
USAGE:          -b   location of the tools bin directory
USAGE:          -p   parameters directly passed to ouafpatch
USAGE:               must be enclosed with quotes: "  "
USAGE:
USAGE:
USAGE:
```

Appendix A

Installation Menu Functionality

The main configuration menu is structured so that related variables and/or options are grouped together and are associated by a menu item number. To access a particular group of variables and options, enter the menu item number associated with that group. Each option is displayed in turn on the screen, along with a prompt so that you can type the desired value for the option, if it is not the same as the default or current value.

When performing the initial installation you need to go through all menu options. The menu options may have a default value, a list of valid values and a validation check.

On each option prompt you can keep the current value by simply leaving the input line empty. In order to erase a variable value you need to enter one dot ("."). The leading spaces will be trimmed out on each values entered. The menu includes the following:

- **Valid Values: [ALFANUM].** This indicates you will need to enter an alphanumeric value in the prompt.
- **Valid Values: [NUM].** This indicates you will need to enter a numeric value in the prompt.

Please also note the following:

- When all options are set, type <P> at the main menu prompt option. This will save the option values selected throughout the configuration.
- During this processing the global variables are validated and the configuration file <SPLEBASE>/etc/ENVIRON.INI is created or updated. This file contains all the variables inputted and calculated. These are needed by the next part of the installation process.
- To exit the configuration utility without saving any of the values entered, type <X> and press 'Enter'.

Installation Menu Functionality Details

The Environment Installation Utility requires that Oracle Client Home is set in the path for the user performing the installation.

Prior to running the installation utility you will need to review the supported platforms document to ensure you have all of the Third Party software installed.

In this menu if the variables are set prior to execution, that value will be defaulted by the installation utility when performing the installation.

When the installation has been completed successfully, the values will be written to an ENVIRON.INI file. When splenviron.sh / cmd is executed, it will read from the ENVIRON.INI file to set the environment variables. Refer to the *Oracle Utilities Application Framework Server Administration Guide* for details about configuring these values.

Install the Oracle Client software specified in the Operating Systems and Application Servers section in **Appendix 2: Supported Platforms and Hardware Requirements** prior to running any of the installation utilities.

The following prompt appears when executing the installation utility:

```
Enter Oracle Client Home Directory (<ENTER> quit):
```

> **Note:** If the environmental variable ORACLE_CLIENT_HOME is set, the install script will validate the variable. If it passes the validation you will not be prompted for it. This is needed in order to run Perl installation utilities.

Encryption Methods

The Oracle Utilities Application Framework installation also uses industry standard cryptography to encrypt passwords that are prompted within the installation.

When these passwords are entered in the command line, the input values are not reflected on the screen when performing the installation.

Appendix B

Installation and Configuration Worksheets

This chapter includes the following sections:

Application Framework Installation and Configuration Worksheets

During the installation and configuration of the application you will need to provide a variety of system values. These worksheets will assist you in providing that information. They should be completed before installing the application framework, as described in the Installing the Application Server Component of Oracle Utilities Application Framework. No Customer Install Value fields should be left blank.

> **Note:** Some web application server information will not be available until the software installation steps have been completed as described in the Installing Application Server Prerequisite Software section.

Refer to the *Server Administration Guide* for additional details (default, valid values, usage, etc.), as applicable.

Menu Block 1: Environment ID, Roles, Third Party Software Configuration

The Environment ID, Roles, Third Party Software Configuration options include:

Menu Option	Name Used in Documentation	Customer Install Value
Environment ID	ENVIRONMENT_ID	
Server Roles	SERVER_ROLES	
Oracle Client Home Directory	ORACLE_CLIENT_HOME	
Web Java Home Directory	JAVA_HOME	
Hibernate JAR Directory	HIBERNATE_JAR_DIR	
**ONS JAR Directory	ONS_JAR_DIR	
Web Application Server Home Directory	WEB_SERVER_HOME	
***Additional JAR Directory	WLTHINT3CLIENT_JAR_DIR	

*   Denotes optional menu items that may be required for the product installation and variables.

**   In order to activate the RAC FCF, the application needs the external ons.jar file, from the ORACLE_HOME path:

```
$ORACLE_HOME/opmn/lib/ons.jar
```

During the installation the relevant option should be populated with the folder location of the ons.jar.

*** Refer to the for more information.

Menu Block 2: Keystore Options

The keystore is a set of files used for encryption, decryption and hash generation. The files reside in the following location:

<SPLEBASE>/ks/.ouaf_keystore

<SPLEBASE>/ks/.ouaf_storepass

In order to run the application correctly, data encryption, decryption and hash generation of data in the database and on the application server must be performed using the same keystore; otherwise, the application will fail.

> **Note**: Populate the “Import Keystore Directory” option to import an existing keystore.

