

Oracle Utilities Smart Grid Gateway

Installation Guide

Release 2.2.0

E80262-01

December 2016

Copyright © 2011, 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

Contents

Preface	i-i
Audience	i-i
Related Documents	i-i
Conventions	i-ii
Acronyms.....	i-ii
 Chapter 1	
Introduction	1-1
Installation Overview	1-2
Application Architecture	1-4
Tier 1: Desktop/Client, or Presentation Tier	1-4
Tier 2: Web Application Server, Business Application Server, Batch Server Tier.....	1-4
Tier 3: Database, or Persistence Tier	1-4
Installation Components	1-4
Installation Types	1-5
Initial Installation	1-5
Demo Installation	1-5
Upgrade Installation	1-6
Recommendations for Creating a Production Environment	1-6
Media Pack Components	1-7
Documentation Packages	1-7
Installation Packages.....	1-7
 Chapter 2	
Supported Platforms and Hardware Requirements	2-1
Software and Hardware Considerations	2-2
Operating Systems and Application Servers	2-3
Hardware Requirements.....	2-4
Application Server Memory Requirements	2-4
Additional Notes on Supported Platforms.....	2-5
Support for Software Patches and Upgrades	2-5
 Chapter 3	
Planning the Installation	3-1
Before You Install	3-2
Application Server Clustering	3-2
Prerequisite Software List	3-2
Prerequisite Software for Database Server.....	3-2
Prerequisite Software for Application Server	3-2
Web Browser Requirements.....	3-3
AIX 7.1 TL01+/AIX 7.2 TL00+ Application Server.....	3-4
Oracle Linux 6.5+/7.x or Red Hat Linux 6.5+/7.x Operating System	3-8
Oracle Solaris 11 Application Server	3-12

Windows Server 2012 R2 Application Server.....	3-15
Readiness Checklist	3-17
Chapter 4	
Installing Oracle Utilities Smart Grid Gateway—Initial Installation.....	4-1
Before You Install	4-1
Initial Installation Procedure	4-1
Database Component Installation.....	4-1
Application Components Installation.....	4-2
After the Installation.....	4-22
Chapter 5	
Installing Oracle Utilities Smart Grid Gateway—Demo Installation	5-1
Before You Install	5-1
Demo Installation Procedure	5-1
Database Component Installation.....	5-1
Application Components Installation.....	5-2
After the Installation.....	5-21
Chapter 6	
Installing Oracle Utilities Smart Grid Gateway—Upgrade Installation	6-1
Before You Upgrade.....	6-1
Upgrade Procedure	6-1
Database Component Upgrade	6-1
Application Components Upgrade	6-2
Operating the Application.....	6-23
Chapter 7	
Configuring the Oracle Utilities Smart Grid Gateway Adapters	7-1
Configuration Tasks for the MV90 Adapter.....	7-2
Deploying the OSB Adapter for the MV90.....	7-2
Starting the Application	7-5
Configuration Tasks for the Adapter Development Kit.....	7-6
Deploying the OSB Adapter for the Adapter Development Kit	7-6
Deploying the SOA Adapter for the Adapter Development Kit.....	7-9
Configuring Security for the SOA System	7-14
Starting the Application	7-19
Configuration Tasks for the Adapter for Networked Energy Services	7-20
Deploying the OSB Adapter for Networked Energy Services	7-20
Deploying the SOA Adapter for Networked Energy Services	7-23
Deploying the Test Harness.....	7-25
Configuring the Networked Energy Services Head-End System to Report Events	7-26
Configuring Security for the SOA System	7-28
Starting the Application	7-33
Configuration Tasks for the Adapter for Itron OpenWay	7-34
Deploying the OSB Adapter for the Itron OpenWay.....	7-34
Deploying the SOA Adapter for the Itron OpenWay	7-37
Configuring Security for the SOA System	7-40
Starting the Application	7-42
Configuration Tasks for the Adapter for Landis+Gyr.....	7-43
Deploying the OSB Adapter for Landis+Gyr.....	7-43
Deploying the SOA Adapter for Landis+Gyr.....	7-46
Configuring Security for the SOA System	7-49
Starting the Application	7-54
Configuration Tasks for the Adapter for Sensus RNI.....	7-55
Deploying the OSB Adapter for Sensus RNI	7-55
Deploying the SOA Adapter for Sensus RNI	7-58

Configuring Security for the SOA System	7-63
Starting the Application	7-67
Configuration Tasks for the Adapter for Silver Spring Networks.....	7-69
Deploying the OSB Adapter for Silver Spring Networks.....	7-69
Deploying the SOA Adapter for Silver Spring Networks	7-72
Configuring Security for the SOA System	7-79
Starting the Application	7-81
Operating the Application	7-81
Creating an OSB Example Domain	7-82
Creating a SOA Example Domain	7-82
Chapter 8	
Installing Oracle Utilities Service Order Management	8-1
Installation Overview	8-1
Initial Installation	8-1
Demo Installation	8-2
Chapter 9	
Additional Tasks	9-1
Importing Self-Signed Certificates	9-2
Customizing Configuration Files	9-2
Integrating Existing Customer Modifications	9-2
Generating the Application Viewer	9-3
Building Javadocs Indexes	9-3
Configuring the Environment for Batch Processing	9-3
Customizing the Logo	9-4
Configuring Secure Sockets Layer (SSL).....	9-4
Setting Up an Application Keystore	9-5
Domain Templates (Linux Weblogic 12.1.3.0+ only)	9-6
Database Patching	9-8
Appendix A	
Installation Menu Functionality	A-1
Installation Menu Functionality Overview	A-1
Installation Menu Functionality Details	A-1
.....	A-2
Appendix B	
Installation and Configuration Worksheets	B-1
Application Framework Installation and Configuration Worksheets	B-1
Environment ID, Roles, Third Party Software Configuration	B-2
Keystore Options	B-4
Environment Installation Options	B-5
Environment Description.....	B-7
WebLogic Business Application Server Configuration.....	B-8
WebLogic Web Application Server Configuration	B-9
Database Configuration	B-11
General Configuration Options.....	B-14
SSL Certificate Keystore (Weblogic Only).....	B-16
OUAF TrustStore Options	B-17
Advanced Menu Options.....	B-19
WebLogic Advanced Environment Memory Configuration	B-22
Advanced Web Application Configuration.....	B-24
WebLogic Diagnostics	B-27
OIM Configuration Settings.....	B-27
Cloud Related Options.....	B-28
.....	B-29

Service and Measurement Data Foundation Installation and Configuration Worksheets.....	B-30
WebLogic OSB Configuration.....	B-30
WebLogic SOA Configuration	B-33
WebLogic SOA Configuration Plan	B-35
Configuration for DataRaker Integration.....	B-36
Advanced Menu Options.....	B-38
Smart Grid Gateway Installation and Configuration Worksheets	B-43
For the Adapter Development Kit.....	B-43
For the Adapter for Networked Energy Services	B-45
For the Adapter for Itron OpenWay	B-47
For the Adapter for Landis+Gyr.....	B-50
For the Adapter for Sensus RNI	B-52
For the Adapter for Silver Spring Networks	B-54
 Appendix C	
Common Maintenance Activities	C-1
 Appendix D	
Oracle Utilities Application Framework 4.3.0 Service Pack 3 (4.3.0.3.0) Fixes.....	D-1

Preface

This guide describes how to install Oracle Utilities Smart Grid Gateway, including:

- [Audience](#)
- [Related Documents](#)
- [Conventions](#)
- [Acronyms](#)

Audience

Oracle Utilities Smart Grid Gateway Installation Guide is intended for system administrators installing Oracle Utilities Smart Grid Gateway.

To use this document you should have:

- Experience installing and configuring application servers and other software
- Administrative privileges on the host where you are installing the 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 Guide*
- *Oracle Utilities Smart Grid Gateway Licensing Information User Manual*

Configuration and User Guides

- *Oracle Utilities Meter Data Management / Oracle Utilities Smart Grid Gateway V2.2.0 Business User Guide*
- *Oracle Utilities Meter Data Management / Oracle Utilities Smart Grid Gateway V2.2.0 Administrative User Guide*

Supplemental Documents

-
- *Oracle Utilities Smart Grid Gateway Server Administration Guide*
 - *Oracle Utilities Smart Grid Gateway Security Guide*

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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

Acronym	Definition
Oracle RAC FCF	Oracle Real Application Clusters Fast Connection Failover
RMI	Remote Method Invocation
SOAP	Simple Object Access Protocol
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

Chapter 1

Introduction

This chapter provides an overview of the installation of Oracle Utilities Smart Grid Gateway. 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:

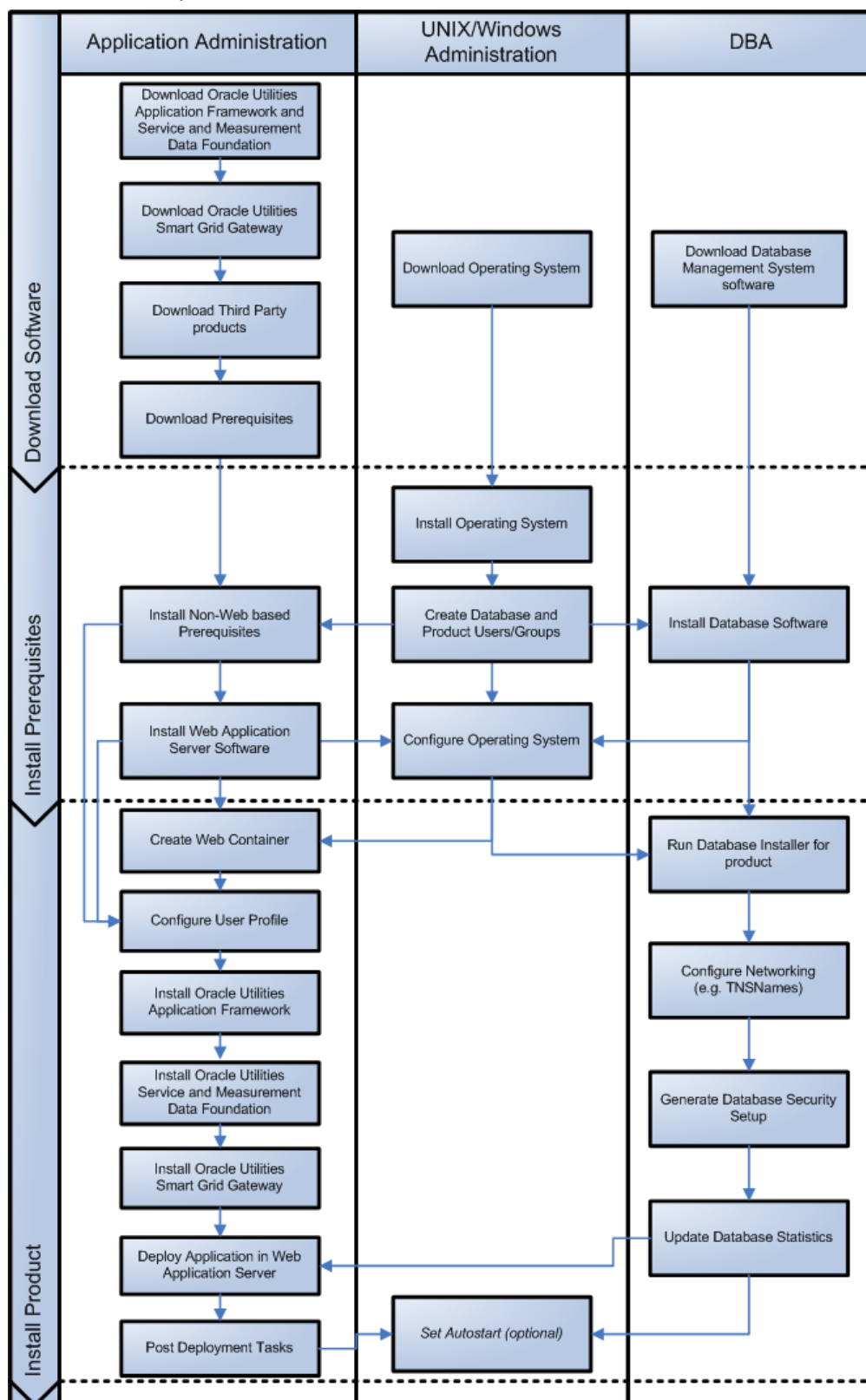
Note: For installing of Oracle Utilities Service Order Management, please refer to chapter [Installing Oracle Utilities Service Order Management](#).

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 document *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 document *Oracle Utilities Smart Grid Gateway Database Administrator's Guide*.
5. Install all required third-party software as described in [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 the Oracle Utilities Service and Measurement Data Foundation for the application.
8. Install Oracle Utilities Smart Grid Gateway.
9. 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](#).
10. 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 Architecture

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

Please see the Oracle Utilities Smart Grid Gateway *Server Administration Guide* 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 will also run within this tier. You can have multiple batch server instances that serve 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 Service and Measurement Data Foundation database
 - Oracle Utilities Smart Grid Gateway database
- Application Components:
 - Oracle Utilities Application Framework application
 - Oracle Utilities Service and Measurement Data Foundation application
 - Oracle Utilities Smart Grid Gateway 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 version 2.1.0.3 to version 2.2.0.

Please 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 of the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for more information.
- Application components:
 - Oracle Utilities Application Framework application
 - Oracle Utilities Application Framework Single Fix Pre-Requisite Rollup for Oracle Utilities Service and Measurement Data Foundation
 - Oracle Utilities Service and Measurement Data Foundation application
 - Oracle Utilities Smart Grid Gateway application

See [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 of the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide* for more information.
- Application components:
 - Oracle Utilities Application Framework application
 - Oracle Utilities Application Framework Single Fix Pre-Requisite Rollup for Oracle Utilities Service and Measurement Data Foundation
 - Oracle Utilities Service and Measurement Data Foundation application
 - Oracle Utilities Smart Grid Gateway application

See [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 version 2.1.0.3 to 2.2.0.

Note: If you have a version prior to 2.1.0.3, you must upgrade to 2.1.0.3 before upgrading to 2.2.0.

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

- Database components:
Refer to the “Upgrade Install” section of the Oracle Utilities Smart Grid Gateway *Database Administrator's Guide* for more information.
- Application components:
 - Oracle Utilities Application Framework application
 - Oracle Utilities Application Framework Single Fix Pre-Requisite Rollup for Oracle Utilities Service and Measurement Data Foundation
 - Oracle Utilities Service and Measurement Data Foundation application
 - Oracle Utilities Smart Grid Gateway application

See [Installing Oracle Utilities Smart Grid Gateway—Upgrade Installation](#) for the instructions for installing 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). Please refer to the appendix “Configuration Migration Assistant” in the Oracle Utilities Smart Grid Gateway *Configuration Guide* for more details about 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 V2.2.0 Release Notes*
- *Oracle Utilities Smart Grid Gateway V2.2.0 Quick Install Guide*
- *Oracle Utilities Smart Grid Gateway V2.2.0 Install Documentation*
- *Oracle Utilities Smart Grid Gateway V2.2.0 User Documentation*
- *Oracle Utilities Smart Grid Gateway V2.2.0 Supplemental Documentation*
- *Oracle Utilities Service Order Management V2.2.0 User Documentation*

Installation Packages

- Oracle Utilities Application Framework V4.3.0 Service Pack 3 Multiplatform
- Oracle Utilities Application Framework V4.3.0 Service Pack 3 Single Fix Prerequisite Rollup for SMDF V2.2.0
- Oracle Utilities Service and Measurement Data Foundation V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway V2.2.0 Oracle Database Multiplatform
- Oracle Utilities Smart Grid Gateway MV-90 Adapter for Itron V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter Development Kit V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter for NES V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter for Landis+Gyr V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter for Sensus RNI V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Adapter for Silver Spring Networks V2.2.0 Multiplatform
- Oracle Utilities Smart Grid Gateway Integration for Outage Operations Release V2.2.0

Chapter 2

Supported Platforms and Hardware Requirements

This section gives 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. It includes:

- [Software and Hardware Considerations](#)
- [Operating Systems and Application Servers](#)
- [Hardware Requirements](#)
- [Application Server Memory Requirements](#)
- [Additional Notes on Supported Platforms](#)
- [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, please see the document *Oracle Utilities Application Framework Architecture Guidelines*, available on My Oracle Support (Article ID 807068.1).

The final hardware and software decisions must comply with the specific requirements of Oracle Utilities Smart Grid Gateway, as described in the rest of this chapter.

Operating Systems and Application Servers

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

Oracle Utilities Smart Grid Gateway and Adapters

Operating System and Web Browser (Client)	Operating System (Server)	Chipset	Application Server	Database
Windows 7, 8.1, 10 (Internet Explorer 11, Firefox ESR 45)	AIX 7.1 TL01+	POWER	WebLogic	Oracle 12.1.0.1+
	AIX 7.2 TL00+	64-bit	12.1.3.0+*	
	Oracle Linux 6.5+, 7.x (64-bit) (based on Red Hat Enterprise Linux (64-bit))**	x86_64	WebLogic 12.1.3.0+*	Oracle 12.1.0.1+
	Oracle Solaris 11 (64-bit)	SPARC	WebLogic 12.1.3.0+*	Oracle 12.1.0.1+
	Windows Server 2012 R2 (64-bit)	x86_64	WebLogic 12.1.3.0+*	Oracle 12.1.0.1+

Note: Oracle Utilities Service Order Management only supports WebLogic version 12.1.3.0+.

Oracle Utilities Smart Grid Gateway OSB and SOA Adapters

Adapter	Operating System (Server)	Chipset	Application Server	Database
OSB Adapters SOA Adapters (Not applicable for MV90 Adapter for Itron)	AIX 7.1 TL01+	POWER	WebLogic	Oracle 12.1.0.1+
	AIX 7.2 TL00+	64-bit	12.2.1.0	
	Oracle Linux 6.5+, 7.x (64-bit) (based on Red Hat Enterprise Linux (64-bit))**	x86_64	WebLogic 12.2.1.0	Oracle 12.1.0.1+
	Oracle Solaris 11 (64-bit)	SPARC	WebLogic 12.2.1.0	Oracle 12.1.0.1+
	Windows Server 2012 R2 (64-bit)	x86_64	WebLogic 12.2.1.0	Oracle 12.1.0.1+

* A plus sign (+) after the fourth digit in the version number indicates that this and all higher versions of WebLogic are supported. For example, 12.1.3.0+ means that 12.1.3.0 and any higher 12.1.3.x.x versions are supported.

WebLogic 12.1.3.0+ is currently supported for both embedded and native installations. In future releases of the application, using a later version of WebLogic, for example 12.2.*, embedded installations will not be supported. Only the native installation will be supported.

** Oracle Utilities Smart Grid Gateway is supported on the versions of Oracle Linux specified. Because Oracle Linux is 100% userspace-compatible with Red Hat Enterprise Linux, Oracle Utilities Smart Grid Gateway also is supported on Red Hat Enterprise Linux for this release.

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**.

The platforms listed above are current at the time of release. For the most current supported platforms, please refer to Oracle Utilities Product Matrix on My Oracle Support (MOS) Knowledge Article (Doc ID 1454143.1).

Hardware Requirements

Client Side Hardware Requirements

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.

Disk Space Requirements

The approximate disk space requirements in a standard installation are as follows:

Location	Size	Usage
Install_dir Location	5 GB minimum	This location is 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.
Log Location	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	Size	Usage
Location of the application web work files on the web servers	1.5 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	4 GB	The application gets installed from this location. You need enough space to uncompress the files and install the application.
Oracle data area	4 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.

Additional Notes on Supported Platforms

Oracle Database Server

This version of Oracle Utilities Smart Grid Gateway is supported on Oracle Database Server 12.1.0.1+ on operating systems listed in above section. The following versions of the database are supported:

- Oracle Database Enterprise Edition

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

Oracle WebLogic Server Information

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*.

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.

Oracle Support Policy on VMWare

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

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 from this rule is Hibernate software version 4.1.0. This version 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](#)
- [Readiness Checklist](#)

Before You Install

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

Application Server Clustering

If you are considering application server clustering, refer to the following whitepaper, available on My Oracle Support, for additional information:

- Implementing Oracle ExaLogic and/or Oracle WebLogic Clustering (Doc Id: 1334558.1)

Additional information about Weblogic clustering can be found at http://docs.oracle.com/cd/E17904_01/web.1111/e13709/toc.htm

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 12.1.0.1+** - 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

Note: 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 12c Client
- JDK 1.8.0_92+ (64-bit)
- Oracle WebLogic 12c (12.1.3.0+)
- Hibernate 4.1.0 Final
- Oracle Service Bus 12.2.1.0

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 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0

- Oracle SOA Suite 12.2.1.0

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

Note: Oracle SOA Suite 12.2.1.0 requires Oracle WebLogic Server (12.2.1.0).

Note: Oracle Utilities Service Order Management only supports Oracle Service Bus/Oracle SOA Suite 12.2.1.0

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:

Browsers	Windows OS
Internet Explorer 11 Firefox ESR 45	Windows OS 7, 8.1, 10 (64-bit)

Installing Prerequisite Software

This chapter 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 TL01+/AIX 7.2 TL00+ Application Server](#)
- [Oracle Linux 6.5+/7.x or Red Hat Linux 6.5+/7.x Operating System](#)
- [Oracle Solaris 11 Application Server](#)
- [Windows Server 2012 R2 Application Server](#)

AIX 7.1 TL01+/AIX 7.2 TL00+ 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 TL01+ AIX 7.2 TL00+	POWER 64-bit	Oracle WebLogic 12c (12.1.3.0+) 64-bit

AIX 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 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 12c — 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 version 8.0 SR15 64-bit, IBM SDK, Java Technology Edition, Version 8.0

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), ensure 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 4.1.0 before installing Oracle Utilities Smart Grid Gateway.

To install Hibernate:

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/
```

Click the “4.1.0.Final” link to download the zip file.

3. Extract the contents of the archive file:

```
jar xvf hibernate-release-4.1.0.Final.zip
```

Note: You must have Java JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

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

```
copy hibernate-release-4.1.0.Final/lib/optional/
ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/optional/
ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
copy 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 (12.1.3.0+) 64-bit

Oracle WebLogic software can be downloaded from the Oracle web site. 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 Server.

Oracle Service Bus 12.2.1.0

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

Note: Oracle Service Bus 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

Oracle SOA Suite 12.2.1.0

Oracle SOA Suite, specifically BPEL Process Manager, is required for an implementation that plans to use a productized adapter or the generic adapter to implement two-way communications for processing meter commands.

Note: Oracle SOA Suite 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

Oracle Linux 6.5+/7.x or Red Hat Linux 6.5+/7.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 6.5+,7.x (64-bit) based on Red Hat Enterprise Linux (64-bit)	x86_64	Oracle WebLogic 12c (12.1.3.0+) 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 12c — 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 Version 8.0 Update 92+, 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 4.1.0 before installing Oracle Utilities Smart Grid Gateway.

To install Hibernate:

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/>

Click the “4.1.0.Final” link to download the zip file.

3. Extract the contents of the archive file:

```
jar xvf hibernate-release-4.1.0.Final.zip
```

Note: You must have Java JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

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

```
copy hibernate-release-4.1.0.Final/lib/optional/
ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/optional/
ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
copy 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 (12.1.3.0+) 64-bit

Oracle WebLogic software can be downloaded from the Oracle web site. 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 Server.

Oracle Service Bus 12.2.1.0

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

Note: Oracle Service Bus 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

Oracle SOA Suite 12.2.1.0

Oracle SOA Suite, specifically BPEL Process Manager, is required for an implementation that plans to use a productized adapter or the generic adapter to implement two-way communications for processing meter commands.

Note: Oracle SOA Suite 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

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 (12.1.3.0+) 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 12c — 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 Version 8.0 Update 92+, 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 4.1.0 before installing Oracle Utilities Smart Grid Gateway.

To install Hibernate:

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/
```

Click the “4.1.0.Final” link to download the zip file.
3. Extract the contents of the archive file:

```
jar xvf hibernate-release-4.1.0.Final.zip
```

Note: You must have Java JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

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

```
copy hibernate-release-4.1.0.Final/lib/optional/
    ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/optional/
    ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
    hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
    hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
    hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
    javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
copy hibernate-release-4.1.0.Final/lib/required/
    jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
copy 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 (12.1.3.0+) 64-bit

Oracle WebLogic software can be downloaded from the Oracle web site. 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 Server.

Oracle Service Bus 12.2.1.0

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

Note: Oracle Service Bus 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

Oracle SOA Suite 12.2.1.0

Oracle SOA Suite, specifically BPEL Process Manager, is required for an implementation that plans to use a productized adapter or the generic adapter to implement two-way communications for processing meter commands.

Note: Oracle SOA Suite 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

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 (12.1.3.0+) 64-bit

Web/Application Server Tier

Oracle Client 12c — 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 Version 8.0 Update 92+, 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 4.1.0 before installing Oracle Utilities Smart Grid Gateway.

To install Hibernate:

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/>

Click the “4.1.0.Final” link to download the zip file.

3. Extract the contents of the archive file:

```
jar xvf hibernate-release-4.1.0.Final.zip
```

Note: You must have Java JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

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

```
copy hibernate-release-4.1.0.Final\lib\optional\
ehcache\ehcache-core-2.4.3.jar %HIBERNATE_JAR_DIR%
copy hibernate-release-4.1.0.Final\lib\optional\
ehcache\hibernate-ehcache-4.1.0.Final.jar %HIBERNATE_JAR_DIR%
```

```

copy hibernate-release-4.1.0.Final\lib\required\
  hibernate-commons-annotations-4.0.1.Final.jar
%HIBERNATE_JAR_DIR%
copy hibernate-release-4.1.0.Final\lib\required\
  hibernate-core-4.1.0.Final.jar %HIBERNATE_JAR_DIR%
copy hibernate-release-4.1.0.Final\lib\required\
  hibernate-jpa-2.0-api-1.0.1.Final.jar %HIBERNATE_JAR_DIR%
copy hibernate-release-4.1.0.Final\lib\required\
  javassist-3.15.0-GA.jar %HIBERNATE_JAR_DIR%
copy hibernate-release-4.1.0.Final\lib\required\
  jboss-logging-3.1.0.CR2.jar %HIBERNATE_JAR_DIR%
copy 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 (12.1.3.0+) 64-bit

Oracle WebLogic software can be downloaded from the Oracle web site. 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 Server.

Oracle Service Bus 12.2.1.0

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

Note: Oracle Service Bus 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

Oracle SOA Suite 12.2.1.0

Oracle SOA Suite, specifically BPEL Process Manager, is required for an implementation that plans to use a productized adapter or the generic adapter to implement two-way communications for processing meter commands.

Note: Oracle SOA Suite 12.2.1.0 requires Oracle WebLogic Server 12.2.1.0.

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 download web site:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html>

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 [Operating Systems and Application Servers](#) for more details.
2. Install prerequisite software. Refer to the [Installing Prerequisite Software](#) for more details.
3. Ensure that you have downloaded the Oracle Utilities Smart Grid Gateway V2.2.0 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 for installing Oracle Utilities Smart Grid Gateway for the first time or from scratch. This chapter includes:

- [Before You Install](#)
- [Initial 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.

Initial 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. Refer to the section “**Initial Install**” of the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide*, which provides instructions on installing the database component.

Application Components Installation

A successful installation consists of the following steps:

- [Installing the Oracle Utilities Application Framework V4.3.0 Service Pack 3 \(4.3.0.3\) Application Component](#)
- [Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDf V2.2.0](#)
- [Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component](#)
- [Installing the Oracle Utilities Smart Grid Gateway Application Component](#)

Installing the Oracle Utilities Application Framework V4.3.0 Service Pack 3 (4.3.0.3) 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 V4.3.0 Service Pack 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 V4.3.0 Service Pack 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, follow these steps:

1. Log in to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.3.0.3.0 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-V4.3.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
5. Decompress the file:

```
cd <TEMPDIR>
jar -xvf FW-V4.3.0.3.0-MultiPlatform.jar
```

Note: You will need to have Java JDK installed on the machine used to (un)jar the application server installation package. Please install the JDK that is supported for the install on your platform to be able to use the jar command. This is the location of Java packages: <http://www.oracle.com/technetwork/java/archive-139210.html>

A sub-directory named “FW.V4.3.0.3.0” 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>/FW.V4.3.0.3.0` 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 4.3.0 Service Pack 3.

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 `<TEMPDIR>/FW.V4.3.0.3.0` directory.
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:${PERL_HOME}/lib/site_perl:<OUAF
    Installer Decompressed location/bin/perl>
export PERLLIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
    Installer Decompressed location/bin/perl>
export LD_LIBRARY_PATH=${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
```

5. The Oracle Utilities Application Framework specific menu appears.
6. Follow the messages and instructions that are produced by the application installation utility.
7. Select each menu item to configure the values. For detailed description of the values, refer to [Appendix B: Installation and Configuration Worksheets](#).
8. 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. Third Party Software Configuration
   Oracle Client Home Directory: <Mandatory>
   Web Java Home Directory:      <Mandatory>
   Child JVM Home Directory:
   COBOL Home Directory:
   Hibernate JAR Directory: <Mandatory>
   ONS JAR Directory:
   Web Application Server Home Directory: <Mandatory>
   ADF Home Directory:
   OIM OAM Enabled Environment:

2. Keystore Options
   Store Type:                      JCEKS
   Alias:                          ouaf.system
   Alias Key Algorithm:             AES
   Alias Key Size:                 128
   HMAC Alias:                     ouaf.system.hmac
   Padding:                        PKCS5Padding
   Mode:                           CBC

50. Environment Installation Options
   Environment Mount Point: <Mandatory> - Install Location
   Log Files Mount Point: <Mandatory> - ThreadPoolWorker Logs
                                   Location

   Environment Name: <Mandatory>
   Web Application Server Type:                      WLS
   Install Application Viewer Module:                true
```

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

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

9. 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
   WebLogic Server Name:        myserver
   Business Server Application Name: SPLService
   MPL Admin Port Number:       <Mandatory> - Multipurpose Listener
                                   Port
   MPL Automatic startup:       false
```

3. Web Application Server Configuration

Web Server Host: <Mandatory>
Web Server Port Number: <Mandatory>
Web Context Root: ouaf
WebLogic JNDI User ID: <Mandatory>
WebLogic JNDI Password: <Mandatory>
WebLogic Admin System User ID: <Mandatory>
WebLogic Admin System Password: <Mandatory>
WebLogic Server Name: myserver
Web Server Application Name: SPLWeb
Application Admin User ID: <Mandatory>
Application Admin Password: <Mandatory>
Expanded Directories: false
Application Viewer Module: true

4. Database Configuration

Application Server Database User ID: <Mandatory>
Application Server Database Password: <Mandatory>
MPL Database User ID: <Mandatory>
MPL Database Password: <Mandatory>
XAI Database User ID: <Mandatory>
XAI Database Password: <Mandatory>
Batch Database User ID: <Mandatory>
Batch Database Password: <Mandatory>
Database Name: <Mandatory>
Database Server: <Mandatory>
Database Port: <Mandatory>
ONS Server Configuration:
Database Override Connection String:
Oracle Client Character Set NLS_LANG:

5. General Configuration Options

Batch RMI Port: <Mandatory> - RMI port
for batch
Batch Mode: <Mandatory> - CLUSTERED
or DISTRIBUTED
Coherence Cluster Name: <Mandatory> - Unique
name for batch
Coherence Cluster Address: <Mandatory> - Unique
Multicast address
Coherence Cluster Port: <Mandatory> - Unique
port for batch cluster
Coherence Cluster Mode: <Mandatory> - prod

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

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

10. When you are done with the parameter setup, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.
11. Once the install has finished, the installation log location appears 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. You can now install Oracle Utilities Service and Measurement Data Foundation as described in the following section.

Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite

Rollup for SMDF V2.2.0

1. Create a <TEMPDIR> directory on the host server that is independent of any current or other working application environment.
2. Copy the file "Oracle Utilities Application Framework V4.3.0 Service Pack 3 Single Fix Prerequisite Rollup.zip" in the delivered package to <TEMPDIR>.

If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
3. Upon extracting the zip, file 'Application-Server-Multiplatform' sub-directory will be created.
4. Refer to the Readme.txt inside 'Application-Server-Multiplatform' file for instructions on installing the Oracle Utilities Application Framework 4.3.0 Service Pack 3 Prerequisite Single Fixes.

These patches are also available for download separately from My Oracle Support.

See [Appendix D](#) for a list of the patches contained in the rollup.

Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component

This section describes how to install the application component of Oracle Utilities Service and Measurement Data Foundation, including:

- [Copying and Decompressing Install Media](#)
- [Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0](#)
- [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#)

Copying and Decompressing Install Media

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

The Oracle Utilities Service and Measurement Data Foundation is delivered as a separate installation package. Please refer to the chapter [Supported Platforms and Hardware Requirements](#) for installation details regarding the database and operating system versions supported for the Service and Measurement Data Foundation. Also see the section [Installing Prerequisite Software](#) for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Log in 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.
2. Create a <TEMPDIR> directory on the application server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Application Framework.
3. Copy the file SMDF-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your application server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SMDF-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a sub-directory named MDF.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0

This section outlines the steps for installing the Service and Measurement Data Foundation:

Preparing for the Installation

1. Log on as Oracle Utilities Service and Measurement Data Foundation Administrator (default cissys).
2. Initialize the Framework environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Application

1. Change to the <TEMPDIR>/MDF.V2.2.0 directory.
2. Execute the script:

UNIX:

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

Windows:

```
install.cmd
```

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

The configuration menu for the Oracle Utilities Service and Measurement Data Foundation Application appears.

3. Select menu item 8 to configure OSB.
Use the completed OSB configuration worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
4. Select menu item 9 to configure SOA.
Use the completed SOA configuration worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
5. Select menu item 10 to configure the SOA Configuration Plan.
Use the completed SOA Configuration Plan (MDF) worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
6. When you are done with the parameter setup, choose option P to proceed with the installation.

Installation of Oracle Utilities Service and Measurement Data Foundation Application Server is complete if no errors occurred during installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation

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 Service and Measurement Data Foundation:

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.

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 Service and Measurement Data Foundation.

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.

Installing the Oracle Utilities Smart Grid Gateway Application Component

This section describes how to install the application component 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](#)

Installing the MV90 Adapter for Itron

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

- [Preinstallation Tasks for the MV90 Adapter](#)
- [Installing the MV90 Adapter](#)

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

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-MV90-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-MV90-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named MV90.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the MV90 Adapter - To install the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Change to the <TEMPDIR>/MV90.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.cmd
```

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

3. Choose option P to proceed with the installation.

Once the install has finished successfully, execute the postinstallation 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:

- [Preinstallation Tasks for the Adapter Development Kit](#)
- [Installation Tasks for the Adapter Development Kit](#)

Preinstallation Tasks for the Adapter Development Kit - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-DG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-DG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named DG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installation Tasks for the Adapter Development Kit - This section describes the installation of the Adapter Development Kit, including:

- [Initializing the Service and Measurement Data Foundation](#)
- [Installing the Adapter Development Kit](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Adapter Development Kit

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

1. Change to the <TEMPDIR>/DG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See **Smart Grid Gateway Installation and Configuration Worksheets** on page 4-46.

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Networked Energy Services](#)
- [Installing the Adapter for Networked Energy Services](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D4-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D4-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D4.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation -

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D4.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

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:

- [Preinstallation Tasks for the Adapter for Itron OpenWay](#)
- [Installation Tasks for the Adapter for Itron OpenWay](#)

Preinstallation Tasks for the Adapter for Itron OpenWay - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D8-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D8-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D8.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Installing the Adapter for Itron OpenWay](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).

-
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Adapter for Itron OpenWay

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

1. Change to the <TEMPDIR>/D8.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Landis+Gyr](#)
- [Installing the Adapter for Landis+Gyr](#)

Preinstallation Tasks for the Adapter for Landis+Gyr - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-LG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-LG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named LG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/LG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).
4. When you are done setting up the parameters, choose option P to proceed with the installation.

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Sensus RNI](#)
- [Installing the Adapter for Sensus RNI](#)

Preinstallation Tasks for the Adapter for Sensus RNI - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D6-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-D6-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D6.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D6.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Silver Spring Networks](#)
- [Installing the Adapter for Silver Spring Networks](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D7-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-D7-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D7.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D7.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

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 following section.

Chapter 5

Installing Oracle Utilities Smart Grid Gateway— Demo Installation

This chapter provides instructions for setting up a demo application of Oracle Utilities Smart Grid Gateway for demonstration or training purposes. This chapter includes:

- [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. Refer to the section “**Demo Install**” of the *Oracle Utilities Smart Grid Gateway Database Administrator's Guide*, which provides instructions on installing the database component.