Keystore options include:

Menu Option	Name Used in Documentation	Customer Install Value
Import Keystore Directory	KS_IMPORT_KEYSTORE_FOLDER	

Menu Block 50: Environment Installation Options

Environment installation options include:

Menu Option	Name Used in Documentation	Customer Install Value
Environment Mount Point	SPLDIR	
Log File Mount Point	SPLDIROUT	
Environment Name	SPLENVIRON	
Installation Application Viewer Module	WEB_ ISAPPVIEWER	
Install Demo Generation Cert Script	CERT_INSTALL_ SCRIPT	
Install Sample CM Source Code	CM_INSTALL_ SAMPLE	

Menu Block 1: Environment Description

The environment description menu option includes:

Menu Option	Name Used in Documentation	Customer Install Value
Environment Description	DESC	

Menu Block 2: [WebLogic] Business Application Server Configuration

WebLogic Business Application Server configuration options include:

Menu Option	Name Used in Documentation	Customer Install Value
Business Server Host	BSN_WLHOST	
Business Server Application Name	BSN_APP	

Menu Block 3: [WebLogic] Web Application Server Configuration

WebLogic Web Application Server configuration options include:

Menu Option	Name Used in Documentation	Customer Install Value
Web Server Host	WEB_WLHOST	
Weblogic SSL Port Number	WEB_WLSSLPORT	
Weblogic Console Port Number	WLS_ADMIN_PORT	
Web Context Root	WEB_CONTEXT_ ROOT	
WebLogic JNDI User ID	WEB_WLSYSUSER	
WebLogic JNDI Password	WEB_WLSYSPASS	
WebLogic Server Name	WEB_WLS_ SVRNAME	
Web Server Application Name	WEB_APP	
Deploy Application Viewer Module	WEB_DEPLOY_ APPVIEWER	
Enable The Unsecured Health Check Service	WEB_ENABLE_ HEALTHCHECK	
MDB RunAs User ID	WEB_IWS_MDB_ RUNAS_USER	
Super User Ids	WEB_IWS_SUPER_ USERS	

Menu Block 4 - Database Configuration

The parameters below and in the worksheet are for the database configuration. Note that if changes are made to any of the database menu option items below, thus potentially connecting to a different schema, a warning will be displayed in the screen next to the actual option that has been changed.

Menu Option	Name Used in Documentation	Customer Install Value
Application Server Database User ID	DBUSER	
Application Server Database Password	DBPASS	
XAI Database User ID	XAI_DBUSER	
XAI Database Password	XAI_DBPASS	
Batch Database User ID	BATCH_DBUSER	
Batch Database Password	BATCH_DBPASS	
Web JDBC DataSource Name	JDBC_NAME	
Database Name	DBNAME	
Database Server	DBSERVER	
Database Port	DBPORT	
ONS Server Configuration	ONSCONFIG	
Database Override Connection String	DB_OVERRIDE_ CONNECTION	
Character Based Database	CHAR_BASED_DB	
Oracle Client Character Set NLS_LANG	NLS_LANG	

Menu Block 5 - General Configuration Options

The general configuration options include:

Menu Option	Name Used in Documentation	Customer Install Value
Batch RMI Port	BATCH_RMI_PORT	
RMI Port number for JMX Business	BSN_JMX_RMI_PORT_ PERFORMANCE	
RMI Port number for JMX Web	WEB_JMX_RMI_PORT_PERFORMANCE	
JMX Enablement System User ID	BSN_JMX_SYSUSER	
JMX Enablement System Password	BSN_JMX_SYSPASS	

Menu Option	Name Used in Documentation	Customer Install Value
Coherence Cluster Name	COHERENCE_ CLUSTER_NAME	
Coherence Cluster Address	COHERENCE_ CLUSTER_ADDRESS	
Coherence Cluster Port	COHERENCE_ CLUSTER_PORT	
Coherence Cluster Mode	COHERENCE_ CLUSTER_MODE	

Menu Block 6 - OUAF TrustStore Options

The OUAF truststore configuration is required for IWS.

Menu Option	Name Used in Documentation	Customer Install Value
Import TrustStore Directory	TS_IMPORT_KEYSTORE_FOLDER	

Menu Block 8 - OSB Configuration

The OSB configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
OSB Home		
OSB Host Server	slc11cds.us.oracle.com	
OSB Port Number		
OSB SSL Port Number		
OSB Managed Server Port Number		
OSB Managed Server SSL Port Number		
JDBC URL for Database		
OSB Service Table Schema Name		
OSB Service Table Schema Password		
OSB WebLogic User Name		
OSB WebLogic User Password		

Menu Option	Name Used in Documentation	Customer Install Value
Mount Point for OSB Files	/spl/sploutput/osb	

Menu Block 9 - SOA Configuration

The SOA configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
SOA Home		
SOA Host Server	slc11cds.us.oracle.com	
SOA Port Number		
SOA SSL Port Number		
SOA Internal URL		
SOA External URL		
JDBC URL for SOA Database		
SOA Service Table Schema Name		
SOA Service Table Schema Password		
SOA WebLogic User Name		
SOA WebLogic User Password		
Specify the Path for XAI/IWS Service	XAIApp/xaiservert	

Menu Block 10 - SOA Configuration Plan (MDF)

The SOA configuration plan (MDF) includes:

Menu Option	Name Used in Documentation	Customer Install Value
MDF Bulk Request Callback URL		
MDF Headend HTTP Connection Timeout	50000	
MDF Headend HTTP Read Timeout	500000	
MDF SOA Request Queue JNDI Name	queue/BulkRequestQueue	

Menu Option	Name Used in Documentation	Customer Install Value