Application Components Installation

A successful installation consists of the following steps:

- [Installing the Oracle Utilities Application Framework Application V4.3.0 Service Pack 3 \(4.3.0.3 Component\)](#)
- [Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDP V2.2.0](#)
- [Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component](#)
- [Installing the Oracle Utilities Smart Grid Gateway Application Component](#)

Installing the Oracle Utilities Application Framework Application V4.3.0 Service Pack 3 (4.3.0.3 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 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, follow these steps:

1. Log in to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.3.0.3.0 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-V4.3.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
5. Decompress the file:

```
cd <TEMPDIR>
jar -xvf FW-V4.3.0.3.0-MultiPlatform.jar
```

Note: You will need to have Java JDK installed on the machine used to (un)jar the application server installation package. Please install the JDK that is supported for the install on your platform to be able to use the jar command. This is the location of Java packages: <http://www.oracle.com/technetwork/java/archive-139210.html>

A sub-directory named “FW.V4.3.0.3.0” 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>/FW.V4.3.0.3.0 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 V4.3.0 Service Pack 3.

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 <TEMPDIR>/FW.V4.3.0.3.0 directory.
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:${PERL_HOME}/lib/site_perl:<OUAF
    Installer Decompressed location/bin/perl>
export PERLLIB=${PERL_HOME}/lib:${PERL_HOME}/lib/site_perl:<OUAF
    Installer Decompressed location/bin/perl>
export LD_LIBRARY_PATH=${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
```

5. The Oracle Utilities Application Framework specific menu appears.
6. Follow the messages and instructions that are produced by the application installation utility.
7. Select each menu item to configure the values. For detailed description of the values, refer to [Appendix B: Installation and Configuration Worksheets](#).
8. 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. Third Party Software Configuration
   Oracle Client Home Directory: <Mandatory>
   Web Java Home Directory:      <Mandatory>
   Child JVM Home Directory:
   COBOL Home Directory:
   Hibernate JAR Directory: <Mandatory>
   ONS JAR Directory:
   Web Application Server Home Directory: <Mandatory>
   ADF Home Directory:
   OIM OAM Enabled Environment:

2. Keystore Options
   Store Type:                      JCEKS
   Alias:                          ouaf.system
   Alias Key Algorithm:             AES
   Alias Key Size:                 128
   HMAC Alias:                     ouaf.system.hmac
   Padding:                        PKCS5Padding
   Mode:                           CBC

50. Environment Installation Options
   Environment Mount Point: <Mandatory> - Install Location
   Log Files Mount Point:<Mandatory> - ThreadPoolWorker Logs
                                   Location

   Environment Name:<Mandatory>
   Web Application Server Type:      WLS
   Install Application Viewer Module: true
```

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

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

9. 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
   WebLogic Server Name:        myserver
   Business Server Application Name: SPLService
   MPL Admin Port Number:       <Mandatory> - Multipurpose Listener
                                   Port
   MPL Automatic startup:       false
```

3. Web Application Server Configuration

Web Server Host: <Mandatory>
Web Server Port Number: <Mandatory>
Web Context Root: ouaf
WebLogic JNDI User ID: <Mandatory>
WebLogic JNDI Password: <Mandatory>
WebLogic Admin System User ID: <Mandatory>
WebLogic Admin System Password: <Mandatory>
WebLogic Server Name: myserver
Web Server Application Name: SPLWeb
Application Admin User ID: <Mandatory>
Application Admin Password: <Mandatory>
Expanded Directories: false
Application Viewer Module: true

4. Database Configuration

Application Server Database User ID: <Mandatory>
Application Server Database Password: <Mandatory>
MPL Database User ID: <Mandatory>
MPL Database Password: <Mandatory>
XAI Database User ID: <Mandatory>
XAI Database Password: <Mandatory>
Batch Database User ID: <Mandatory>
Batch Database Password: <Mandatory>
Database Name: <Mandatory>
Database Server: <Mandatory>
Database Port: <Mandatory>
ONS Server Configuration:
Database Override Connection String:
Oracle Client Character Set NLS_LANG:

5. General Configuration Options

Batch RMI Port: <Mandatory> - RMI port
for batch
Batch Mode: <Mandatory> - CLUSTERED
or DISTRIBUTED
Coherence Cluster Name: <Mandatory> - Unique
name for batch
Coherence Cluster Address: <Mandatory> - Unique
Multicast address
Coherence Cluster Port: <Mandatory> - Unique
port for batch cluster
Coherence Cluster Mode: <Mandatory> - prod

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

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

10. When you are done with the parameter setup, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.
11. Once the install has finished, the installation log location appears 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. You can now install Oracle Utilities Service and Measurement Data Foundation as described in the following section.

Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite

Rollup for SMDF V2.2.0

1. Create a <TEMPDIR> directory on the host server that is independent of any current or other working application environment.
2. Copy the file 'Oracle Utilities Application Framework V4.3.0 Service Pack 3 Single Fix Prerequisite Rollup.zip' in the delivered package to <TEMPDIR>.

If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
3. Upon extracting the zip, file 'Application-Server-Multiplatform' sub-directory will be created.
4. Refer to the Readme.txt inside 'Application-Server-Multiplatform' file for instructions on installing the Oracle Utilities Application Framework 4.3.0 Service Pack 3 Prerequisite Single Fixes.

These patches are also available for download separately from My Oracle Support.

See [Appendix D](#) for a list of the patches contained in the rollup.

Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component

This section describes how to install the application component of Oracle Utilities Service and Measurement Data Foundation, including:

- [Copying and Decompressing Install Media](#)
- [Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0](#)
- [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#)

Copying and Decompressing Install Media

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

The Oracle Utilities Service and Measurement Data Foundation is delivered as a separate installation package. Please refer to the chapter [Supported Platforms and Hardware Requirements](#) for installation details regarding the database and operating system versions supported for the Service and Measurement Data Foundation. Also see the section [Installing Prerequisite Software](#) for prerequisite third-party software installation instructions.

Download the installation package and proceed as follows:

1. Log in 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.
2. Create a <TEMPDIR> directory on the application server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Application Framework.
3. Copy the file SMDF-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your application server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SMDF-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a sub-directory named MDF.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installing Oracle Utilities Service and Measurement Data Foundation V2.2.0

This section outlines the steps for installing the Service and Measurement Data Foundation:

Preparing for the Installation

1. Log on as Oracle Utilities Service and Measurement Data Foundation Administrator (default cissys).
2. Initialize the Framework environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Application

1. Change to the <TEMPDIR>/MDF.V2.2.0 directory.
2. Execute the script:

UNIX:

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

Windows:

```
install.cmd
```

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

The configuration menu for the Oracle Utilities Service and Measurement Data Foundation Application appears.

3. Select menu item 8 to configure OSB.
Use the completed OSB configuration worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
4. Select menu item 9 to configure SOA.
Use the completed SOA configuration worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
5. Select menu item 10 to configure the SOA Configuration Plan.
Use the completed SOA Configuration Plan (MDF) worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).
6. When you are done with the parameter setup, choose option P to proceed with the installation.

Installation of Oracle Utilities Service and Measurement Data Foundation Application Server is complete if no errors occurred during installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation

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 Service and Measurement Data Foundation:

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.
- **OSB SSL Port Number** is the port of the OSB SSL admin 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 Service and Measurement Data Foundation

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 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 Application Component

This section describes how to install the application component 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](#)

Installing the MV90 Adapter for Itron

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

-
- [Preinstallation Tasks for the MV90 Adapter](#)
 - [Installing the MV90 Adapter](#)

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

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-MV90-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-MV90-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named MV90.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the MV90 Adapter - To install the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Change to the <TEMPDIR>/MV90.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.cmd
```

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

3. Choose option P to proceed with the installation.

Once the install has finished successfully, execute the postinstallation 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:

- [Preinstallation Tasks for the Adapter Development Kit](#)
- [Installation Tasks for the Adapter Development Kit](#)

Preinstallation Tasks for the Adapter Development Kit - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
 2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
 3. Copy the file SGG-DG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
 4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-DG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named DG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installation Tasks for the Adapter Development Kit - This section describes the installation of the Adapter Development Kit, including:

- [Initializing the Service and Measurement Data Foundation](#)
- [Installing the Adapter Development Kit](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Adapter Development Kit

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

1. Change to the <TEMPDIR>/DG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Smart Grid Gateway Installation and Configuration Worksheets](#).

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Networked Energy Services](#)
- [Installing the Adapter for Networked Energy Services](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default `cissys`). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a `<TEMPDIR>` directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same `<TEMPDIR>` used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file `SGG-D4-V2.2.0-MultiPlatform.jar` in the delivered package to a `<TEMPDIR>` on your host server. If you are using FTP to transfer this file, remember to use the `BINARY` option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D4-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D4.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

To initialize the Service and Measurement Data Foundation:

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D4.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

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:

- [Preinstallation Tasks for the Adapter for Itron OpenWay](#)
- [Installation Tasks for the Adapter for Itron OpenWay](#)

Preinstallation Tasks for the Adapter for Itron OpenWay - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid

Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D8-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D8-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D8.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Installing the Adapter for Itron OpenWay](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Adapter for Itron OpenWay

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

1. Change to the <TEMPDIR>/D8.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#) on page 4-46.

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Landis+Gyr](#)
- [Installing the Adapter for Landis+Gyr](#)

Preinstallation Tasks for the Adapter for Landis+Gyr - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-LG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-LG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named LG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/LG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).
4. When you are done setting up the parameters, choose option P to proceed with the installation.

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Sensus RNI](#)
- [Installing the Adapter for Sensus RNI](#)

Preinstallation Tasks for the Adapter for Sensus RNI - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D6-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-D6-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D6.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D6.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Silver Spring Networks](#)
- [Installing the Adapter for Silver Spring Networks](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)
- [Initializing the Service and Measurement Data Foundation](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D7-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-D7-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D7.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

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

1. Change to the <TEMPDIR>/D7.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

Once the install has finished successfully, execute postinstallation 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 following section.

Chapter 6

Installing Oracle Utilities Smart Grid Gateway— Upgrade Installation

This chapter provides instructions for upgrading Oracle Utilities Smart Grid Gateway v2.1.0.3 to version Oracle Utilities Smart Grid Gateway 2.2.0.

Note: If you have a version prior to 2.1.0.3, you must upgrade to 2.1.0.3 before upgrading to 2.2.0.

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, in the [Supported Platforms and Hardware Requirements](#).

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

Upgrade of the database component of Oracle Utilities Smart Grid Gateway must be complete before you can proceed with the following sections. Refer to the section “**Upgrade Install**” of the *Oracle Utilities Smart Grid Gateway Database Administrator’s Guide*, which provides instructions on upgrading the database component.

Application Components Upgrade

A successful upgrade consists of the following steps:

- [Upgrading the Oracle Utilities Application Framework Application Component to V4.3.0 Service Pack 3](#)
- [Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDf V2.2.0](#)
- [Upgrading the Oracle Utilities Service and Measurement Data Foundation Application Component to V2.2.0](#)
- [Upgrading the Oracle Utilities Smart Grid Gateway Application Component](#)

Upgrading the Oracle Utilities Application Framework Application Component to V4.3.0 Service Pack 3

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 GatewayV2.1.0.3](#)

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, follow these steps:

1. Log in to the application server host with the Oracle Utilities Application Framework administrator user ID.
2. Download the Oracle Utilities Application Framework V4.3.0.3 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-V4.3.0.3.0-MultiPlatform.jar from the delivered package to the <TEMPDIR>. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
5. Decompress the file:

```
cd <TEMPDIR>
jar -xvf FW-V4.3.0.3.0-MultiPlatform.jar
```

Note: You will need to have Java JDK installed on the machine used to (un)jar the application server installation package. Please install the JDK that is supported for the install on your platform to be able to use the jar command. This is the location of Java packages: <http://www.oracle.com/technetwork/java/archive-139210.html>

A sub-directory named “FW.V4.3.0.3.0” 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>/FW.V4.3.0.3.0` 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 upgrade process. The installation utility does not create a backup of existing environment.

Upgrading the Application Component Over Oracle Utilities Smart Grid GatewayV2.1.0.3

This section outlines the steps for upgrading the application component of Oracle Utilities Application Framework over Oracle Utilities Smart Grid Gateway 2.1.0.3.

Note: Customers who have a version prior to 2.1.0.3 must install 2.1.0.3 before upgrading to 2.2.0

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 Service and Measurement Data Foundation Base 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. Stop the environment, if running:

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

5. Change directory to the `<TEMP_DIR>/FWV4.3.0.3.0` directory.

NOTE: While installing the FW V4.3.0.3 from the previous environment V2.1.0.3 to V2.2.0, the install utility removes the existing environment and re-creates the environment. Make a backup before you proceed with installing FW V4.3.0.3 to retain any configurations for future reference.

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

UNIX:

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

Windows:

```
install.cmd
```

7. The Oracle Utilities Application Framework specific menu appears.
8. Follow the messages and instructions that are produced by the application installation utility.
9. Select each menu item to configure the values. For detailed description of the values, refer to the [Installation and Configuration Worksheets](#).
10. 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. Third Party Software Configuration
   Oracle Client Home Directory: <Mandatory>
   Web Java Home Directory:      <Mandatory>
   Child JVM Home Directory:
   COBOL Home Directory:
   Hibernate JAR Directory: <Mandatory>
   ONS JAR Directory:
   Web Application Server Home Directory: <Mandatory>
   ADF Home Directory:
   OIM OAM Enabled Environment:

2. Keystore Options
   Store Type:                      JCEKS
   Alias:                          ouaf.system
   Alias Key Algorithm:             AES
   Alias Key Size:                 128
   HMAC Alias:                    ouaf.system.hmac
   Padding:                       PKCS5Padding
   Mode:                          CBC

50. Environment Installation Options
   Environment Mount Point: <Mandatory> - Install Location
   Log Files Mount Point: <Mandatory> - ThreadPoolWorker Logs
                                   Location

   Environment Name: <Mandatory>
   Web Application Server Type:                      WLS
   Install Application Viewer Module:                true
```

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

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

11. 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
   WebLogic Server Name:        myserver
   Business Server Application Name: SPLService
   MPL Admin Port Number:       <Mandatory> - Multipurpose Listener
                                   Port
   MPL Automatic startup:       false

3. Web Application Server Configuration
   Web Server Host:             <Mandatory>
   Web Server Port Number:      <Mandatory>
   Web Context Root:            ouaf
   WebLogic JNDI User ID:       <Mandatory>
   WebLogic JNDI Password:     <Mandatory>
   WebLogic Admin System User ID: <Mandatory>
   WebLogic Admin System Password: <Mandatory>
   WebLogic Server Name:        myserver
   Web Server Application Name:  SPLWeb
   Application Admin User ID:    <Mandatory>
   Application Admin Password:   <Mandatory>
   Expanded Directories:        false
   Application Viewer Module:    true

4. Database Configuration
   Application Server Database User ID: <Mandatory>
   Application Server Database Password: <Mandatory>
   MPL Database User ID:               <Mandatory>
   MPL Database Password:              <Mandatory>
   XAI Database User ID:               <Mandatory>
   XAI Database Password:              <Mandatory>
   Batch Database User ID:             <Mandatory>
   Batch Database Password:            <Mandatory>
   Database Name:                     <Mandatory>
   Database Server:                   <Mandatory>
   Database Port:                     <Mandatory>
   ONS Server Configuration:
   Database Override Connection String:
   Oracle Client Character Set NLS_LANG:

5. General Configuration Options
   Batch RMI Port:                    <Mandatory> - RMI port
                                           for batch
   Batch Mode:                        <Mandatory> - CLUSTERED
                                           or DISTRIBUTED
   Coherence Cluster Name:            <Mandatory> - Unique
                                           name for batch
   Coherence Cluster Address:         <Mandatory> - Unique
                                           multicast address
   Coherence Cluster Port:            <Mandatory> - Unique
                                           port for batch cluster
   Coherence Cluster Mode:            <Mandatory> - prod

```

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

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

-
12. When you are done with the parameter setup, proceed with the option P. The utility writes the configured parameters and their values into the configuration file.
 13. Once the upgrade install has finished, the installation log location appears on the screen. If the log does not list any error messages, the upgrade installation of the application component of Oracle Utilities Application Framework is complete. You can now upgrade Oracle Utilities Service and Measurement Data Foundation as described in the following section.

Installing Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDf V2.2.0

1. Create a <TEMPDIR> directory on the host server that is independent of any current or other working application environment.
2. Copy the file 'Oracle Utilities Application Framework V4.3.0 Service Pack 3 Single Fix Prerequisite Rollup.zip' in the delivered package to <TEMPDIR>.

If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

3. Upon extracting the zip file 'Application-Server-Multiplatform' sub-directory will be created.
4. Refer to the Readme.txt inside 'Application-Server-Multiplatform' file for instructions on installing the Oracle Utilities Application Framework 4.3.0 Service Pack 3 Prerequisite Single Fixes.

These patches are also available for download separately from My Oracle Support.

See [Appendix D](#) for a list of the patches contained in the rollup.

Upgrading the Oracle Utilities Service and Measurement Data Foundation Application Component to V2.2.0

This section describes how to upgrade the application component of Oracle Utilities Service and Measurement Data Foundation, including:

- [Copying and Decompressing Install Media](#)
- [Upgrading the Application Component](#)
- [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#)

Copying and Decompressing Install Media

The Oracle Utilities Service and Measurement Data Foundation 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.

1. Log in to the application 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.
2. Download the Oracle Utilities Service and Measurement Data Foundation V2.2.0 Multiplatform from Oracle Software Delivery Cloud.
3. Create a <TEMPDIR> directory on the application server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Application Framework.
4. Copy the file SMDf-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your application server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

-
5. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SMDf-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a sub-directory named MDF.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Upgrading the Application Component

Follow the steps below to install the application component of Oracle Utilities Service and Measurement Data Foundation:

1. Log on as Oracle Utilities Service and Measurement Data Foundation Administrator (default cissys).
2. Initialize the Framework environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if it is running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Installing the Application

1. Change to the <TEMPDIR>/MDF.V2.2.0 directory.
2. Execute the script:

UNIX:

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

Windows:

```
install.cmd
```

Note: On UNIX, ensure that you have the proper execute permission on install.sh. While installing Oracle Utilities Service and Measurement Data Foundation 2.2.0 the utility removes the existing environment and recreates the environment. Make a backup before you proceed ahead.

The configuration menu for the Oracle Utilities Service and Measurement Data Foundation Application appears.

3. Select menu item 8 to configure OSB.

Use the completed OSB configuration worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).

4. Select menu item 9 to configure SOA.

Use the completed SOA configuration worksheet to assist you in this step. See the [Installation](#)

[and Configuration Worksheets.](#)

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

Use the completed SOA Configuration Plan (MDF) worksheet to assist you in this step. See the [Installation and Configuration Worksheets](#).

When you are done with the parameter setup, choose option P to proceed with the installation.

Installation of Oracle Utilities Service and Measurement Data Foundation Application Server is complete if no errors occurred during installation.

Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation

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 Service and Measurement Data Foundation:

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.

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 Service and Measurement Data Foundation

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 server.
- **SOA Port Number** is the port of the SOA managed server.

Upgrading the Oracle Utilities Smart Grid Gateway Application Component

This section describes how to install the application component 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 for Silver Spring Networks](#)

Upgrading the MV90 Adapter for Itron

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

- [Preinstallation Tasks for the MV90 Adapter](#)
- [Upgrading the MV90 Adapter](#)

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

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-MV90-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>

jar -xvf SGG-MV90-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named MV90.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

-
3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the MV90 Adapter - To upgrade the Oracle Utilities Smart Grid Gateway MV90 Adapter:

1. Change to the <TEMPDIR>/MV90.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.cmd
```

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

3. Choose option P to proceed with the installation.

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:

- [Preinstallation Tasks for the Adapter Development Kit](#)
- [Installation Tasks for the Adapter Development Kit](#)

Preinstallation Tasks for the Adapter Development Kit - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-DG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-DG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named DG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installation Tasks for the Adapter Development Kit - This section describes the installation of the Adapter Development Kit, including:

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter Development Kit](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter Development Kit

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

1. Change to the <TEMPDIR>/DG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See **Smart Grid Gateway Installation and Configuration Worksheets** on page 4-46.

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

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:

- [Preinstallation Tasks for the Adapter for Networked Energy Services](#)
- [Installation Tasks for the Adapter for Networked Energy Services](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D4-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D4-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D4.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter for Networked Energy Services](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter for Networked Energy Services

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

1. Change to the <TEMPDIR>/D4.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. Select menu item 17 to configure the URI of the head-end system.

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#) on page 4-46.

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

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:

- [Preinstallation Tasks for the Adapter for Itron OpenWay](#)
- [Installation Tasks for the Adapter for Itron OpenWay](#)

Preinstallation Tasks for the Adapter for Itron OpenWay - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid

Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D8-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.

4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D8-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D8.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter for Itron OpenWay](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter for Itron OpenWay

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

1. Change to the <TEMPDIR>/D8.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#) on page 4-46.

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

Once the install has finished successfully, execute postinstallation 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:

- [Preinstallation Tasks for the Adapter for Landis+Gyr](#)
- [Installation Tasks for the Adapter for Landis+Gyr](#)

Preinstallation Tasks for the Adapter for Landis+Gyr - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-LG-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
```

```
jar -xvf SGG-LG-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named LG.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Installation Tasks for the Adapter for Landis+Gyr - This section describes the installation of the Adapter for Sensus RNI, including:

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter for Landis+Gyr](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter for Landis+Gyr

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

1. Change to the <TEMPDIR>/LG.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

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:

- [Preinstallation Tasks for the Adapter for Sensus RNI](#)
- [Installation Tasks for the Adapter for Sensus RNI](#)

Preinstallation Tasks for the Adapter for Sensus RNI - This section describes the steps that should be taken before installing Oracle Utilities Smart Grid Gateway, including:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D6-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D6-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D6.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter for Sensus RNI](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation environment that you want to install the product into.

UNIX:

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

Windows:

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

3. Stop the environment if running.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter for Sensus RNI

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

1. Change to the <TEMPDIR>/D6.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#) on page 4-46.

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

Once the install has finished successfully, execute postinstallation steps described in [Configuration Tasks for the Adapter for Sensus RNI](#).

Upgrading the Adapter for Silver Spring Networks

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

- [Preinstallation Tasks for the Adapter for Silver Spring Networks](#)
- [Installation Tasks for the Adapter for Silver Spring Networks](#)

Preinstallation 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:

- [Installation Prerequisite](#)
- [Copying and Decompressing the Installation Media](#)

Installation Prerequisite

The Oracle Utilities Service and Measurement Data Foundation 2.2.0 application must be installed prior to installing Oracle Utilities Smart Grid Gateway 2.2.0.

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 a separate 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. Log in to the host server as the Oracle Utilities Service and Measurement Data Foundation administrator user ID (default cissys). This is the same user ID that was used to install the Oracle Utilities Service and Measurement Data Foundation.
2. Create a <TEMPDIR> directory on the host server, which is independent of any current or other working Oracle Utilities Smart Grid Gateway application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Service and Measurement Data Foundation.
3. Copy the file SGG-D7-V2.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR> on your host server. If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
4. Decompress the file:

```
cd <TEMPDIR>
jar -xvf SGG-D7-V2.2.0-MultiPlatform.jar
```

For Windows installations, include the location of the JDK in your path before you execute the jar command.

For both Unix and Windows platforms, a subdirectory named D7.V2.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

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

- [Initializing the Service and Measurement Data Foundation](#)
- [Upgrading the Adapter for Silver Spring Networks](#)

Initializing the Service and Measurement Data Foundation

1. Log on as Oracle Utilities Smart Grid Gateway Administrator (default cissys).
2. Initialize the Service and Measurement Data Foundation 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.

UNIX:

```
$SPLEBASE/bin/spl.sh stop
```

Windows:

```
%SPLEBASE%\bin\spl.cmd stop
```

Upgrading the Adapter for Silver Spring Networks

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

1. Change to the <TEMPDIR>/D7.V2.2.0 directory.
2. Execute the install script:

UNIX:

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

Windows:

```
install.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.

3. 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. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

Use the completed SOA configuration worksheet to assist you in this step. See [Appendix B: Installation and Configuration Worksheets](#).

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

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 Oracle Utilities Smart Grid Gateway *Server Administration Guide* for more information on further configuring and operating the system.

Chapter 7

Configuring the Oracle Utilities Smart Grid Gateway Adapters

This section describes configuration tasks such as deploying OSB and SOA adapters for the Oracle Utilities Smart Grid Gateway adapters. This section includes:

- [Configuration Tasks for the MV90 Adapter](#)
- [Configuration Tasks for the Adapter Development Kit](#)
- [Configuration Tasks for the Adapter for Networked Energy Services](#)
- [Configuration Tasks for the Adapter for Itron OpenWay](#)
- [Configuration Tasks for the Adapter for Landis+Gyr](#)
- [Configuration Tasks for the Adapter for Sensus RNI](#)
- [Configuration Tasks for the Adapter for Silver Spring Networks](#)
- [Operating the Application](#)
- [Creating an Example Weblogic Domain](#)
- [Deploying OSB Adapter on SSL](#)
- [Deploying SOA Composites on SSL](#)
- [Deploying OSB Adapters with DataRaker](#)

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:

```
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>
```

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>
```

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>
```

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>
```

This will not override any OSB custom changes

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) for more information about deploying OSB components on a separate WebLogic server.

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-2.2.0.0.0.jar
spl-d5-osb-2.2.0.0.0.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 “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=<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_MV90.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_MV90.xml -Dadmin.user=<ADMIN_USER>
-Dadmin.password=<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_MV90.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

Starting the Application

The OSB WebLogic server instance should be up and running before starting the main application.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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`

1. Start up the environment. Run the following command:

UNIX: `spl.sh start`

Windows: `spl.cmd start`

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: `spl.sh stop`

Windows: `spl.cmd stop`

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>
```

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>
```

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>
```

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>
```

This will not override any OSB custom changes

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) for more information about deploying OSB components on a separate WebLogic server.

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-dl-osb-2.2.0.0.0.jar
spl-dg-osb-2.2.0.0.0.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=<OSB_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_DG.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_DG.xml
-Dadmin.user=<OSB_ADMIN_USER>
-Dadmin.password=<OSB_ADMIN_PASSWORD> -Douaf.user=<JMS_USER>
-Douaf.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>
```

This will not override any OSB custom changes

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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_DG.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

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>
```

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>
```

6. Import the Policy Templates and Policies.
 - a. First, import the policy template jar using Enterprise Manager.

i. For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

iii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iv. Click on **Web Services Assertion Templates** at the top of the page

v. Click on **Import** and import the following:

- sgg-d1-policy.jar

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:

i. Import the “sgg_dg_cfs_multispeak_header_client_policy” policy file (\$SPLEBASE/soaapp) using Enterprise Manager.

ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

iii. 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”

iv. Right click on the domain and navigate to **Web Services, WSM Policies**.

iv. Click on **Import** and import the following zip:

- 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

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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. Append 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-dl-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>
```
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.
 - i. For **Linux:**

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows:**

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```
 - ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
 - iii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iv. Click on **Web Services Assertion Templates** at the top of the page

v. Click on **Import** and import the following zip:

- sgg-d1-policy.jar
- 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:

i. Import the “sgg_dg_cfs_multispeak_header_client_policy” policy file (\$SPLEBASE/soaapp) using Enterprise Manager.

ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

iii. 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”

iv. Right click on the domain and navigate to **Web Services, WSM Policies.**

iv. Click on **Import** and import the following zip:

- sgg_dg_cfs_multispeak_header_client_policy.zip

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, please 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_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_DG.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

```
%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_DG.xml
```



```
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

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>
```

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.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:** sgg.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 15.
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 15.
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.

Field	Default Value	Description
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.dl.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_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" & "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.
 - In Oracle Enterprise Manager, navigate to the **DG/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **MR_Server**.
 - In the Attached Policies window, select the oracle/wss_http_token_client_policy.
 - Click **Detach** to remove the default security policy.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the MR_Server reference.
8. Attach the policy to the CD_Server reference on the Common composite.
 - Navigate to the **DG/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **CD_Server**.
 - In the Attached Policies window, select the oracle/wss_http_token_client_policy.
 - Click **Detach** to remove the default security policy.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the CD_Server reference.
9. Attach the policy to the OD_Server reference on the Common composite.
 - Navigate to the **DG/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **OD_Server**.

- In the Attached Policies window, select the oracle/wss_http_token_client_policy.
- Click **Detach** to remove the default security policy.
- In the Available Policies window, select the policy that you just created.
- 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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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
```

To start up the environment, run the following command:

UNIX: spl.sh start

Windows: spl.cmd start

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: spl.sh stop

Windows: spl.cmd stop

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>
```

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>
```

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>
```

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>
```

This will not override any OSB custom changes

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-2.2.0.0.0.jar
spl-d4-osb-2.2.0.0.0.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 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=<OSB_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_D4.xml
update_osb -Dadmin.user=<OSB_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_D4.xml
-Dadmin.user=<OSB_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_D4.xml
update_osb -Dadmin.user=<OSB_ADMIN_USER>
-Dadmin.password=<OSB_ADMIN_PASSWORD>
-Douaf.user=<JMS_USER> -Douaf.password=<JMS_PASSWORD>
```

This will not override any OSB custom changes

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>

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
cd %SPLEBASE%\soaapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D4.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D4.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

```
%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D4.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

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>
```

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>
```

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>
```

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 on 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. In the Type field, select **Password**.
8. Click **OK**.

Importing the Policy Templates

To import the policy assertion templates:

1. First, import the policy template jar using Enterprise Manager.
 - a. For **Linux**:


```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f 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 following zip:
 - sgg-d1-policy.jar

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
ant -f package-soa-policy.xml -Dproduct=d4
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d4
```

- 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 following zip:
- sgg-d4-policy.jar

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:

- In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
- Right click on the domain and navigate to **Web Services, Policies**. In the **Applies To** field, select either **All** or **Service Clients**.
- Select the policy oracle/wss_http_token_client_policy.
- 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 and click **Save**.
 - Click **OK**.
- 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 29.

Field	Default Value	Description
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 29.
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.dl.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_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" & "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>
</orawsp:SGGCredentialStoreInsertionXPath>

```

6. Save the policy.

7. Attach the policy to the User Manger reference.

- In Oracle Enterprise Manager, Navigate to the **AuthenticationMgr** composite. The full path is **SOA/soa-infra/Echelon/AuthenticationMgr**.
- On the Policies tab, from the **Attach To/Detach From** menu, select **UserManager**.
- In the Available Policies window, select the policy that you just created.
- 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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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`

1. Start up the environment. Run the following command:

UNIX: `spl.sh start`

Windows: `spl.cmd start`

Follow the messages on the screen along with the logs in `$SPLSYSTEMLOGS` directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: `spl.sh stop`

Windows: `spl.cmd stop`

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>
```

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.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_D8.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_D8.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

To Deploy on a Separate WebLogic Instance:

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-2.2.0.0.0.jar  
spl-d8-osb-2.2.0.0.0.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 "D8-SystemModule"
 - Under "D8-SystemModule" create a sub-deployment "D8-JMSFAServer" and target it to "OSB-JMSServer"
 - 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 Stndalone 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.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_D8.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_D8.xml
-Dadmin.user=<OSB_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:

```

%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>

```

This will not override any OSB custom changes.

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. 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>

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D8.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

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_D8.xml
deployTestHarness -Dserver.password=<SOA_USER>
-Dserver.password=<SOA_PASSWORD>
```

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>
```

To Deploy on a Separate SOA on a WebLogic Instance:

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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. Append 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>
```
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.
6. 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 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_MDF.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D8.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

```
%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D8.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

7. 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>
```

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>
```

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 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.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. First, import the policy template jar using Enterprise Manager.
 - a. For **Linux**:


```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

 For **Windows**

```
cd %SPLEBASE%/soaapp
ant -f 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 following zip:
 - sgg-d1-policy.jar

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
ant -f package-soa-policy.xml -Dproduct=d8
```

For **Windows**

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d8
```
 - 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 **Import** and import the following zip:
 - sgg-d8-policy.jar

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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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

To start up the environment, run the following command:

UNIX: spl.sh start

Windows: spl.cmd start

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with post installation steps. Use the following utility to stop the environment:

UNIX: spl.sh stop

Windows: spl.cmd stop

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>
```

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.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_LG.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_LG.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

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-2.2.0.0.0.jar
spl-d3-osb-2.2.0.0.0.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 “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, please refer to the section Deploying OSB adapter on SSL.

UNIX:

```
cd $SPLEBASE/osbapp
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_LG.xml
-Dadmin.user=<OSB_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:

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
osb_LG.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_LG.xml
-Dadmin.user=<OSB_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:

```
%SPLEBASE%/product/apache-ant/bin/ant -buildfile deploy-
osb_LG.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.

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, 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
```

- a. 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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_LG.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

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>
```

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>
```

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-dl-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 section [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>

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_LG.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>

%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_LG.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

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>
```

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.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:** sgg.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. In the Type field, select **Password**.
8. Click **OK**.

Importing the Policy Templates and Policies

Follow the procedure below to import policy templates and policies:

1. First, import the policy template jar using Enterprise Manager.

i. For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

iii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iv. Click on **Web Services Assertion Templates** at the top of the page

v. Click on **Import** and import the following:

- sgg-d1-policy.jar

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.

i. For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d3
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d3
```

ii. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

iii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iv. Click on **Web Services Assertion Templates** at the top of the page

v. Click on **Import** and import the following:

- sgg-d3-policy.jar

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**.
 - 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 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.dl.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" & "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>
</orawsp:SGGCredentialStoreInsertionXPath>

```

6. Save the policy.
7. Attach the policy to the MR_CB reference on the CommissionDecommission composite.
 - In Oracle Enterprise Manager, navigate to the **CommissionDecommission** composite.
 - From the **Attach To/Detach From** menu, select **MR_CB**.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the MR_CB reference.
8. Attach the policy to the CD_CB reference on the ConnectDisconnect composite.
 - Navigate to the **ConnectDisconnect** composite.
 - From the **Attach To/Detach From** menu, select **CD_CB**.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the CD_CB reference.
9. Attach the policy to the MR_CB reference on the OnDemandRead composite.
 - Navigate to the **OnDemandRead** composite.
 - From the **Attach To/Detach From** menu, select **MR_CB**.
 - In the Available Policies window, select the policy that you just created.
 - 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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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`

1. Start up the environment. Run the following command:

UNIX: `spl.sh start`

Windows: `spl.cmd start`

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: `spl.sh stop`

Windows: `spl.cmd stop`

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 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>
```

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>
```

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>
```

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>
```

This will not override any OSB custom changes

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-2.2.0.0.0.jar
spl-d6-osb-2.2.0.0.0.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 “D6-SystemModule”.
 - Under “D6-SystemModule” create a sub-deployment “D6-JMSFAServer” and target it to “OSB-JMSServer”.
 - 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=<OSB_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_D6.xml
update_osb -Dadmin.user=<ADMIN_USER> -
Dadmin.password=<OSB_ADMIN_PASSWORD> Douaf.user=<JMS_USER> -
Douaf.password=<JMS_PASSWORD>
```

Windows:

```
cd %SPLEBASE%\osbapp

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
osb_D6.xml
-Dadmin.user=<OSB_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_D6.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

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, 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
```

- a. 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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
cd %SPLEBASE%\soaapp
```

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D6.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

4. Deploy the Test Harness 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_D6.xml
deployTestHarness -Dserver.password=<SOA_USER>
-Dserver.password=<SOA_PASSWORD>
```

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>
```

5. Import the Policy Templates and Policies.

- a. First, import the policy template jar using Enterprise Manager.

For Linux:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For Windows:

```
cd %SPLEBASE%\soaapp
```

```
ant -f package-soa-policy.xml -Dproduct=d1
```

In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

ii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iii. Click on **Web Services Assertion Templates** at the top of the page

iv. Click on **Import** and import the following zip:

- sgg-d1-policy.jar

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.

For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d6
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d6
```

In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.

ii. Right click on the domain and navigate to **Web Services, WSM Policies**.

iii. Click on **Web Services Assertion Templates** at the top of the page

iv. Click on **Import** and import the following zip:

- sgg-d6-policy.jar

This file is located in the following directory:

UNIX: \$SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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. Append 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-dl-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>

```

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.

For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

- i. In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
- ii. Right click on the domain and navigate to **Web Services, WSM Policies**.
- iii. Click on **Web Services Assertion Templates** at the top of the page
- iv. Click on **Import From File** and import the following zip:

- sgg-d1-policy.jar

This file is located in the following directory:

UNIX: \$SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

- First, import the policy template jar using Enterprise Manager.