MDF SOA Notify Queue JNDI Name	queue/BulkNotifyQueue	
MDF SOA Command Queue JNDI Name	queue/BulkCommandQueue	
SGG-NMS TestHarness Partition Name	SGG-NMS_Test	

Menu Block 11 - Configuration for DataRaker Integration

The DataRaker Integration configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
JNDI Name of Destination Queue to publish SGG payloads for DataRaker Integration Tool	DataRakerQueue	
Number of records (SGG Payloads) to accumulate	100	
Max file size for the accumulated (SGG Payloads) file in Kilobytes	524288	
Specify a time which, when exceeded, causes a new outgoing file to be created in seconds	600	
Polling frequency of Staging directory for new files in seconds	60	
Mount point/directory for the accumulated SGG payload file	/spl/sploutput/staging	
Mount Point/directory for the converted XML file to place for DataRaker	/spl/sploutput/int	

Menu Block 16 - SOA Configuration Plan (LG)

The SOA configuration plan (LG) includes:

Menu Option	Name Used in Documentation	Customer Install Value
LG SOA Partition Name	LG	

Menu Option	Name Used in Documentation	Customer Install Value
LG SOA TestHarness Partition Name	LG_Test	
AMI Event Subscriber Output Path	/spl/sploutput/osb/lg-cim-event	
MR_Server endpoint URI		
CD_Server endpoint URI		
CIM_Server endpoint URI		
MeteringServer endpoint URI		
Security policy attached to outbound web service calls to a CIM interface	sgg/d3_cfs_cim_header_client_policy	
Security policy attached to inbound web service calls from a CIM interface	sgg/d3_cim_token_service_policy	
The name of the OWSM policy to use when SOA calls a head end system	oracle/ http_basic_auth_over_ssl_client_policy	
The name of the OWSM policy to use when SOA is called by a head end system	oracle/ http_basic_auth_over_ssl_service_policy	

Menu Block 17 - SOA Configuration Plan (NES)

The SOA configuration plan (NES) includes:

Menu Option	Name Used in Documentation	Customer Install Value
NES endpoint URI		
SOA partition to which the application is installed	Echelon	
Path to the NES EventManager web service on the head end system	CoreServices/EventManager.asmx	
Path to the NES GatewayManager web service	CoreServices/GatewayManager.asmx	
Path to the NES DeviceManager web service on the head end system	CoreServices/DeviceManager.asmx	
Path to the NES SettingManager web service on the head end system	CoreServices/SettingManager.asmx	

Menu Option	Name Used in Documentation	Customer Install Value
Path to the NES UserManager web service on the head end system	CoreServices/UserManager.asmx	
Name of the OWSM policy to use when SOA calls a head end system	oracle/ http_basic_auth_over_ssl_client_policy	
Name of the OWSM policy to use when SOA is called by a head end system	oracle/ http_basic_auth_over_ssl_service_policy	

Menu Block 18 - SOA Configuration Plan (Sensus)

The SOA configuration plan (Sensus) includes:

Menu Option	Name Used in Documentation	Customer Install Value
Sensus SOA TestHarness Partition Name	Sensus_Test	
Sensus SOA Partition Name	Sensus	
MR Server Endpoint URI		
CD Server Endpoint URI		
OD Server Endpoint URI		
Headend Http Read Timeout	500000	
Headend Http Connection Timeout	50000	
The name of the OWSM policy to use when SOA calls a head end system	oracle/ http_basic_auth_over_ssl_client_policy	
The name of the OWSM policy to use when SOA is called by a head end system	oracle/ http_basic_auth_over_ssl_service_policy	

Menu Block 19 - SOA Configuration Plan (SSN)

The SOA configuration plan (Sensus) includes:

Menu Option	Name Used in Documentation	Customer Install Value
SSN SOA Partition Name	SSN	
SOA Weblogic User Name		
SSN SOA Queue JNDI Name	queue/SSNODRQ	

Menu Option	Name Used in Documentation	Customer Install Value
SSN Headend DataAggregation Endpoint URI		
The URL for the SSN 4.7 DataAggregation service (DataAggregation.asmx)	http://127.0.0.1/CoreServices/DataAggregation.asmx	
The URL for the SSN 4.10 DataAggregation service	https://ssn.ssnsgs.net:3000/amm/webservice/v2_1/DataAggregat...	
SSN Headend DeviceManager Endpoint URI		
The URL for the SSN 4.7 DeviceManager service (DeviceManager.asmx)	http://127.0.0.1/CoreServices/DeviceManager.asmx	
The URL for the SSN 4.10 DeviceManager service	https://ssn.ssnsgs.net:3000/amm/webservice/v2_1/DeviceManage...	
SSN Headend DeviceResults Endpoint URI		
The URL for the SSN 4.7 DeviceResults service (DeviceResults.asmx)	http://127.0.0.1/CoreServices/DeviceResults.asmx	
The URL for the SSN 4.10 DeviceResults service	https://ssn.ssnsgs.net:3000/amm/webservice/v2_1/DeviceResult...	
SSN Headend JobManager Endpoint URI		
The URL for the SSN 4.7 JobManager service (JobManager.asmx)	http://127.0.0.1/CoreServices/JobManager.asmx	
The URL for the SSN 4.10 JobManager service:	https://ssn.ssnsgs.net:3000/amm/webservice/v2_1/JobManagerPo...	
The name of the OWSM policy to use when SOA calls a head end system	oracle/http_basic_auth_over_ssl_client_policy	
The name of the OWSM policy to use when SOA is called by a head end system	oracle/http_basic_auth_over_ssl_service_policy	

Menu Block 20 - SSN JMS Source Destination Bridge Configuration

The SSN JMS Source Destination Bridge configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
SSN Bridge Destination Name	SSNTestHarnessBridgeDestination	
SSN Bridge Destination Additional Classpath		
SSN Bridge Destination Connection URL		
SSN Bridge Destination Initial Context Factory	weblogic.jndi.WLInitialContextFactory	
SSN Bridge Connection Factory JNDI Name	jms/SSNTestHarnessConnectionFactory	
SSN Bridge Destination Queue JNDI Name	queue/SSNTestSSNODRQ	
SSN Destination Bridge Username		

Menu Block 21 - DG Reference Implementation SOA Configuration

The DG Reference Implementation SOA configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
DG SOA Partition Name	DG	
MR Server Endpoint URI		
CD Server Endpoint URI		
OD Server Endpoint URI		
Headend Http Read Timeout	500000	
Headend Http Connection Timeout	50000	
DG SOA TestHarness Partition Name	DG_Test	

Menu Block 22 - SOA Configuration Plan (Itron Openway)

The SOA Configuration Plan (Itron Openway) configuration includes:

Menu Option	Name Used in Documentation	Customer Install Value
Itron SOA Partition Name	Itron	

Menu Option	Name Used in Documentation	Customer Install Value
Headend Http Read Timeout	500000	
Headend Http Connection Timeout	50000	
DataSubscriberService Output Path		
ExceptionSubscriberService Output Path		
Itron Headend DataService Endpoint URI		
Itron Headend DiagnosticService Endpoint URI		
Itron Headend UtilService Endpoint URI		
Itron Headend ControlService Endpoint URI		
Itron Headend ProvisioningService Endpoint URI		
Itron Headend ProvisioningService370 Endpoint URI		
Itron Headend ControlService370 Endpoint URI:		
Itron SOA TestHarness Partition Name	Itron_Test	
The name of the OWSM policy to use when SOA calls a head end system	oracle/ http_basic_auth_over_ssl_client_policy	
The name of the OWSM policy to use when SOA is called by a head end system	oracle/ http_basic_auth_over_ssl_service_policy	

Advanced Menu Options

The advanced menu options are not available during installation. These options can be accessed after installation using the following commands:

Unix:

```
$SPLEBASE/bin/configureEnv.sh -a
```

Windows

```
%SPLEBASE%\bin\configureEnv.cmd -a
```

Menu Block 50 - WebLogic Advanced Environment Miscellaneous Configuration

WebLogic advanced environment miscellaneous configurations include:

Menu Option	Name Used in Documentation	Customer Value Install
OUAF DBMS Scheduler User	OUAF_DBMS_SCHEDULER_USER	
WebLogic ThreadPoolWorker Enabled	WLS_THEADPOOLWORKERENABLED	
Online JVM Batch Server Enabled	BATCHENABLED	
Online JVM Batch Number of Threads	BATCHTHREADS	
Online JVM Batch Scheduler Daemon Enabled	BATCHDAEMON	
Enable Batch Edit Functionality	BATCHEDIT_ ENABLED	
Batch Online Log Directory	BATCH_ONLINE_LOG_DIR	
JDBC Read Timeout	JDBC_TIMEOUT	
Enable JMS Global Flush for Batch	ENABLE_JMS_GLOBAL_FLUSH	
Add UsernameToken.xml	ADD_USERNAMETOKEN_XML	
IWS deployment target	WLS_CLUSTER_NAME	
Web Admin Server Host	WEB_ADMIN_SERVER	
Split File Size in MB	TEMPSTORAGE_SPLITFILESIZE	
GIS Service Running on the same Web Server	GIS	
GIS Service URL	GIS_URL	
GIS WebLogic System User ID	GIS_WLSYSUSER	
GIS WebLogic System Password	GIS_WLSYSPASS	
Online Display Software Home	ONLINE_DISPLAY_HOME	
Max Queries To Hold In Cache Across All Threads	XQUERIES_TO_ CACHE	
Seconds Timeout Flush Cache Completely	XQUERY_CACHE_ FLUSH_TIMEOUT	

Menu Block 51 - WebLogic Advanced Environment Memory Configuration

WebLogic advanced environment memory configurations include:

Menu Option	Name Used in Documentation	Customer Install Value
Global JVM Arguments	GLOBAL_JVMARGS	
Ant Min Heap Size	ANT_OPT_MIN	
Ant Max Heap Size	ANT_OPT_MAX	
Ant Additional Options	ANT_ADDITIONAL_OPT	
Thread Pool Worker Java Min Heap Size	BATCH_MEMORY_OPT_MIN	
Thread Pool Worker Java Max Heap Size	BATCH_MEMORY_OPT_MAX	
Thread Pool Worker Additional Options	BATCH_MEMORY_ ADDITIONAL_OPT	

Menu Block 52 - Advanced Web Application Configuration

Advanced web application configurations include:

Menu Option	Name Used in Documentation	Customer Install Value
Web Application Cache Settings	WEB_L2_CACHE_MODE	
Web Server Port Number	WEB_WLPORT	
CSRF Protection For REST Services	CSRF_PROTECTION	
OWSM Protection For REST Services	OWSM_PROTECTION_FOR_ REST_SERVICES	
Domain Home Location	WLS_DOMAIN_HOME	
Batch Cluster URL	WEB_BATCH_CLUSTER_URL	
Strip HTML Comments	STRIP_HTML_COMMENTS	
Authentication Login Page Type	WEB_WLAUTHMETHOD	
Web Form Login Page	WEB_FORM_LOGIN_PAGE	
Web Form Login Error Page	WEB_FORM_LOGIN_ERROR_ PAGE	