For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d6
```

For **Windows**:

```
cd %SPLEBASE%\soaapp
ant -f package-soa-policy.xml -Dproduct=d6
```

- In Oracle Enterprise Manager, navigate to **WebLogic Domain** and select the required SOA domain.
- Right click on the domain and navigate to **Web Services, WSM Policies**.
- Click on **Web Services Assertion Templates** at the top of the page
- Click on **Import From File** and import the following zip:

- sgg-d6-policy.jar

This file is located in the following directory:

UNIX: \$SPLEBASE/soaapp/policies/jars

Windows: %SPLEBASE%\soaapp\policies\jars

- 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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D6.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

```
%SPLEBASE%\product\apache-ant\bin\ant
```

```
-buildfile deploy-soa_D6.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

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>
```

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 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.d6.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.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 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. 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 the Security Credentials" on page 64.
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 64.
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_Sensus" 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.dl.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_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" & "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.
 - In Oracle Enterprise Manager, navigate to the **Sensus/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **MR_Server**.
 - In the Attached Policies window, select the oracle/wss_http_token_client_policy.
 - Click **Detach** to remove the default security policy.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the MR_Server reference.
8. Attach the policy to the CD_Server reference on the Common composite.
 - Navigate to the **Sensus/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **CD_Server**.
 - In the Attached Policies window, select the oracle/wss_http_token_client_policy.
 - Click **Detach** to remove the default security policy.
 - In the Available Policies window, select the policy that you just created.
 - Click **Attach** to attach the policy to the CD_Server reference.
9. Attach the policy to the OD_Server reference on the Common composite.
 - Navigate to the **Sensus/Common** composite.
 - Navigate to the Policies tab.
 - From the **Attach To/Detach From** menu, select **OD_Server**.
 - In the Attached Policies window, select the oracle/wss_http_token_client_policy.
 - Click **Detach** to remove the default security policy.
 - In the Available Policies window, select the policy that you just created.
 - 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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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`

1. Start up the environment. Run the following command:

UNIX: spl.sh start

Windows: spl.cmd start

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: spl.sh stop

Windows: spl.cmd stop

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 the section 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>
```

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>
```

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>
```

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>
```

This will not override any OSB custom changes.

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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-2.2.0.0.0.jar
spl-d7-osb-2.2.0.0.0.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 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, please refer to the section Deploying OSB adapter on SSL.

UNIX:

```
cd $SPLEBASE/osbapp
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-osb_D7.xml
```

```
-Dadmin.user=<OSB_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_D7.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_D7.xml
-Dadmin.user=<OSB_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.

```
%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>
```

This will not override any OSB custom changes

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 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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-soa_D7.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

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_D7.xml
deployTestHarness -Dserver.password=<SOA_USER>
-Dserver.password=<SOA_PASSWORD>
```

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>
```

To Deploy on a Separate WebLogic Instance

Note: See [Configuration of Oracle Fusion Middleware Components on a Separate Server from Oracle Utilities Service and Measurement Data Foundation](#) 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. Append following XML snippet to
<MIDDLEWARE_HOME>\user_projects\domains\SGG_2007_SOADomain\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>
```

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:
 - Under Domain Structure, navigate to **Services, Messaging, JMS Servers**
 - On the JMS Servers Page, Click on **New**.
 - 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.
- On the Create JMS System Module screen, enter name, for example, SSN-SystemModule (You can leave other fields empty if you want.)
 - 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
 - On the next screen click **Finish and Activate changes**.
- c. Create Queues:
- Click on **New** in JMS Module to create the Queue.
 - Provide a name (for example, SSNTestSSNODRQ) and a JNDI name (for example, queue/SSNTestSSNODRQ).
 - 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 (E.g. SSN-JMSFAServer) and click **OK**.
 - Select the target JMS Server we created (E.g. SSN-JMSServer) and Click **finish**.
 - Click on **New** in JMS Module to create the Queue.
 - Provide a name (e.g., SSNODRQ) and a JNDI name (e.g., 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
- Click on **New** in JMS Module to create the Connection factory
 - Give the Connection factory a name (for example, SSNTestHarnessConnectionFactory) and JNDI name (for example, jms/SSNTestHarnessConnectionFactory). Click **Next**.
 - 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**.
 - Click on **New** in JMS Module to create the Connection factory.
 - Give the Connection factory a name (for example, SSNConnectionFactory) and JNDI name (for example, jms/SSNConnectionFactory). Click **Next**.
 - 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:
- Under Domain Structure, navigate to **Services, Messaging, Bridge, JMS Bridge Destinations**

- On the JMS Bridge Destinations Page, Click on **New** button. 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: Once you created JMS Bridge Destination, Click on Services > Messaging > Bridge > JMS Bridge Destinations > SSNSOABridgeDestination.

- On the SSNSOABridgeDestination page, Enter username and password values, Click **Save**.
- f. Create a Target JMS Bridge Destination
- Under Domain Structure, navigate to **Services, Messaging, Bridge, JMS Bridge Destinations**.
 - On the JMS Bridge Destinations Page, Click **New**. 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: Once you created 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 on **New** button. 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 section [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>
```

```
$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-soa_D7.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

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>
```

```
%SPLEBASE%\product\apache-ant\bin\ant
-buildfile deploy-soa_D7.xml
-Dserver.user=<ADMIN_USER> -Dserver.password=<ADMIN_PASSWORD>
```

8. 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:

```
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>
```


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>
```

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.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. First, import the policy template jar using Enterprise Manager.

For **Linux**:

```
cd $SPLEBASE/soaapp
ant -f package-soa-policy.xml -Dproduct=d1
```

For **Windows**:

```
cd %SPLEBASE%/soaapp
ant -f 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 following zip:
 - sgg-d1-policy.jar

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.

The first time you start Oracle Utilities Smart Grid Gateway, you need to log in to 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`

1. Start up the environment. Run the following command:

UNIX: `spl.sh start`

Windows: `spl.cmd start`

Follow the messages on the screen along with the logs in \$SPLSYSTEMLOGS directory to ensure that the environment was started successfully.

If the startup failed, identify the problem by reviewing the logs. Resolve any issues before attempting to restart the environment.

You should postpone the startup process until you are done with postinstallation steps.

Use the following utility to stop the environment:

UNIX: `spl.sh stop`

Windows: `spl.cmd stop`

Operating the Application

At this point your installation and custom integration process is complete. Be sure to read the Oracle Utilities Smart Grid Gateway *Server Administration Guide* for more information on further configuring and operating the system.

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:

For **Linux**:

```
cd $SPLEBASE/bin
./createDomain.sh -t OSB
```

For **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:

For **Linux**:

```
cd $SPLEBASE/bin
./createDomain.sh -t SOA
```

For **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:

```
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_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> -
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>
```

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> -
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>
```

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

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 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>

$SPLEBASE/product/apache-ant/bin/ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

Windows:

```
%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy
-soa_MDF.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>

%SPLEBASE%\product\apache-ant\bin\ant -buildfile deploy-
soa_<adapter>.xml
-Dserver.user=<SOA_USER> -Dserver.password=<SOA_PASSWORD>
```

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_<adapter>.xml deployTestHarness -Dserver.password=<SOA_USER>
-Dserver.password=<SOA_PASSWORD>
```

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>
```

6. The following commands are required when using Custom trust store, <adapter> in below commands should be replaced with respective adapter name i.e (LG, D4, D6, D7, D8, DG)
7. Add the following line in the file soa.properties,

```
javax.net.ssl.trustStorePassword=<passphrase_of_truststore
_for_soa_deployment>
located at below locations:
```

Linux: \$SPLEBASE/soaapp

Windows: %SPLEBASE%/soapp

8. 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_<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 section [Deploying SOA Composites on SSL](#).

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> -Ddeploy.dataraker=true
```

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> -Ddeploy.dataraker=true
```

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> -Ddeploy.dataraker=true
```

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> -Ddeploy.dataraker=true
```

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 “-Ddeploy.dataraker=true”

The 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_deployment>
-D 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](#) for more details.

Note: Oracle Utilities Service Order Management only supports WebLogic version 12.1.3.0+ and Oracle Service Bus/Oracle SOA Suite 12.2.1.

3. Ensure that you have downloaded the Oracle Utilities Service Order Management V2.2.0 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 sections [Initial Installation](#) or [Demo Installation](#) 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*.
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*.

Initial Installation

A successful initial installation of SOM involves the installation of the following components:

- Oracle Utilities Service Order Management Database Component
For the steps to install the database, refer to the chapter “Installing the Version 2.2.0 Database for Service Order Management” in the *Oracle Utilities Smart Grid Gateway Database Administrator Guide*.

-
- Oracle Utilities Application Framework V4.3.0 Service Pack 3 (4.3.0.3) Application Component
 - Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDF V2.2.0
 - Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component
 - Oracle Utilities Meter Data Management V2.2.0 Application Component
 - MV90 Adapter for Itron
 - Adapter for Landis+Gyr

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 Version 2.2.0 Database for Service Order Management” in the Oracle Utilities Smart Grid Gateway *Database Administrator Guide*.
- Oracle Utilities Application Framework V4.3.0 Service Pack 3 (4.3.0.3) Application Component
- Oracle Utilities Application Framework V4.3.0.3 Single Fix Prerequisite Rollup for SMDF V2.2.0
- Oracle Utilities Service and Measurement Data Foundation V2.2.0 Application Component.
- Oracle Utilities Meter Data Management V2.2.0 Application Component
- MV90 Adapter for Itron
- Adapter for Landis+Gyr

To install all of the above components, follow the instructions mentioned in chapter [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](#)
- [Configuring Secure Sockets Layer \(SSL\)](#)
- [Setting Up an Application Keystore](#)
- [Domain Templates \(Linux Weblogic 12.1.3.0+ only\)](#)
- [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 by running the following:

Unix:

```
$SPLEBASE/bin/splenvron.sh -e $SPLENVIRON
For example:
/ouaf/TEST_ENVIRON1/bin/splenvron.sh -e TEST_ENVIRON1
```

Windows:

```
%SPLEBASE%\bin\splenvron.cmd -e %SPLENVIRON%
For example:
D:\ouaf\TEST_ENVIRON1\bin\splenvron.cmd -e TEST_ENVIRON1
```

3. Execute 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. Execute 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 `$SPL/EBASE/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` file.

Configuring Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network to authenticate each other's identity and by encrypting the data exchanged between the applications. Authentication allows a server, and optionally a client, to verify the identity of the application on the other end of a network connection. Encryption makes data transmitted over the network intelligible only to the intended recipient.

Follow these steps to configure Secure Sockets Layer:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server.

Use the digital certificates, private keys, and trusted CA certificates provided by the WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.
2. Store the identity and trust.

Private keys and trusted CA certificates which specify identity and trust are stored in keystores.
3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.

See "Configure keystores" in the Oracle WebLogic Server Administration Console Online Help.

For additional information on configuring keystores, refer to <http://docs.oracle.com/middleware/1213/wls/WLACH/taskhelp/security/ConfigureKeystoresAndSSL.html>
4. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console.

Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).

For additional information, refer to the following topics:

- Servers: Configuration: SSL (<http://docs.oracle.com/middleware/1213/wls/WLACH/pagehelp/Corecoreserverserverconfigssltitle.html>)

- Configure two-way SSL (<http://docs.oracle.com/middleware/1213/wls/WLACH/taskhelp/security/ConfigureTwoWaySSL.html>)
- Obtaining and Storing Certificates for Production Environments (http://docs.oracle.com/middleware/1213/wls/SECMG/identity_trust.htm#SECMG798)
- Configuring Keystores with WebLogic Server (http://docs.oracle.com/middleware/1213/wls/SECMG/identity_trust.htm#SECMG383)

Note: Depending on your choice of implementation you may need to change some configuration files. These files are managed by templates and will be overwritten if the procedures documented in “Customizing Configuration Files” are not followed.

The identity and trust keystore files and other SSL certificate related options are configured using the `configureEnv.sh|cmd` utility.

Setting Up an Application Keystore

This section describes how to set up a keystore in your system. The keystore is used for functionality such as digital signatures for document numbers, and encryption for credit card security.

Note that this is different from the Oracle Utilities Application Framework (also called the system) keystore and the weblogic SSL keystores.

For additional information about document numbers, digital signatures, and encryption, see the online help.

For additional information about using the Java keytool utility, see the following section of the Oracle Java SE documentation:

<http://docs.oracle.com/javase/7/docs/technotes/tools/solaris/keytool.html>

Follow this procedure to set up the keystore in your environment:

1. Generate the keystore. The following command creates the file ".mykeystore" in directory `${SPLEBASE}`:

```
keytool -genkeypair -alias <keyalias> -keyalg RSA -sigalg
SHA256withRSA -keystore ${SPLEBASE}/<filename> -keysize 1024
-storetype JCEKS -dname "CN=<name>, OU=<unit>, O=<organization>,
C=<country>" -validity 365
```

For example:

```
keytool -genkeypair -alias ouaf.application -keyalg RSA -sigalg
SHA256withRSA -keystore ${SPLEBASE}/.mykeystore -keysize 1024
-storetype JCEKS -dname "CN=Mark Jones, OU=TUGBU, O=Oracle, C=US"
-validity 365
```

The utility will prompt you for the keystore and key passwords. Make sure that they are the same.

2. Configure the following template files by adding the following entries:

For WebLogic Server:

- To enable in WebLogic, edit the following in `${SPLEBASE}/templates/startWeblogic.sh.template`:

```
JAVA_OPTIONS="$JAVA_OPTIONS
-Dcom.oracle.ouaf.keystore.file=${SPLEBASE}/<filename>"
```

```
JAVA_OPTIONS="$JAVA_OPTIONS"
-Dcom.oracle.ouaf.keystore.password=<keystore_password>"
```

For <keystore_password>, use the same password entered in the keytool utility.

- To enable this in batch, edit the threadpoolworker.properties.template:

```
com.oracle.ouaf.keystore.file=@force_forward_slash(SPLEBASE)@/.mykeystore
com.oracle.ouaf.keystore.password=<keystore_password>
```

Note: Because the path needs to be passed with forward slashes even on Windows platforms, the force_forward_slash function will convert any "\" to "/".

For <keystore_password>, use the same password entered in the keytool utility.

For WebSphere Server:

- Create the password file.

```
echo ab987c | tr -d '\n'>$SPLEBASE/.passFile
```

Note: In above command, please replace "ab987c" with your password string.

- Add Keystore entries to spl.properties templates:

Open each of the five spl.properties templates mentioned below and add the following two lines in each of the templates

```
com.oracle.ouaf.keystore.file=@SPLEBASE@/.mykeystore
com.oracle.ouaf.keystore.passwordFileName=@force_forward_slash(
SPLEBASE)@/.passFile
```

List of spl.properties templates (located in \${SPLEBASE}/templates/ folder):

- spl.properties.iws.template
 - spl.properties.template
 - spl.properties.service.template
 - spl.properties.XAIAApp.template
 - spl.properties.standalone.template
3. Re-initialize the environment to propagate these changes by executing the initialSetup.sh/cmd.
 4. Restart the environment.

Domain Templates (Linux Weblogic 12.1.3.0+ only)

The intended use of the domain templates is for native/clustered installation of the Oracle Utilities Application Framework (OUAF) environment into a Weblogic domain. The domain template(s) defines the core set of resources within a Weblogic domain, including an Administration Server along with the basic configuration information for a Oracle Utilities Application Framework based application. The domain template is a “snapshot” of the delivered embedded “splapp” domain. When working with domain templates you will need to manage the application (stopping, starting, deployment, undeployment) utilizing the Weblogic delivered utilities.

- Install and configure application stack (OUAF and Edge Product)

Note: Environment will need to be configuring to deploy in ear format.

- Review domain templates (Simple /Complex)

- Execute config.sh and enter the path of the domain template file
- Configure domain
- Complete domain configuration

Note: Configure nodemanager.properties and setDomainEnv.sh

- Update SPLEBASE (ENVIRON.INI)

Detailed Description

The product installation includes a two predefined WebLogic Server Domain templates. The delivered domain templates are located under the SPLEBASE:

\$SPLEBASE/tools/domaintemplates

- Oracle-Utilities-Simple-Linux-12.1.3.0.0.jar
- Oracle-Utilities-Complex-Linux-12.1.3.0.0.jar

The Simple Domain Template is for use with one machine and does not include a Weblogic cluster, this domain configuration is similar to current delivered embedded splapp domain, with the exception that there will be two Weblogic servers (utilities_server1 and a "Admin Server").

The Complex Domain Template is configured for use with a pre-configured Weblogic cluster, with one machine configured, node manager settings, and one managed server configured.

The delivered domain templates defines the full set of resources within an Oracle Utilities Application Framework domain including:

- Demo certificates (the demo certificates will need to be updated for production use)
- Setting of XML Registry Settings
- Setting of Default users and groups
- Machine configuration
- Default Users and Groups

Note: The Users and Groups match the delivered values delivered with the embedded domain.

- JTA Settings
- Node Manager Settings
- WebLogic Server

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 be 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: splenvron.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

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

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 splenvron 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/createDBStandalone.sh
```

Windows:

```
%SPLEBASE%\bin\createDBStandalone.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_43020_BLD001,slc04lds:1522:Z143Q12C"
```

- Sample Execution – Prompting for a Password

```
./ouafDatabasePatch.sh -p "-t O -d  
CISADM_Z1_12C_43020_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

Installation Menu Functionality Overview

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 within that group 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.

Note: When working with the menu you will see 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 an numeric value in the prompt.

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 '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.

In the worksheets there are three different types of values given:

-
- Default Values are the values that will be defaulted when running the installation utility.
 - Security Values denote values that should be changed when in production.
 - Example Values are values that can be used for a default installation.

Note: The production environment should not be run with default values. See the *Server Administration Guide* specific to this product, for additional information about configuring these values.

When you enter passwords you will not see the password characters on the screen because they are entered in silent mode. Passwords are encrypted when the values are entered.

Install the Oracle Client software specified in the section **Supported Platforms** prior to running any of the installation utilities.

The following prompt will appear 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

When the application server choice is Oracle WebLogic, the Oracle Utilities Application Framework installation uses the WebLogic API to encrypt the User ID and password that perform admin functions for the WebLogic application servers. Please refer to the WebLogic documentation for further information about the encryption.

The Oracle Utilities Application Framework installation also uses industry standard cryptography to encrypt passwords that are prompted within the installation.

In each case these passwords are entered in the command line but the inputted values are not reflected on the screen when performing the installation.

Appendix B

Installation and Configuration Worksheets

This section includes the following topics:

- [Application Framework Installation and Configuration Worksheets](#)
- [Service and Measurement Data Foundation Installation and Configuration Worksheets](#)
- [Smart Grid Gateway Installation and Configuration Worksheets](#)
 - [For the Adapter Development Kit](#)
 - [For the Adapter for Networked Energy Services](#)
 - [For the Adapter for Itron OpenWay](#)
 - [For the Adapter for Landis+Gyr](#)
 - [For the Adapter for Sensus RNI](#)
 - [For the Adapter for Silver Spring Networks](#)

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 [Chapter 5: 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 [Chapter 6: Installing Application Server Prerequisite Software](#).

Environment ID, Roles, Third Party Software Configuration