Application Viewer Form Login Page	WEB_APPVIEWER_FORM_ LOGIN_PAGE	
Application Viewer Form Login Error Page	WEB_APPVIEWER_FORM_ LOGIN_ERROR_PAGE	

Menu Option	Name Used in Documentation	Customer Install Value
Help Form Login Page	WEB_HELP_FORM_LOGIN_PAGE	
Help Form Login Error Page	WEB_HELP_FORM_LOGIN_ERROR_PAGE	
Web Security Role	WEB_SECURITY_NAME	
Web Principal Name	WEB_PRINCIPAL_NAME	
Application Viewer Security Role	WEB_APPVIEWER_ROLE_NAME	
Application Viewer Principal Name	WEB_APPVIEWER_PRINCIPAL_NAME	
This is a development environment	WEB_ISDEVELOPMENT	
Preload All Pages on Startup	WEB_PRELOADALL	
Maximum Age of a Cache Entry for Text	WEB_MAXAGE	
Maximum Age of a Cache Entry for Images	WEB_MAXAGEI	
JSP Recompile Interval (s)	WEB_WLPAGECHECKSECONDS	
Enable Strict Transport Security	STRICT_TRANSPORT_SECURITY	
Strict Transport Security Max Age	HSTS_MAX_AGE	
Strict Transport Security Include Subdomains	HSTS_SUBDOMAINS	
Strict Transport Security Preload	HSTS_PRELOAD	

Menu Block 54 - WebLogic Diagnostics

WebLogic diagnostic options include:

Menu Option	Name Used in Documentation	Customer Install Value
Diagnostic Context Enabled	WLS_DIAGNOSTIC_CONTEXT_ENABLED	

Menu Block 55 - URI, File and URL Related Options

URI, File and URL Related Options include:

Menu Option	Name Used in Documentation	Customer Install Value
Restriction URIs Enable	CLOUD_RESTRICTION_URIS_ ENABLE	
Custom SQL Security	CUSTOM_SQL_SECURITY	
White List Full Path	CLOUD_WHITE_LIST_PATH	
Custom White List Full Path	CLOUD_CUSTOM_WHITE_LIST _PATH	
Substitution Variable List File Location	CLOUD_SUBSTITUTION_VARIA BLE_LIST_FILE_LOCATION	
Directory For Variable F1_CMA_FILES	CLOUD_LOCATION_ F1_MIGR_ASSISTANT_FILES	
URI For Variable F1_OAUTH2_URI	CLOUD_LOCATION_F1_ OAUTH2_URI	
URI for Variable F1_BASE_REST_URL	CLOUD_LOCATION_F1_BASE_ REST_URL	
URI for Variable F1_OPEN_API_BASE_URL	CLOUD_LOCATION_F1_OPEN_ API_BASE_URL	
URI For Variable F1_BASE_WEB_URI	CLOUD_LOCATION_F1_BASE_ WEB_URI	
URI For Variable F1_BASE_IWS_URI	CLOUD_LOCATION_F1_BASE_I WS_URI	
Consolidated Logfile Full Path	CONSOLIDATED_LOG_FILE_P ATH	
Temporary File Location	TMP_FILE_LOCATION	

Menu Block 56 - Mobile Security Configuration

Mobile Security configurations include:

Menu Option	Name Used in Documentation	Customer Install Value
Enable Mobile Application	MOBILE_ENABLED	
Deploy Only Mobile Web Application	MOBILE_APP_ONLY	
Mobile Application Directory	MOBILE_APPDIR	
Allow Self Signed SSL Certificates	ALLOW_SELFSIGNED_SSL	
Force Http Connection	FORCE_HTTP	

Menu Option	Name Used in Documentation	Customer Install Value
Web Mobile Form Login Page	WEB_MOBILE_FORM_LOGIN_PAGE	
Web Mobile Form Login Error Page	WEB_MOBILE_FORM_LOGIN_ERROR_PAGE	

Meter Data Management Installation and Configuration Worksheets

During the installation and configuration of the application you will need to provide a variety of system values. These worksheets will assist you in providing that information. They should be completed before installing the application framework, as described in Installing Application Components. No Customer Install Value fields should be left blank.

Some web application server information will not be available until the software installation steps have been completed as described in Installing Application Server Prerequisite Software.

> **Note:** The OSB configuration and SOA configuration menus are optional for Oracle Utilities Meter Data Management and Oracle Utilities Customer to Meter, and can be skipped. These configurations are required in case another product such as Oracle Utilities Smart Grid Gateway will also be installed on top of Oracle Utilities Meter Data Management.

WebLogic OSB Configuration

The WebLogic OSB configuration includes:

Menu Option	Name Used In Documentation	Customer Install Value
OSB Home	OSB_HOME	
OSB Host Server	OSB_HOST	
OSB Port Number:	OSB_PORT_NUMBER	
OSB SSL Port Number	OSB_SSL_PORT	
OSB Managed Server Port Number	OSB_MS_PORT_NUMBER	
OSB Managed Server SSL Port Number	OSB_MS_SSL_PORT_NUMBER	
JDBC URL for database	DBURL_OSB	
OSB Service Table Schema Name	RCUSTBSCHEMA_OSB	

Menu Option	Name Used In Documentation	Customer Install Value
OSB Service Table Schema Password	RCUSTBSCHEMAPWD_OSB	
OSB WebLogic User Name	WEBLOGIC_USERNAME_OSB	
OSB WebLogic User Password	WEBLOGIC_PASSWORD_OSB	
Mount Point for OSB files	OSB_LOG_DIR	

WebLogic SOA Configuration

The WebLogic SOA Configuration includes:

Menu Option	Name Used in this Documentation	Customer Install Value
SOA Home	SOA_HOME	
SOA Host Server	SOA_HOST	
SOA Port Number:	SOA_PORT_NUMBER	
SOA SSL Port Number	SOA_SSL_PORT_NUMBER	
SOA Internal URL	SOA_INTERNAL_URL	
SOA External URL	SOA_EXTERNAL_URL	
JDBC URL for database	DBURL_SOA	
SOA Service table schema Name	RCUSTBSCHEMA_SOA	
SOA Service table schema Password	RCUSTBSCHEMAPWD_SOA	
SOA WebLogic User Name	WEBLOGIC_USERNAME_SOA	
SOA WebLogic User Password	WEBLOGIC_PASSWORD_SOA	
Specify the path for XAI/IWS Service	WEB_SERVICE_PATH	

WebLogic SOA Configuration Plan

This configuration is required for installing the following adapters:

- Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay

The WebLogic SOA Configuration Plan includes:

Menu Option	Name Used In Documentation	Customer Install Value
MDF Bulk Request Callback URL	D1_BULK_REQUEST_ CALLBACK_URL	

Menu Option	Name Used In Documentation	Customer Install Value
MDF Headend http connection timeout	D1_HEADEND_HTTP_CONN_ TIMEOUT	
MDF Headend http read timeout	D1_HEADEND_HTTP_READ_ TIMEOUT	
MDF SOA Request Queue JNDI Name	SOA_REQUEST_QUEUE_D1	
MDF SOA Notify Queue JNDI Name	SOA_NOTIFY_QUEUE_D1	
MDF SOA Command Queue JNDI Name	SOA_COMMAND_QUEUE_D1	
SGG-NMS TestHarness Partition Name	SOA_PARTITION_D1	

Configuration for DataRaker Integration

The Configuration for DataRaker Integration includes:

Menu Option	Name Used In Documentation	Customer Install Value
Destination Queue to publish SGG payloads for DataRaker Integration Tool	SGG_DR_INT_QUEUE	
Number of records (SGG Payloads) to accumulate	SOA_DR_PUBLISH_SIZE	
Max file size for the accumulated (SGG Payloads) file in Kilobytes	SOA_DR_FILE_SIZE	
Specify a time which, when exceeded, causes a new outgoing file to be created in seconds	SOA_DR_ELAPSED_TIME	
Polling frequency of Staging directory for new files in seconds	SOA_DR_POLLING_FREQ	
Mount point/directory for the accumulated SGG payload file	SOA_DR_STAGING_DIR	
Mount Point/directory for the converted XML file to place for DataRaker	SOA_DR_INTEGRATION_DIR	

Advanced Menu Options

The advanced menu options are not available during installation. These options can be accessed after installation using the following commands:

Unix

```
$SPLEBASE/bin/configureEnv.sh -a
```

Windows

```
%SPLEBASE%\bin\configureEnv.cmd -a
```

Advanced Menu Option for OSB SSL Deployment

The Advanced Menu Option for OSB SSL deployment includes:

Menu Option	Name Used In Documentation	Customer Install Value
Enable OSB SSL Port	OSB_SSL	
OSB Trust Keystore Type	OSB_TRUST_KS	
OSB Trust Keystore File Type	OSB_TRUST_KS_TYPE	
OSB Trust Keystore File	OSB_TRUST_KS_FILE	

Advanced Environment Memory Configurations

The Advanced Environment Memory configurations include:

Menu Option	Name Used In Documentation	Customer Install Value
SOA Initial Heap Size	SOA_MEMORY_OPT_MIN	
SOA Maximum Heap Size	SOA_MEMORY_OPT_MAX	
SOA Minimum Perm Size	SOA_MEMORY_OPT_MINPERM SIZE	
SOA Maximum Perm Size	SOA_MEMORY_OPT_ MAXPERM SIZE	
SOA Application Additional Options	SOA_JVM_ADDITIONAL_OPT	
The name of the OWSM policy to use when SOA calls another SOA service	SOA_SOA_CLIENT_POLICY	
The name of the OWSM policy to use when SOA is called by another SOA service	SOA_SOA_SERVICE_POLICY	
The name of the OWSM policy to use when SOA calls an OUAF service	SOA_SOA_SERVICE_POLICY	

The Advanced Memory Configurations for OSB includes:

Menu Option	Name Used In Documentation	Customer Install Value
OSB Initial Heap Size	OSB_MEMORY_OPT_MIN	
OSB Maximum Heap Size	OSB_MEMORY_OPT_MAX	
OSB Minimum Perm Size	OSB_MEMORY_OPT_MINPERMSIZE	
OSB Maximum Perm Size	OSB_MEMORY_OPT_MAXPERMSIZE	
OSB Application Additional Options	OSB_JVM_ADDITIONAL_OPT	

The Data Migration options include:

Menu Option	Name Used In Documentation	Customer Install Value
Enable Data Migration	DATA_MIGRATION	
Data Migration Database User	DATA_MIGRATION_DB_USER	
Data Migration Database Password	DATA_MIGRATION_DB_PASS	

The Advanced Configurations for SOA include:

Menu Option	Name Used In Documentation	Customer Install Value
Enable SOA SSL Port	SOA_SSL	
SOA Trust Keystore Type	SOA_TRUST_KS	
SOA Trust Keystore File Type	SOA_TRUST_KS_ TYPE	
SOA Trust Keystore File	SOA_TRUST_KS_ FILE	

The SSN SOA TestHarness configurations include:

Menu Option	Name Used In Documentation	Customer Install Value
SSN TestHarness SOA Host Server	SOA_HOST_TEST_D7	
SSN TestHarness SOA Port Number	SOA_PORT_NUMBER_D7	
SSN SOA TestHarness Partition Name	SOA_PARTITION_TEST_D7	

Menu Option	Name Used In Documentation	Customer Install Value
SSN SOA TestHarness Queue JNDI Name	SOA_QUEUE_TEST_D7	

Smart Grid Gateway Installation and Configuration Worksheets

During the installation and configuration of the application you will need to provide a variety of system values. These worksheets will assist you in providing that information. They should be completed before installing the application framework, as described in **Installing Application Components** on page 4-2. No Customer Install Value fields should be left blank.

> **Note:** Some web application server information will not be available until the software installation steps have been completed as described in Installing Application Server Prerequisite Software.