```

*****
* Environment Installation Options *
*****
1. Environment ID, Roles, Third Party Software Configuration
   Environment ID:
   Server Roles:
   Oracle Client Home Directory:
   Web Java Home Directory:
   Hibernate JAR Directory:
   ONS JAR Directory:
   Web Application Server Home Directory:
   WebLogic Server Thin-Client JAR Directory:
   ADF Home Directory:
   OIM OAM Enabled Environment: false

```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Environment ID	ENVIRONMENT_ID	Identifier to associate different application servers as part of the same environment. On a new installation, the default is a random 8 digit number.	
Server Roles	SERVER_ROLES	The type of role the server performs whether for batch or online. A server may be configured to have an online and/or batch role. Only the menu items appropriate to the role will appear on the menus, and only the appropriate scripts will be executable in the application server.	
Oracle Client Home Directory	ORACLE_CLIENT_HOME	The home directory of the Oracle Client. The application will use the Perl included under this Oracle Client. Example Location: /oracle/client/product/12.1.0.2.0	
Web Java Home Directory	JAVA_HOME	Java home that will be used by the web application server. Example Location: /ouaf/java/jdk1.8.0_31	
Hibernate JAR Directory	HIBERNATE_JAR_DIR	Location on the disk where the hibernate jar files are installed.	
**ONS JAR Directory	ONS_JAR_DIR	Location on the disk where the ons-12.1.0.1.jar file is installed. **Required for Oracle RAC installation. See the <i>Server Administration Guide</i> for more information.	
Web Application Server Home Directory	WEB_SERVER_HOME	Location on the disk where the application server is installed. Example Location: WebLogic: /ouaf/middleware/wlserver_12.1.3 To validate the home directory, check if the following jar files exist in the appropriate path: \$WEB_SERVER_HOME/server/lib/weblogic.jar %WEB_SERVER_HOME%\server\lib\weblogic.jar	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
WebLogic Server Thin-Client JAR Directory	WLTHINT3CLIENT_JAR_DIR	Location where wlthint3client.jar is located. Populate only if WEB_SERVER_HOME is empty and if the application needs to access JMS from a batch job.	
* ADF Home Directory	ADF_HOME	Location on the disk where ADF is installed. Example Location: /ouaf/jdev11_1_1_8 Note: This is an optional value.	
OIM OAM Enabled Environment	OPEN_SPML_ENABLED_ENV	Denotes if an environment will be integrating with Oracle Identity Manager for user propagation. Valid values: true false Defaulted value: false	

* 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.

Keystore Options

Note: 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.

Please review the Security Guide for more information on setting up keystores.

2. Keystore Options

Import Keystore Directory:

Store Type:

JCEKS

Alias:

ouaf.system

Alias Key Algorithm:

AES

Alias Key Size:

128

HMAC Alias:

ouaf.system.hmac

Padding:

PKCS5Padding

Mode:

CBC

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Import Keystore Directory	KS_IMPORT_KEYSTORE_FOLDER	<p>Specify this option if you want to import the keystore files from an external location or directory, during the installation process. This is needed when the customer has an existing environment that has a keystore and the database your new application server.</p> <p>After installation is complete, to configure keystore options, perform the following sequence: configureEnv.sh cmd -i (enter keystore options) initialSetup.sh cmd -s (loads keystore) configureEnv.sh cmd (reenter ouaf encrypted security information such as passwords) initialSetup.sh cmd (distribute the encrypted data)</p> <p>If this option is left empty, the install process creates a new keystore from scratch.</p>	
Store Type	KS_STORETYPE	Value used for keytool option -storetype Default value: JCEKS	
Alias	KS_ALIAS	Value used for keytool option -alias Default value: ouaf.system	
Alias Key Algorithm	KS_ALIAS_KEYALG	Value used for keytool option -keyalg	
Alias Key Size	KS_ALIAS_KEYSIZE	Value used for keytool option -keysize	
HMAC Alias	KS_HMAC_ALIAS	<p>Value used for keytool option -alias</p> <p>The following values are fixed:</p> <ul style="list-style-type: none">- HMAC Alias Key Algorithm: HmacSHA256- HMAC Alias Key Size: 256 <p>Default value: ouaf.system.hmac</p>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Padding	KS_PADDING	Value used for encryption/decryption Default value: PKCS5Padding	
Mode	KS_MODE	Value used for encryption/decryption Default Vaule: CBC	

Environment Installation Options

50. Environment Installation Options

Environment Mount Point:

Log Files Mount Point:

Environment Name:

Web Application Server Type:

WLS

Install Application Viewer Module:

true

Install Demo Generation Cert Script:

true

Install Sample CM Source Code:

true

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Environment Mount Point	<SPLDIR>	<p>The mount point into which the application is installed. For example: /ouaf for UNIX and C:\ouaf for Windows.</p> <p>This mount point MUST exist and the administrator user ID MUST be able to write to this directory. (This is the user ID that is created specifically to administer the product environments; the default is cissys). The installation sets permissions on all subdirectories installed under this directory.</p> <p>See <SPLENVIRON> below for more information on how this mount point is used.</p>	
Log File Mount Point	<SPLDIROUT>	<p>A mount point that will contain any application output or application logs. Example value is /ouaf/sploutput for UNIX installation or C:\ouaf\sploutput for Windows.</p> <p>This mount point MUST exist and the administrator user ID MUST be able to write to this directory. (This is the user ID that is created specifically to administer the product environments; the default is cissys).</p> <p>For each environment initialized, the application logs will be written to the directory <SPLDIROUT>/<SPLENVIRON></p> <p>Note: Later in the installation the splenvron.sh (splenvron.cmd) script will set the \$SPLOUTPUT (%SPLOUTPUT%) environment variable to point to:<SPLDIROUT>/<SPLENVIRON></p>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Environment Name	<SPLENVIRON>	<p>A descriptive name to be used as both a directory name under the mount point <SPLDIR> and an environment descriptor. This value typically identifies the purpose of the environment. For example, DEV01 or CONV.</p> <p>On installation a directory <SPLDIR>/<SPLENVIRON> is created, under which the Oracle Utilities Application Framework and <Product Name> software resides.</p> <p>When multiple environments are set up on the machine you will typically have directories such as: /ouaf/DEV01/.... /ouaf/CONV/....</p> <p>Each of these contains a complete version of the Oracle Utilities Application Framework and <Product Name>.</p> <p>Note: Later in the installation process, the splenvIRON.sh (splenvIRON.cmd) script will set \$SPLEBASE (%SPLEBASE%) environment variable to point to <SPLDIR>/<SPLENVIRON></p>	
Web Application Server Type	<SPLWAS>	<p>A web application server for the environment to be used. The following value must be selected:</p> <p>Valid values: WLS: WebLogic</p> <p>Note: Not all web application servers are supported on all platforms; refer to Supported Platforms section for details.</p>	
Installation Application Viewer Module	<WEB_ISAPVIEWER>	<p>Denotes if the Application Viewer Web Module will be installed in the environment. When this value is set to false the application viewer will not be accessible in the environment.</p> <p>Valid values: true: Application Viewer module will be installed. false: Application Viewer module will not be installed.</p> <p>Default value: true</p> <p>Note: When the value of false is selected, the Application Viewer will only be installed at a later date by a complete reinstall of the application.</p>	
Install Demo Generation Cert Script	CERT_INSTALL_SCRIPT	<p>You can install/uninstall later by executing the following script: perl [INSTALL_PACKAGE_FOLDER]/installAR.plx</p> <p>Valid values: true: Demo Generation Cert Script will be installed. false: Demo Generation Cert Script will not be installed.</p> <p>Default value: true</p>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Install Sample CM Source Code	CM_INSTALL_SAMPLE	<p>You can install/uninstall later by executing the following script: perl [INSTALL_PACKAGE_FOLDER]/installAR.plx</p> <p>Valid values: true: Sample CM Source Code will be installed. false: Sample CM Source Code will not be installed.</p> <p>Default value: true</p>	

Environment Description

1. Environment Description
Environment Description:

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Environment Description	DESC	This is a free form text field to describe the purpose of the environment.	

WebLogic Business Application Server Configuration

The WebLogic parameters below and in the worksheet are for a WebLogic installation.

2. Business Application Server Configuration

Business Server Host:	<machine_name>
WebLogic Server Name:	myserver
Business Server Application Name:	SPLService
MPL Admin Port Number:	
MPL Automatic startup:	false

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Business Server Host	BSN_WLHOST	The host name on which the business application server resides. Default value: <current server name>	
WebLogic Server Name	BSN_WLS_SVRNAME	The name of the WebLogic server where the business application resides. Default value: myserver Note: If there is not a previously created WebLogic server, take the default value of “myserver”.	
Business Server Application Name	BSN_APP	The name of the business application server. Default value: SPLService	
MPL Admin Port number	MPLADMINPORT	The port number for the Multi Purpose Listener (MPL) Admin Server. Example value: 6502	
MPL Automatic Startup	MPLSTART	Automatically starts the MPL Listener whenever environment starts. Default value: false	

WebLogic Web Application Server Configuration

The WebLogic parameters below and in the worksheet are for a WebLogic installation.

3. Web Application Server Configuration

```

Web Server Host:                                     <machine_name>
Weblogic SSL Port Number:
Weblogic Console Port Number:
WebLogic Additional Stop Arguments:
Web Context Root:
WebLogic JNDI User ID:
WebLogic JNDI Password:
WebLogic Admin System User ID:
WebLogic Admin System Password:
WebLogic Server Name:                               myserver
Web Server Application Name:                         SPLWeb
Deploy Using Archive Files:                         true
Deploy Application Viewer Module:                   true
Enable The Unsecured Health Check Service:          false
MDB RunAs User ID:
Super User Ids:                                     SYSUSER
  
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Web Server Host	WEB_WLHOST	The host name on which the web application server resides. Default value: <current server name>	
Weblogic SSL Port Number	WEB_WLSSLPORT	The port number assigned to WebLogic Secure Sockets connection. This is the port number that is used for Secure Sockets connecting to the WebLogic server. For Production, additional actions are required. Do NOT run Production with Demo certificates Example value: 6501	
Weblogic Console Port Number	WLS_ADMIN_PORT	The port number to access the WebLogic Console using https You will use this port when accessing the WebLogic Console Example value: 6500	
Weblogic Additional Stop Arguments	ADDITIONAL_STOP_WEBLOGIC	This value will be needed when running the WebLogic Console using a different port number (e.g.) -Dweblogic.security.TrustKeyStore=DemoTrust -Dweblogic.security.TrustKeystoreType=CustomTrust	
Web Context Root	WEB_CONTEXT_ROOT	A context root name that allows customers to run multiple instances of web application on the same server. Default value: ouaf	
WebLogic JNDI User ID	WEB_WLSYSUSER	The user ID the application uses to connect to the EJB component through JNDI. This is the EJB container user ID. Note: The required value for an initial installation is "ouafjndi". This is a security value.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
WebLogic JNDI Password	WEB_WLSYSPASS	<p>The password the application uses to connect to the EJB component through JNDI.</p> <p>Note: The required value for an initial installation is “jndiadmin”. This value will be saved in encrypted format.</p> <p>This is a security value; it will be encrypted with the Oracle Application Framework Encryption Algorithm.</p>	
WebLogic Admin System User ID	WLS_WEB_WLSYSUSER	<p>The user ID to log in to the Oracle WebLogic console and to administer Oracle WebLogic. The Oracle WebLogic startup and stop script also utilizes this user ID</p> <p>Note: The installation utility will prompt you to enter “Y” to encrypt. For an initial installation, enter Y/y and specify the required value “system”.</p> <p>This is a security value; it will be encrypted with the Weblogic Encryption Algorithm.</p>	
WebLogic Admin System Password	WLS_WEB_WLSYSPASS	<p>The password to login to Oracle WebLogic console and to administer Oracle WebLogic. The Oracle WebLogic startup and stop script also utilize this password.</p> <p>Note: The installation utility will prompt you to enter “Y” to encrypt. For an initial installation, enter Y/y, and specify the required value “ouafadmin”.</p> <p>This is a security value; it will be encrypted with the Weblogic Encryption Algorithm.</p>	
WebLogic Server Name	WEB_WLS_SVRNAME	<p>The name of the WebLogic server where the web application resides.</p> <p>Default value: myserver</p> <p>Note: For an initial installation, use the default value of “myserver”.</p>	
Web Server Application Name	WEB_APP	<p>The name of the web application server.</p> <p>Default value: SPLWeb</p> <p>Note: For an initial installation, use the default value of “SPLWeb”.</p>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Deploy Using Archive Files	WEB_DEPLOY_EAR	<p>When the value is “false” the web application will be deployed in exploded directory format (no WAR/EAR files).</p> <p>When the value is “true”, the web application will be deployed in ear file format.</p> <p>Note: The expanded application folders will always exist under the application folder (<SPLEBASE>/splapp/applications), regardless of the setting of this option.</p> <p>Valid values: true (Deploy EAR files) false (Deploy expanded application folders)</p> <p>Default value: true</p>	
Deploy Application Viewer Module	WEB_DEPLOY_APPVIEWER	<p>When the value is “true” the application viewer will be deployed to the web server. When the value is “false”, the application viewer will not be deployed to the web Server.</p> <p>Note: With either value the application viewer module will still be managed by the upgrade process.</p> <p>Note: When the ‘Install Application Viewer module’ value is set to false from the installation menu, you will not be able to change this value to true to deploy the application viewer.</p> <p>Valid values: true: The application viewer module will be deployed to the web server false: The application viewer module will not be deployed to the web server</p> <p>Default value: true</p>	
Enable The Unsecured Health Check Service	WEB_ENABLE_HEALTHCHECK	Enables the health check feature of the application	
MDB RunAs User ID	WEB_IWS_MDB_RUNAS_USER	The message drive Java Bean RunAs user.	
Super User Ids	WEB_IWS_SUPER_USERS	<p>The application super users.</p> <p>Enter the super users separating them by commas.</p>	

Database Configuration

Note: 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:

4. Database Configuration

Application Server Database User ID:
 Application Server Database Password:
 MPL Database User ID:
 MPL Database Password:
 XAI Database User ID:
 XAI Database Password:
 Batch Database User ID:
 Batch Database Password:
 Web JDBC DataSource Name:
 JDBC Database User ID:
 JDBC Database Password:
 Database Name
 Database Server:
 Database Port:
 ONS Server Configuration:
 Database Override Connection String:
 Character Based Database:
 Oracle Client Character Set NLS_LANG: AMERICAN_AMERICA.AL32UTF8

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Application Server Database User ID	DBUSER	The database user ID that has been configured on the database for the application server connection. This is a security value.	
Application Server Database Password	DBPASS	The database password that has been configured on the database for the application connection. Note: This value will be saved in encrypted format. This is a security value; it will be encrypted with the Oracle Utilities Framework Encryption Algorithm.	
MPL Database User ID	MPL_DBUSER	The database user ID that has been configured on the database for the MPL server connection. This is a security value.	
MPL Database Password	MPL_DBPASS	The database password that has been configured on the database for the MPL server connection. Note: This value will be saved in encrypted format. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.	
XAI Database User ID	XAI_DBUSER	The database user ID that has been configured on the database for the XAI server connection. This is a security value.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
XAI Database Password	XAI_DBPASS	<p>The database password that has been configured on the database for the XAI server connection.</p> <p>Note: This value will be saved in encrypted format.</p> <p>This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.</p>	
Batch Database User ID	BATCH_DBUSER	<p>The database user ID that has been configured on the database for the batch connection.</p> <p>This is a security value.</p>	
Batch Database Password	BATCH_DBPASS	<p>The database password that has been configured on the database for the batch connection.</p> <p>Note: This value will be saved in encrypted format.</p> <p>This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.</p>	
Web JDBC DataSource Name	JDBC_NAME	<p>Populate in order to activate JDBC data source for online.</p> <p>If this is specified, and the environment is native/clustering, make sure that the data source specified, is manually created before the application deployment.</p> <p>When on Weblogic, leave empty to use UCP connection pooling.</p> <p>Example: TPWDataSource</p>	
JDBC Database User ID	DBUSER_WLS	<p>The database user ID that has been configured for the JDBC connection.</p> <p>Set this to the proper value if the Web JDBC DataSource Name is entered.</p> <p>Generally this is set to be same as Application Server Database Login credentials, Username: xxxxxx</p>	
JDBC Database Password	DBPASS_WLS	<p>The database user password that has been configured for the JDBC connection.</p> <p>Set this to the proper value if the Web JDBC DataSource Name is entered.</p> <p>This is a security value; it will be encrypted with the WebLogic Encryption Algorithm.</p> <p>Generally this is set to be same as Application Server Database Login credentials, Password: xxxxxx</p>	
Database Name	DBNAME	The name of the database instance that the application will be connecting to.	
Database Server	DBSERVER	Host name of the server where database resides.	
Database Port	DBPORT	Database port number on the database server used for connecting to the database	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
ONS Server Configuration	ONSCONFIG	ONS Server Configuration is required for Oracle RAC FCF. See the Server Administration Guide for more information. This is an optional value.	
Database Override Connection String	DB_OVERRIDE_CONNECTION	This connection string can be used to override the database information entered above for RAC installation. Set this string to override the standard database connection string, as entered above. See the Server Administration Guide for more information. This is an optional value.	
Character Based Database	CHAR_BASED_DB	Set to true if using a character based database.	
Oracle Client Character Set NLS_LANG	NLS_LANG	The Oracle Database Character Set. Select the Language and Territory that are in use in your country. Default value: AMERICAN_AMERICA.AL32UTF8	

General Configuration Options

Note: See the *Server Administration Guide* for additional details on this configuration.

5. General Configuration Options

```

Batch RMI Port:
RMI Port number for JMX Business:
RMI Port number for JMX Web:
JMX Enablement System User ID:
JMX Enablement System Password:
Coherence Cluster Name:
Coherence Cluster Address:
Coherence Cluster Port:
Coherence Cluster Mode:                                prod

```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Batch RMI Port	BATCH_RMI_PORT	Unique port used by the Batch RMI Example value: 6540	
RMI Port number for JMX Business	BSN_JMX_RMI_PORT_PERFORMANCE	Example value: 6550 Note: This is an optional value.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
RMI Port number for JMX Web	WEB_JMX_RMI_PORT_PERFORMANCE	Example value: 6570 Note: This is an optional value.	
JMX Enablement System User ID	BSN_JMX_SYSUSER	This is used to authenticate incoming JMX requests. Populate if RMI Port numbers are set. Note: This is an optional value.	
JMX Enablement System Password	BSN_JMX_SYSPASS	This is used to authenticate incoming JMX requests. Populate if RMI Port numbers are set. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm. Note: This is an optional value.	
Coherence Cluster Name	COHERENCE_CLUSTER_NAME	Unique name for the batch CLUSTER Note: Value is required when batch mode is CLUSTERED.	
Coherence Cluster Address	COHERENCE_CLUSTER_ADDRESS	Unique multicast address. Note: Value is required when batch mode is CLUSTERED.	
Coherence Cluster Port	COHERENCE_CLUSTER_PORT	Unique port for the batch CLUSTER Note: Value is required when batch mode is CLUSTERED.	
Coherence Cluster Mode	COHERENCE_CLUSTER_MODE	Valid values: dev (Development) prod (Production) Default value: dev	

SSL Certificate Keystore (Weblogic Only)

Note: See the <Product Name> *Security Guide* for additional details on this configuration. By default, SSL (Secure Sockets Layer) certificates are required for authentication. The product provides demo certificates generated with 1024 byte keys. For production environments, please use your own custom certificates.