This section includes worksheets for the following adapters:

- For the Adapter Development Kit
- For the Networked Energy Services Adapter
- For the Itron OpenWay Adapter
- For the Landis+Gyr Adapter
- For the Sensus RNI Adapter
- For the Silver Spring Networks Adapter

For the Adapter Development Kit

The DG reference implementation SOA configurations include:

Menu Option	Name Used in this Documentation	Customer Install Value
DG SOA Partition Name	SOA_PARTITION_DG	DG
MR Server Endpoint URI	Headend_MR_Server_DG	
CD Server Endpoint URI	Headend_CD_Server_DG	
OD Server Endpoint URI	Headend_OD_Server_DG	
Headend Http Read Timeout	Headend_http_read_timeout_DG	
Headend Http Connection Timeout	Headend_http_conn_timeout_DG	

For the Networked Energy Services Adapter

The SOA configuration plan for Networked Energy Services (NES) includes:

Menu Option	Name Used in this Documentation	Customer Install Value
NES endpoint URI	HEADEND_NES	
The SOA partition to which the application is installed	SOA_PARTITION_D4	Echelon
The path to the NES EventManager web service on the head end system	HEADEND_EVENTMANAGER_D4	
The path to the NES GatewayManager web service	HEADEND_GATEWAYMANAGER_D4	
The path to the NES DeviceManager web service on the head end system	HEADEND_DEVICEMANAGER_D4	
The path to the NES SettingManager web service on the head end system	HEADEND_SETTINGMANAGER_D4	
The path to the NES UserManager web service on the head end system	HEADEND_USERMANAGER_D4	
The name of the OWSM policy to use when SOA calls a head end system	D4_SOA_HE_CLIENT_POLICY	
The name of the OWSM policy to use when SOA is called by a head end system	D4_SOA_HE_SERVICE_POLICY	

For the Itron OpenWay Adapter

The SOA configuration plan for Itron OpenWay includes the following menu options.

> **Note:** Replace localhost and port with respective host and port for the below mentioned Endpoint URLs.

Menu Option	Name Used in this Documentation	Customer Install Value
Itron SOA Partition Name	SOA_PARTITION_D8	Itron
Headend Http Read Timeout	HEADEND_HTTP_READ_TIMEOUT_D8	
Headend Http Connection Timeout	HEADEND_HTTP_CONN_TIMEOUT_D8	
DataSubscriberService Output Path	DATASUBSCRIBER_OUTPUT_PATH_D8	

Menu Option	Name Used in this Documentation	Customer Install Value
ExceptionSubscriberService Output Path	EXCEPTIONSUBSCRIBER_OUTPUT_PATH_D8	
Itron Headend DataService Endpoint URI	Headend_DataService_D8	
Itron Headend DiagnosticService Endpoint URI	Headend_DiagnosticService_D8	
Itron Headend UtilService Endpoint URI	Headend_UtilService_D8	
Itron Headend ControlService Endpoint URI	Headend_ControlService_D8	
Itron Headend ProvisioningService Endpoint URI	Headend_ProvisioningService_D8	
Itron Headend ProvisioningService370 Endpoint URI	Headend_ProvisioningService370_D8	
Itron Headend ControlService370 Endpoint URI	Headend_ControlService370_D8	
The name of the OWSM policy to use when SOA calls a head end system	D8_SOA_HE_CLIENT_POLICY	
The name of the OWSM policy to use when SOA is called by a head end system	D8_SOA_HE_SERVICE_POLICY	

For the Landis+Gyr Adapter

The SOA configuration plan for Landis+Gyr includes:

Menu Option	Name Used in this Documentation	Customer Install Value
LG SOA Partition Name	SOA_PARTITION_D3	LG
LG SOA TestHarness Partition Name	SOA_PARTITION_TEST_D3	
AMI Event Subscriber Output Path	AMIEVENTSUBSCRIBER_OUTPUT_PATH_D3	
MR_Server endpoint URI	Headend_MR_Server_D3	
CD_Server endpoint URI	Headend_CD_Server_D3	
CIM endpoint URI	Headend_CIM_Server_D3	

Menu Option	Name Used in this Documentation	Customer Install Value
Metering Server endpoint URI	Headend_Metering_Server_D3	
Security policy attached to outbound web service calls to a CIM interface	SOA_HE_CIM_ CLIENT_POLICY	
Security policy attached to inbound web service calls from a CIM interface	SOA_HE_CIM_ SERVICE_POLICY	
The name of the OWSM policy to use when SOA calls a head end system	D3_SOA_HE_ CLIENT_POLICY	
The name of the OWSM policy to use when SOA is called by a head end system	D3_SOA_HE_ SERVICE_POLICY	

For the Sensus RNI Adapter

The SOA configuration plan for Sensus RNI includes:

Menu Option	Name Used in this Documentation	Customer Install Value
Sensus SOA Partition Name	SOA_PARTITION_D6	Sensus
MR Server Endpoint URI	HEADEND_MR_D6	
CD Server Endpoint URI	HEADEND_CD_D6	
OD Server Endpoint URI	HEADEND_OD_D6	
Headend Http Read Timeout	Headend_http_read_timeout_D6	
Headend Http Connection Timeout	Headend_http_ conn_timeout_D6	
The name of the OWSM policy to use when SOA calls a head end system	D6_SOA_HE_ CLIENT_POLICY	
The name of the OWSM policy to use when SOA is called by a head end system	D6_SOA_HE_ SERVICE_POLICY	

For the Silver Spring Networks Adapter

SOA Configuration Plan (SSN)

The SOA configuration plan for SSN includes the following menu options.

Note: Replace localhost and port with your respective host and port for the Endpoint URLs listed below.

Menu Option	Name Used in this Documentation	Customer Install Value
SOA Partition Name	SOA_PARTITION_D7	
SOA Queue JNDI Name	SOA_QUEUE_D7	
Headend DataAggregation Endpoint URI	Headend_DataAggregation_Server_D7	
The url for the SSN 4.7 DataAggregation service (DataAggregation.asmx)	Headend_DataAggregation_47_Server_D7	
The url for the SSN 4.10 DataAggregation service	Headend_DataAggregation_410_Server_D7	
Headend DeviceManager Endpoint URI	Headend_DeviceManager_Server_D7	
The url for the SSN 4.7 DeviceManager service (DeviceManager.asmx)	Headend_DeviceManager_47_Server_D7	
The url for the SSN 4.10 DeviceManager service	Headend_DeviceManager_410_Server_D7	
Headend DeviceResults Endpoint URI	Headend_DeviceResults_Server_D7	
The url for the SSN 4.7 DeviceResults service (DeviceResults.asmx)	Headend_DeviceResults_47_Server_D7	
The url for the SSN 4.10 DeviceResults service	Headend_DeviceResults_410_Server_D7	
Headend JobManager Endpoint URI	Headend_JobManager_Server_D7	
The url for the SSN 4.7 JobManager service (JobManager.asmx)	Headend_JobManager_47_Server_D7	
The url for the SSN 4.10 JobManager service	Headend_JobManager_410_Server_D7	
The name of the OWSM policy to use when SOA calls a head end system	D7_SOA_HE_CLIENT_POLICY	

Menu Option	Name Used in this Documentation	Customer Install Value
The name of the OWSM policy to use when SOA is called by a head end system	D7_SOA_HE_ SERVICE_POLICY	

SSN JMS Source Destination Bridge Configuration

The SSN JMS source destination bridge configuration includes:

Parameter Description	Name Used in this Documentation	Customer Install Value
Source Bridge Destination Name	SRC_BRG_NAME_D7	
Classpath	SRC_BRG_CLASSPATH_D7	
Connection URL	SRC_BRG_CONN_URL_D7	
Initial Context Factory	SRC_BRG_INITIAL_CONTEXT_ D7	
Connection Factory JNDI Name	SRC_BRG_CONN_FACTORY_D7	
Destination Queue JNDI Name	SRC_BRG_QUEUE_JNDI_D7	
JMS Provider User Name	SRC_BRD_WLS_USER_D7	
JMS Provider User Password	SRC_BRD_WLS_PASS_D7	

Advance Menu Option for Test Harness Configuration

The advanced menu options are not available during installation. These options can be accessed after installation using the following commands:

UNIX

```
$SPLEBASE/bin/configureEnv.sh -a
```

Windows

```
%SPLEBASE%\bin\configureEnv.cmd -a
```

The SSN SOA testharness configurations include:

Parameter Description	Name used in this Document	Customer Install Value
TestHarness SOA Host Server	SOA_HOST_TEST_D7	
TestHarness SOA Port Server	SOA_PORT_NUMBER_TEST_D7	
SOA TestHarness Partition Name	SOA_PARTITION_TEST_D7	
SOA TestHarness Queue JNDI Name	SOA_QUEUE_TEST_D7	

Appendix C

Common Maintenance Activities

This appendix lists frequently-used commands that you use to perform common maintenance activities, such as starting and stopping the environment and thread pool worker, modifying the configuration items.

Run the following commands to perform the common tasks.

To Initialize the Environment

1. Navigate to the <install_dir>/bin directory.
2. Run the following command:

   UNIX

   ```
   ./splenviron.sh -e <Env_Name>
   ```

   Windows

   ```
   splenviron.cmd -e <Env_Name>
   ```

To Start the WebLogic Server

1. Initialize the environment.
2. Navigate to the respective domain's bin folder.
3. Execute the WebLogic Domain Startup command.

To Stop the WebLogic Server

1. Initialize the environment.
2. Navigate to the respective domain's bin folder.
3. Execute the WebLogic Domain Stop command.

To Start the Thread Pool Worker

1. Initialize the environment.
2. Run the following command:

   UNIX

   ```
   $SPLEBASE/bin/threadpoolworker.sh -d Y -p DEFAULT=20 L2OFF=1 -l2
   OFF
   ```

Windows

```
%SPLEBASE%\bin\threadpoolworker.cmd -d Y -p DEFAULT=20 L2OFF=1 -l2
OFF
```

To Stop the Thread Pool Worker

1. Initialize the environment.
2. Run the following command:

   UNIX

   ```
   ./spl.sh -b stop
   ```

   Windows

   ```
   spl.cmd -b stop
   ```

To Modify the Configuration Values

1. Initialize the environment.
2. Run the following command:

   UNIX

   ```
   configureEnv.sh
   ```

   Windows

   ```
   configureEnv.cmd
   ```

   The configuration utility launches menu items. Select any Menu option.

3. Change the menu values.
4. After you change the menu values, press **P** to write the changes to the configuration file.
5. To apply the changes to the environment, run the initial setup script:

   UNIX

   ```
   ./initialSetup.sh
   ```

   Windows

   ```
   initialSetup.cmd
   ```

To Modify the Advanced Menu Option Values

1. Initialize the environment.

   The configuration utility launches menu items.

2. Run the following command:

   UNIX

   ```
   configureEnv.sh -a
   ```

   Windows

   ```
   configureEnv.cmd -a
   ```

3. Select any menu option.

4. Change the menu values.
5. To apply the changes to the environment, run the following initial setup script:

   ```
   initialSetup.sh
   ```

Appendix D

Application Framework Prerequisite Patches

There are no Oracle Utilities Application Framework prerequisite patches to be installed in this release.