6. SSL Certificate Keystore

Certificate Keystore Type:	CUSTOM
Identify Keystore File:	
Identify Keystore File Type:	jks
Identify Keystore Password:	
Identity Private Key Alias:	ouaf_demo_cert
Trust Keystore File:	
Trust Keystore File Type:	jks
Trust Keystore Password:	
Trust Private Key Alias:	ouaf_demo_cert

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Certificate Keystore Type	CERT_KS	<p>If you choose DEMO you need to execute the following script at least once</p> <pre>perl [SPLEBASE]/bin/demo_gen_cert.plx</pre> <p>If you change DEFAULT/CUSTOM to DEMO you need to have installed the demo_gen_cert.plx script, it is part of the demo source in the installation package.</p> <p>Default value: CUSTOM Valid values: DEFAULT,DEMO,CUSTOM</p> <p>The demo_gen_cert.plx script is available if you select the 'Install Demo Generation Cert Script' option during installation. It automates the creation of the Weblogic provided demo certificate using 1024 byte keys.</p>	
Identify Keystore Type	CERT_IDENT_KS_FILE	<p>Mandatory if the type is CUSTOM.</p> <p>No need to populate if type is DEMO, it will use: [SPLEBASE]/splapp/certs/ouaf_demo_ident.jks</p>	
Identify Keystore File Type	CERT_IDENT_KS_TYPE	Default value: jks	
Identify Keystore Password	CERT_IDENT_KS_PWD	This is a security value; it will be encrypted with the WebLogic Encryption Algorithm.	
Identity Private Key Alias	CERT_IDENT_KS_ALIAS	Default value: ouaf_demo_cert	
Trust Keystore File	CERT_TRUST_KS_FILE	<p>Mandatory if the type is CUSTOM.</p> <p>No need to populate if type is DEMO, it will use: [SPLEBASE]/splapp/certs/ouaf_demo_trust.jks</p>	
Trust Keystore File Type	CERT_TRUST_KS_TYPE	Default value: jks	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Trust Keystore Password	CERT_TRUST_KS_PWD	This is a security value; it will be encrypted with the WebLogic Encryption Algorithm.	
Trust Private Key Alias	CERT_TRUST_KS_ALIAS	Default value: ouaf_demo_cert	

OAAF TrustStore Options

Note: See the *Server Administration Guide* for additional details on this configuration.

The OAAF truststore configuration is required for IWS.

7. OAAF TrustStore Options

```

Import TrustStore Directory:
Store Type:                JCEKS
Alias:                     ouaf.system
Alias Key Algorithm:       AES
Alias Key Size:            128
HMAC Alias:                ouaf.system.hmac
Padding:                   PKCS5Padding
Mode:                      CBC

```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Import TrustStore Directory	TS_IMPORT_KEYSTORE_FOLDER	Populate this option if you want to import the TrustStore files from an external location. The import will happen only in case of initial install or initialSetup.sh cmd -S	
Store Type	TS_STORETYPE	Mandatory if setting the ouaf truststore. Value used for keytool option –storetype when creating/using the truststore.	
Alias	TS_ALIAS	Mandatory if setting the ouaf truststore. Value used for keytool option –alias when creating/using the truststore.	
Alias Key Algorithm	TS_ALIAS_KEYALG	Mandatory if setting the ouaf truststore. Value used for keytool option -keyalg when creating/using the truststore.	
Alias Key Size	TS_ALIAS_KEYSIZE	Mandatory if setting the ouaf truststore. Value used for keytool option -keysize when creating/using the truststore.	
HMAC Alias	TS_HMAC_ALIAS	Mandatory if setting the ouaf truststore. Value used for keytool option -alias For the HMAC alias, the following values are fixed: - HMAC Alias Key Algorithm: HmacSHA256 - HMAC Alias Key Size: 256	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Padding	TS_PADDING	Mandatory if setting the ouaf truststore. Value used for encryption/decryption	
Mode	TS_MODE	Mandatory if setting the ouaf truststore. Value used for encryption/decryption	

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
```

WebLogic Advanced Environment Miscellaneous Configuration

```
50. Advanced Environment Miscellaneous Configuration
Online JVM Batch Server Enabled: false
Online JVM Batch Number of Threads:5
Online JVM Batch Scheduler Daemon Enabled: false
Enable Batch Edit Funtionality:false
Batch Online Log Directory:
Enable Web Services Functionality: false
IWS deployment target:
Web Admin Server Host:
GIS Service Running on the same Web Server:true
GIS Service URL:
GIS WebLogic System User ID:
GIS WebLogic System Password:
Online Display Software Home:
Max Queries To Hold In Cache Across All Threads:
Seconds Timeout Flush Cache Completely:
```

Menu Option	Name Used in Documentation	Usage	Customer Value Install
Online JVM Batch Server Enabled	BATCHENABLED	<p>When starting a web application server JVM, this property can be set to “true” to allow the on-line application server to also act as a batch worker in the grid.</p> <p>Default value: false</p> <p>Note: This functionality should only be used in low volume environments.</p>	
Online JVM Batch Number of Threads	BATCHTHREADS	<p>The maximum number of batch processing threads to be executed within a worker JVM when no explicit Distributed Thread Pool is specified. The “DEFAULT” distributed thread pool is used by the batch-scheduling daemon when it initiates processing on batch jobs (typically added via the online system) where no thread pool is specified).</p> <p>Default value: 5</p> <p>Note: This will be only used and activated when BATCHENABLED is set to true.</p>	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
Online JVM Batch Scheduler Daemon Enabled	BATCHDAEMON	<p>In a distributed batch environment, this property can be set to “true” to allow a worker JVM to host the batch scheduling daemon. The daemon accepts online batch submissions requests and automatically submits the work for them.</p> <p>Valid values: true, false</p> <p>Default value: false</p> <p>Note: This will be only used and activated when BATCHENABLED is set to true.</p>	
Enable Batch Edit Functionality	BATCHEDIT_ENABLED	<p>Enable Batch Edit Functionality</p> <p>If enabled, use the bedit.sh cmd script in order to configure the batch</p> <p>Valid values: true, false</p> <p>Default value: false</p>	
Batch Online Log Directory	BATCH_ONLINE_LOG_DIR	This is required for the online batch retrieval feature.	
Enable Web Services Functionality	WEBSERVICES_ENABLED	<p>If enabled, execute the following commands in order to allow the application to re-deploy the Webservices without prompting for the user and password:</p> <ul style="list-style-type: none"> - Add weblogic.jar to the CLASSPATH - Execute: java weblogic.Admin -username [USER NAME] -password [PASSWORD] STOREUSERCONFIG -userconfigfile [SPLEBASE]/etc/.wlsuserconfig-userkeyfile [SPLEBASE]/etc/.wlsuserkey <p>Valid values: true, false</p> <p>Default value: false</p>	
IWS deployment target	WLS_CLUSTER_NAME	This is needed for Web Services deployment and is typically the Weblogic Cluster name. It is mandatory only if Web Services is enabled and the application is running in Weblogic Native mode.	
Web Admin Server Host	WEB_ADMIN_SERVER	It is used for the Web Services deployment. It is also used for importing the certificate from the Web Admin Server (initialSetup.sh cmd -i). If populated, it will override the Web Server Host.	
GIS Service Running on the same Web Server	GIS	<p>Geographical information (GEOCODING) - GIS Service running on the same web application server</p> <p>Valid values: true, false</p> <p>This value is optional. This value will only appear for WebLogic.</p>	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
GIS Service URL	GIS_URL	<p>This is the URL of the external web server.</p> <p>Note: This value will be only be used when GIS is set to true.</p> <p>This value is optional. This value will only appear for WebLogic.</p>	
GIS WebLogic System User ID	GIS_WLSYSUSER	<p>GIS WebLogic System User ID</p> <p>Note: This value will be only be used when GIS is set to true.</p> <p>This value is optional. This value will only appear for WebLogic.</p>	
GIS WebLogic System Password	GIS_WLSYSPASS	<p>GIS WebLogic System Password.</p> <p>Note: This value will be only be used when GIS is set to true.</p> <p>This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm. This value will only appear for WebLogic.</p>	
Online Display Software Home	ONLINE_DISPLAY_HOME	<p>The location of the Online Display Software installation directory.</p> <p>This value is optional.</p>	
Max Queries To Hold In Cache Across All Threads	XQUERIES_TO_CACHE	<p>Max number of queries to hold in the cache across all threads</p> <p>0 = no cache</p> <p>-1 or [empty] = unlimited</p>	
Seconds Timeout Flush Cache Completely	XQUERY_CACHE_FLUSH_TIMEOUT	<p>Number of seconds before cache is flushed Completely</p> <p>0 or [empty] = never auto-flush</p>	

WebLogic Advanced Environment Memory Configuration

51. Advanced Environment Memory Configuration

```

Web Application Java Initial Heap Size:      2048
Web Application Java Max Heap Size:         2048
Web Application Java Max Perm Size:         1024
Web Application Additional Options:
Global JVM Arguments:
Ant Min Heap Size:                          200
Ant Max Heap Size:                          800
Ant Additional Options:
Thread Pool Worker Java Min Heap Size:      512
Thread Pool Worker Java Max Heap Size:      1024
Thread Pool Worker Java Max Perm Size:      512
Thread Pool Worker Additional Options:
Additional Runtime Classpath:
  
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Web Application Java Initial Heap Size	WEB_MEMORY_OPT_MIN	Initial heap size for the application server. Default value: 1024 Note: For WebLogic installation only.	
Web Application Java Max Heap Size	WEB_MEMORY_OPT_MAX	Maximum heap size for the application server. Default value: 1024 Note: For WebLogic installation only.	
Web Application Java Max Perm Size	WEB_MEMORY_OPT_MAXPERMSIZE	Maximum Perm Size for the application server. Default value: 500MB (Linux, Solaris) 300MB (Windows, HP-UX) Note: For WebLogic installation only.	
Web Application Additional Options	WEB_ADDITIONAL_OPTS	Additional options that will be passed in to the web application server JVM. This is optional.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Global JVM Arguments	GLOBAL_JVMARGS	<p>JVM arguments that are passed to all Java server processes such as Weblogic Server, Threadpoolworkers and jobs.</p> <p>Arguments added to all jvms</p> <p>Defaults to -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=<TEMPDIR></p> <p>For AIX environment, please add the following argument for SSL communication-</p> <p>-Dcom.ibm.jsse2.overrideDefaultTLS=true</p>	
Ant Min Heap Size	ANT_OPT_MIN	<p>Minimum Heap Size passed to ANT JVM.</p> <p>Default value: 200</p>	
Ant Max Heap Size	ANT_OPT_MAX	<p>Maximum Heap Size passed to ANT JVM.</p> <p>Default value: 800</p>	
Ant Additional Options	ANT_ADDITIONAL_OPTION	Additional options that are passed into the ANT JVM.	
Thread Pool Worker Java Min Heap Size	BATCH_MEMORY_OPT_MIN	<p>Minimum heap size passed to the Thread Pool Worker.</p> <p>Default value: 512</p>	
Thread Pool Worker Java Max Heap Size	BATCH_MEMORY_OPT_MAX	<p>Maximum heap size passed to the Thread Pool Worker.</p> <p>Default value: 1024</p>	
Thread Pool Worker Java Max Perm Size	BATCH_MEMORY_OPT_MAXPERMSIZE	<p>Maximum perm size passed to the Thread Pool Worker</p> <p>Default value: 768</p>	
Thread Pool Worker Additional Options	BATCH_MEMORY_ADDITIONAL_OPT	Additional Memory Options passed into the Thread Pool Worker.	
Additional Runtime Classpath	ADDITIONAL_RUNTIME_CLASSPATH	<p>Additional Classpath Options passed in when starting the WebLogic JVM</p> <p>Note: For WebLogic installation only. This is an optional value.</p>	

Advanced Web Application Configuration

52. Advanced Web Application Configuration

```

Web Application Cache Settings:                off
Web Server Port Number:
WebLogic Overload Protection:                 system-exit
Domain Home Location:
Batch Cluster URL:
Strip HTML Comments:                         false
Authentication Login Page Type:               FORM
Web Form Login Page:                          /loginPage.jsp
Web Form Login Error Page:                    /formLoginError.jsp
Application Viewer Form Login Page:           /loginPage.jsp
Application Viewer Form Login Error Page:      /formLoginError.jsp
Help Form Login Page:                         /loginPage.jsp
Help Form Login Error Page:                   /formLoginError.jsp
Web Security Role:                            cisusers
Web Principal Name:                           cisusers
Application Viewer Security Role:              cisusers
Application Viewer Principal Name:             cisusers
This is a development environment:            false
Preload All Pages on Startup:                  false
Maximum Age of a Cache Entry for Text:         28800
Maximum Age of a Cache Entry for Images:       28800
JSP Recompile Interval (s):                   43200

```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Web Application Cache Settings	WEB_I2_CACHE_MODE	Default value: off Valid values: off read_write read_only	
Web Server Port Number	WEB_WLPORT	The port number assigned to WebLogic connection. Set this port if the environment is not configured as SSL. Note: For WebLogic installation only. This value is optional. Example Value: 6500	
WebLogic Overload Protection	WLS_OVERRIDE_PROTECT	The overload protection allows for a Weblogic server to be “stopped / exited” when there is an out of memory exception Valid values: system-exit (Exit the server process) no-action (Ignore take no action) Default value: system-exit Note: For WebLogic installation only.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Domain Home Location	WLS_DOMAIN_HOME	<p>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).</p> <p>Note: For WebLogic installation only</p> <p>This value is optional</p>	
Batch Cluster URL	WEB_BATCH_CLUSTER_URL	Example: service:jmx:rmi:///jndi/rmi://[host]:[JMX port]/oracle/ouaf/batchConnector	
StripHTMLComments: false	STRIP_HTML_COMMENTS	<p>Stripping HTML (and JavaScript) comments will increase the security of the system.</p> <p>Default value: false</p> <p>Valid values: true, false</p>	
Authentication Login Page Type	WEB_WLAUTHMETHOD	<p>Specifies which authentication mode should be used. To switch off OUAF Login Page enter: BASIC</p> <p>Valid values: FORM, BASIC</p> <p>Default value: FORM</p>	
Web Form Login Page	WEB_FORM_LOGIN_PAGE	<p>Specify the jsp file used to login into the application.</p> <p>Default value: /loginPage.jsp</p>	
Web Form Login Error Page	WEB_FORM_LOGIN_ERROR_PAGE	<p>Specify the jsp file used when there is an error when logging into the application.</p> <p>Default value: /formLoginError.jsp</p>	
Application Viewer Form Login Page	WEB_APPVIEWER_FORM_LOGIN_PAGE	<p>Specify the jsp file used to login into the application viewer application.</p> <p>Default value: /loginPage.jsp</p>	
Application Viewer Form Login Error Page	WEB_APPVIEWER_FORM_LOGIN_ERROR_PAGE	Specify the jsp file used when there is an error when logging into the application viewer application.	
Help Form Login Page	WEB_HELP_FORM_LOGIN_PAGE	<p>Specify the jsp file used to login into the help application.</p> <p>Default value: /loginPage.jsp</p>	
Help Form Login Error Page	WEB_HELP_FORM_LOGIN_ERROR_PAGE	<p>Specify the jsp file used when there is an error when logging into the help application.</p> <p>Default value: /formLoginError.jsp</p>	
Web Security Role	WEB_PRINCIPAL_NAME	<p>Specify the name of the security role.</p> <p>Default value: cisusers</p>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Web Principal Name	WEB_PRINCIPAL_NAME	Specify the name of a principal that is defined in the security realm. Default value: cisusers	
Application Viewer Security Role	WEB_APPVIEWER_ROLE_NAME	Specify the name of the security role. Default value: cisusers	
Application Viewer Principal Name	WEB_APPVIEWER_PRINCIPAL_NAME	Specify the name of a principal that is defined in the security realm. Default value: cisusers	
This is a development environment	WEB_ISDEVELOPMENT	If the value is “true”, the web application may be used for application development, which will trigger certain generation processes. If the value is “false” the environment will be used as a runtime environment. When you choose “true” (development environment) the startup preload pages will be disabled, and the application security will be less strict. This value also controls the amount of logging information written to the application log files. Valid values: true, false Default value: false	
Preload All Pages on Startup	WEB_PRELOADALL	This controls if the pages should be pre-loaded during the startup of the application or not. Valid values: true, false Default value: false	
Maximum Age of a Cache Entry for Text	WEB_MAXAGE	Default value: 28800	
Maximum Age of a Cache Entry for Images	WEB_MAXAGEI	Default value: 28800	
JSP Recompile Interval (s)	WEB_wlpageCheckSeconds	Default value: 43200 Note: For Weblogic Installation only.	

WebLogic Diagnostics

54. WebLogic Diagnostics

Diagnostic Context Enabled:	false
Diagnostic Volume:	Off
Built-in Module:	None

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Diagnostic Context Enabled	WLS_DIAGNOSTIC_CONTEXT_ENABLED	Enable or disable diagnostic context for the WebLogic Server (WLDF or the weblogic diagnostic framework) Default value: false Valid values: true, false	
Diagnostic Volume	WLS_DIAGNOSTIC_VOLUME	Specifies the volume of diagnostic data that is automatically produced by WebLogic Server at run time Default value: Off Valid values: Off,Low,Medium,High	
Built-in Module	WLS_DIAGNOSTIC_BUILT_IN_MODULE	Specifies the WLDF built-in system resource type to use. If not specified will use the weblogic default.	

OIM Configuration Settings

53. OIM Configuration Settings

SPML SOAP Trace Setting:	false
SPML IDM Schema Name:	F1-IDMUser
SPML OIM Name Space:	http://xmlns.oracle.com/OIM/provisioning
SPML OIM Enclosing Element:	SOAElement

Menu Option	Name Used in Documentation	Usage	Customer Install Value
SPML SOAP Trace Setting	OIM_SPML_SOAP_DEBUG_SETTING	Name of Oracle Identity Manager library for debug Default value: false Valid values: true, false	
SPML IDM Schema Name	OIM_SPML_UBER_SCHEMA_NAME	Name of Oracle Identity Manager library for schema Default value: F1-IDMUser	
SPML OIM Name Space	OIM_SPML_NAME_SPACE	Default Namespace for Oracle Identity Manager integration Default value: http://xmlns.oracle.com/OIM/provisioning	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
SPML OIM Enclosing Element	OIM_SPML_SOAP_ELEMENT	Default top level SOAP Element name for Oracle Identity Manager integration Default value: sOAPElement	

Cloud Related Options

55. Cloud Related Options

Restriction URLs Enable:
 White List Full Path:
 Custom White List Full Path:
 File Parameter Validation:
 Substitution Variable List File Location:
 Directory For Variable F1_MIGR_ASSISTANT_FILES:
 Directory For Variable F1_BI_EXTRACT:
 Directory For Variable F1_PROD_INTER_FILES:
 Directory For Variable F1_CUST_APP_BASE:
 Directory For Variable F1_PROCESS_DIR:
 Directory For Variable F1_SVC_CATALOG_WSDL_DIR:

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Restriction URLs Enable	CLOUD_RESTRICTION_URLS_ENABLE	Default value: false	
White List Full Path	CLOUD_WHITE_LIST_PATH	Full path name of whiteList.xml	
Custom White List Full Path	CLOUD_CUSTOM_WHITE_LIST_PATH	Full path name of CM_whiteList.xml	
File Parameter Validation	CLOUD_FILE_PARAMETER_VALIDATION	For cloud installations it must be set to true. Default value: false	
Substitution Variable List File Location	CLOUD_SUBSTITUTION_VARIABLE_LIST_FILE_LOCATION	Full path to the xml file that contains the list of allowed directories and their corresponding substitution variables. Default value: <SPLEBASE>/etc/substitutionVariableList.xml	
Directory For Variable F1_MIGR_ASSISTANT_FILES	CLOUD_LOCATION_F1_MIGR_ASSISTANT_FILES	Default value: <SPLOUTPUT>/F1_MIGR_ASSISTANT_FILES	
Directory For Variable F1_BI_EXTRACT	CLOUD_LOCATION_F1_BI_EXTRACT	Default value: <SPLOUTPUT>/F1_BI_EXTRACT	
Directory For Variable F1_PROD_INTER_FILES	CLOUD_LOCATION_F1_PROD_INTER_FILES	Default value: <SPLOUTPUT>/F1_PROD_INTER_FILES	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Directory For Variable F1_CUST_APP_BASE	CLOUD_LOCATION_ F1_CUST_APP_BASE	Default value: <SPLOUTPUT>/F1_CUST_APP_BASE	
Directory For Variable F1_PROCESS_DIR	CLOUD_LOCATION_ F1_PROCESS_DIR	Default value: <SPLOUTPUT>/F1_PROCESS_DIR	
Directory For Variable F1_SVC_CATALOG_ WSDL_DIR	CLOUD_LOCATION_ F1_SVC_CATALOG_ WSDL_DIR	Default value: <SPLOUTPUT>/ F1_SVC_CATALOG_WSDL_DIR	

Service and Measurement Data Foundation 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 [Chapter 6: Installing the Application Server Component of Oracle Utilities Service and Measurement Data Foundation](#). 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 [Chapter 6: Installing Application Server Prerequisite Software](#).

WebLogic OSB Configuration

8. OSB Configuration

```

OSB Home:
OSB Host Server: <machine name>
OSB Port Number:
OSB 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:
OSB Weblogic User Password:
Mount point for OSB files: /spl/sploutput/osb
  
```

Table 1:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
OSB Home	OSB_HOME	Location of the directory where OSB is installed. For Example: Unix: /middleware/osb Windows: C:\middleware\osb	
OSB Host Server	OSB_HOST	Host name of the server where the OSB WebLogic server instance will run. Default Value: <current server name>	
OSB Port Number:	OSB_PORT_NUMBER	Admin port number of the OSB WebLogic server instance. Note: This also specifies the port number on which the example OSB WebLogic server will listen.	

Table 1:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
OSB SSL Port Number	OSB_SSL_PORT	<p>SSL Admin port number of the OSB Weblogic server instance.</p> <p>This is the port number that is used as a part of the OSB URL request to connect to the host. This value is required for creation of example OSB Weblogic server instance.</p>	
JDBC URL for database	DBURL_OSB	<p>The JDBC URL of the database where the OSB Schemas are located.</p> <p>For Example: jdbc:oracle:thin:@host:port:OSBDB</p> <p>This value is required for the example WebLogic server instance.</p>	
OSB Service Table Schema Name	RCUSTBSHEMA_OSB	<p>OSB Schema name or prefix used when RCU is executed. Example: <PREFIX>_STB</p> <p>This value is required for the example WebLogic server instance.</p>	
OSB Service Table Schema Password	RCUSTBSCHEMAPWD_OSB	<p>Password of OSB Schema used.</p> <p>This value is required for the example WebLogic server instance.</p>	
OSB WebLogic User Name	WEBLOGIC_USERNAME_OSB	<p>WebLogic user ID for the WebLogic instance where the OSB adapter will be deployed.</p> <p>This value is required for the example WebLogic server instance.</p>	
OSB WebLogic User Password	WEBLOGIC_PASSWORD_OSB	<p>WebLogic user password for the WebLogic instance where the OSB adapter will be deployed.</p> <p>This value is required for the example WebLogic server instance.</p>	
OSB WebLogic User Password	OSB_PASS_WLS	<p>WebLogic user password for the WebLogic instance where the OSB adapter will be deployed.</p> <p>This value is required for Oracle Utilities Application Framework to connect to OSB.</p>	

Table 1:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Mount point for OSB files	OSB_LOG_DIR	Location of the network share or mount point where the OSB files will be dropped. This path should be accessible from the machine where OSB WebLogic instance is running. For example: /ouaf/osb/<ENVIRONMENT NAME>/ Default Value: /spl/sploutput/osb	

WebLogic SOA Configuration

9. SOA Configuration

SOA Home:

SOA Host Server:

<machine name>

SOA Port Number:

SOA SSL Port Number:

JDBC URL for database:

Database User Name (SOAINFRA):

Database Password (SOAINFRA):

Database User Name (MDS):

Database Password (MDS):

Database User Name (ORASDPM):

Database Password (ORASDPM):

Specify the path for XAI/IWS Service

Table 2:

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
SOA Home	SOA_HOME	Location of the directory where SOA is installed. For Example: Unix: /middleware/Soa Windows: C:\middleware\Soa	
SOA Host Server	SOA_HOST	Host name of the server where the SOA WebLogic server instance will run. Default Value: <current server name>	
SOA Port Number:	SOA_PORT_NUMBER	Admin port number of the SOA WebLogic server instance. This is the port number that is used as a part of the SOA URL request to connect to the host.	
SOA SSL Port Number	SOA_SSL_PORT_NUMBER	Admin port number of the SOA WebLogic server instance. This is the port number that is used as a part of the SOA URL request to connect to the host. This value is required for the example WebLogic server instance.	
JDBC URL for database	DBURL_SOA	The JDBC URL of the database where the SOA schemas are located. For Example: jdbc:oracle:thin:@host:port:SOADB	

Table 2:

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
SOA Service table schema Name	RCUSTBSHEMA_SOA	SOA Schema name or prefix used when RCU is executed. Example: <PREFIX>_STB This value is required for the example WebLogic server instance.	
SOA Service table schema Password	RCUSTBSCHEMAPWD_SOA	Password of SOA Schema This value is required for the example WebLogic server instance.	
SOA Weblogic User Name	WEBLOGIC_USERNAME_SOA	WebLogic user ID for the WebLogic instance where the SOA adapter will be deployed. This value is required for the example WebLogic server instance.	
SOA Weblogic User Password	WEBLOGIC_PASSWORD_SOA	WebLogic user password for the WebLogic instance where the SOA adapter will be deployed. This value is required for the example WebLogic server instance.	
Specify the path for XAI/IWS Service	WEB_SERVICE_PATH	Path for XAI/IWS Service. This value is required to choose between XAI/IWS Services	

WebLogic SOA Configuration Plan

This configuration is required for installing the following adapters:

- Oracle Utilities Smart Grid Gateway Adapter for Itron OpenWay

10. SOA Configuration Plan (MDF)

```

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
MDF SOA Notify Queue JNDI Name: queue/BulkNotifyQueue
MDF SOA Commnad Queue JNDI Name: queue/BulkCommandQueue
SGG-NMS Test Harness Partition Name: SGG-NMS Test
  
```

Table 3:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
MDF Bulk Request Callback URL	D1_BULK_REQUEST_CALLBACK_URL	This is the URL from the edge application that receives any fault responses in Bulk Command BPEL processing. Default value: empty	
MDF Headend http connection timeout	D1_HEADEND_HTTP_CONN_TIMEOUT	MDF Headend http connection timeout value. Default value: 50000	
MDF Headend http read timeout	D1_HEADEND_HTTP_READ_TIMEOUT	MDF Headend http read timeout value. Default value: 500000	
MDF SOA Request Queue JNDI Name	SOA_REQUEST_QUEUE_D1	MDF SOA Request Queue JNDI Name. Default Value: queue/BulkRequestQueue	
MDF SOA Notify Queue JNDI Name	SOA_NOTIFY_QUEUE_D1	MDF SOA Notify Queue JNDI Name. Default Value: queue/BulkNotifyQueue	
MDF SOA Commnad Queue JNDI Name	SOA_COMMAND_QUEUE_D1	MDF SOA Commnad Queue JNDI. Default Value: queue/BulkCommandQueue	
SGG-NMS TestHarness Partition Name	SOA_PARTITION_D1	SGG-NMS TestHarness Partition Name Default Value: SGG-NMS_Test	

Configuration for DataRaker Integration

11. Configuration for DataRaker Integration

Destination Queue to publish SGG payloads
for DataRaker Integration Tool:

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 second 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

Table 4:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Destination Queue to publish SGG payloads for DataRaker Integration Tool	SGG_DR_INT_QUEUE	JNDI name of Destination Queue to publish SGG payloads for DataRaker Integration Tool. Default value: DataRakerQueue	
Number of records (SGG Payloads) to accumulate	SOA_DR_PUBLISH_SIZE	Number of records (SGG Payloads) to accumulate. Default value: 100	
Max file size for the accumulated (SGG Payloads) file in Kilobytes	SOA_DR_FILE_SIZE	Max file size for the accumulated (SGG Payloads) file in Kilobytes. Default value: 524288	
Specify a time which, when exceeded, causes a new outgoing file to be created in seconds	SOA_DR_ELAPSED_TIME	Specify a time which, when exceeded, causes a new outgoing file to be created in seconds. Default Value: 600	
Polling frequency of Staging directory for new files in seconds	SOA_DR_POLLING_FREQ	Polling frequency of Staging directory for new files in seconds. Default Value: 60	

Table 4:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Mount point/directory for the accumulated SGG payload file	SOA_DR_STAGING_DIR	Mount point/directory for the accumulated SGG payload file. Default Value: /spl/sploutput/staging	
Mount Point/directory for the converted XML file to place for DataRaker	SOA_DR_INTEGRATION_DIR	Mount Point/directory for the converted XML file to place for DataRaker. Default Value: /spl/sploutput/int	

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

60. Advanced Configurations for OSB

```
Enable OSB SSL Port: true
OSB Trust Keystore Type: Demo
OSB Trust Keystore File Type : JKS
OSB Trust Keystore File:
```

Table 5:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Enable OSB SSL Port	OSB_SSL	To enable SSL for OSB deployment set this as 'true' else set to 'false'. Valid Values: true,false Default value: true	
OSB Trust Keystore Type	OSB_TRUST_KS	Specify whether OSB server is using Demo or Custom trust. Valid Values:Demo,Custom Default value: Demo	
OSB Trust Keystore File Type	OSB_TRUST_KS_TYPE	Specify the Trust store Type for OSB. Valid Values:JKS,JCEKS Default Value:JKS If OSB Trust Keystore Type is Demo, Please specify JKS	
OSB Trust Keystore File	OSB_TRUST_KS_FILE	The path and file name of the Trust Keystore. No need to input this if OSB Trust Keystore Type is Demo	

Advanced Environment Memory Configurations

61. Advanced Memory Configurations for SOA

```
SOA Initial Heap Size: 1024
SOA Maximum Heap Size: 2048
SOA Minimum Perm Size: 512
SOA Maximum Perm Size: 1024
SOA Application Additional Options:
```

The name of the OWSM policy to use when SOA calls another SOA service:
 oracle/http_basic_auth_over_ssl_client_policy

The name of the OWSM policy to use when SOA is called by another SOA service:
 oracle/http_basic_auth_over_ssl_service_policy

The name of the OWSM policy to use when SOA calls an OUA service:
 oracle/http_basic_auth_over_ssl_client_policy

Table 6:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
SOA Initial Heap Size	SOA_MEMORY_OPT_MIN	Initial heap size for the SOA server. Default value: 1024 Note: For WebLogic installation only.	
SOA Maximum Heap Size	SOA_MEMORY_OPT_MAX	Maximum heap size for the SOA server. Default value: 2048 Note: For WebLogic installation only.	
SOA Minimum Perm Size	SOA_MEMORY_OPT_MINPERMSIZE	Maximum Perm Size for the SOA server. Default value: 512 Note: For WebLogic installation only.	
SOA Maximum Perm Size	SOA_JVM_ADDITIONAL_OPT	Additional options that will be passed in to the SOA server JVM. Optional Entry. Note: For WebLogic installation only.	
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 calls another SOA service Default Value: oracle/http_basic_auth_over_ssl_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 is called by another SOA service Default Value: oracle/http_basic_auth_over_ssl_service_policy	

Table 6:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
The name of the OWSM policy to use when SOA calls an OUA service	SOA_SOA_SERVICE_POLICY	The name of the OWSM policy to use when SOA calls an OUA service. Default Value: oracle/ http_basic_auth_over_ssl_client_policy	

62. Advanced Memory Configurations for OSB

OSB Initial Heap Size: 512
 OSB Maximum Heap Size: 1024
 OSB Minimum Perm Size: 512
 OSB Maximum Perm Size: 1024
 OSB Application Additional Options:

Table 7:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
OSB Initial Heap Size	OSB_MEMORY_OPT_MIN	Initial heap size for the OSB server. Default value: 512 Note: For WebLogic installation only	
OSB Maximum Heap Size	OSB_MEMORY_OPT_MAX	Maximum heap size for the OSB server. Default value: 1024 Note: For WebLogic installation only.	
OSB Minimum Perm Size	OSB_MEMORY_OPT_MINPERMSIZE	Maximum Perm Size for the OSB server. Default value: 512 Note: For WebLogic installation only.	
OSB Maximum Perm Size	OSB_MEMORY_OPT_MAXPERMSIZE	Maximum Perm Size for the OSB server. Default value: 1024 Note: For WebLogic installation only.	
OSB Application Additional Options	OSB_JVM_ADDITIONAL_OPT	Additional options that will be passed in to the OSB server JVM. Optional Entry. Note: For WebLogic installation only.	

63. Data Migration

Enable Data Migration: FALSE
 Data Migration Database User:
 Data Migration Database Password:

Table 8:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Enable Data Migration	DATA_MIGRATION	Specify to enable Data Migration Functionality. Valid Values: TRUE,FALSE Default value: FALSE	
Data Migration Database User	DATA_MIGRATION_DB_USER	User name of the Data Migration Database.	
Data Migration Database Password	DATA_MIGRATION_DB_PASS	Password of the Data Migration Database.	

64. Advanced Configurations for SOA

```

Enable SOA SSL Port:true
SOA Trust Keystore Type: Demo
SOA Trust Keystore File Type :JKS
SOA Trust Keystore File:

```

Table 9:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
Enable SOA SSL Port	SOA_SSL	To enable SSL for SOA deployment set this as 'true' else set to 'false'. Valid Values: true, false Default value: true	
SOA Trust Keystore Type	SOA_TRUST_KS	Specify whether SOA server is using Demo or Custom trust Valid Values: Demo, Custom Default value: Demo	
SOA Trust Keystore File Type	SOA_TRUST_KS_TYPE	Specify the Trust store Type for SOA. Valid Values: JKS, JCEKS Default Value: JKS If SOA Trust Keystore Type is Demo, Please specify JKS.	

Table 9:

Menu Option	Name Used In Documentation	Usage	Customer Install Value
SOA Trust Keystore File	SOA_TRUST_KS_FILE	The path and file name of the Trust Keystore. No need to input this if SOA Trust Keystore Type is Demo	

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 [Chapter 6: Installing the Application Server Component of Oracle Utilities Service and Measurement Data Foundation](#). 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 [Chapter 6: Installing Application Server Prerequisite Software](#).

This section includes worksheets for the following adapters:

- [For the Adapter Development Kit](#)
- [For the Adapter for Networked Energy Services](#)
- [For the Adapter for Itron OpenWay](#)
- [For the Adapter for Landis+Gyr](#)
- [For the Adapter for Sensus RNI](#)
- [For the Adapter for Silver Spring Networks](#)

For the Adapter Development Kit

```
21. DG Reference Implementation SOA Configurations
   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
```

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
DG SOA Partition Name	SOA_PARTITION_DG	SOA DG partition name. Default Value: DG	DG
MR Server Endpoint URI	Headend_MR_Server_DG	URL for the headend system running the MR service. For Example: http://localhost:port/soa-infra/services/DG_Test/DGTestHarness/MR_Server	
CD Server Endpoint URI	Headend_CD_Server_DG	URL for the headend system running CD service For Example: http://localhost:port/soa-infra/services/DG_Test/DGTestHarness/CD_Server	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
OD Server Endpoint URI	Headend_OD_Server_DG	URL for the headend system running OD service For Example: http://localhost:port/soa-infra/services/DG_Test/DGTestHarness/OD_Server	
Headend Http Read Timeout	Headend_http_read_timeout_DG	Headend http read timeout value Default Value: 500000	
Headend Http Connection Timeout	Headend_http_conn_timeout_DG	Headend Http Connection Timeout value Default Value: 50000	

For the Adapter for Networked Energy Services

17. SOA Configuration Plan (NES)

NES endpoint URI:

The SOA partition to which the application is installed:

The path to the NES EventManager web service on the head end system:

The path to the NES GatewayManager web service:

The path to the NES DeviceManager web service on the head end system:

The path to the NES SettingManager web service on the head end system:

The path to the NES UserManager web service on the head end system:

The name of the OWSM policy to use when SOA calls a head end system:

The name of the OWSM policy to use when SOA is called by a head end system:

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
NES endpoint URI	HEADEND_NES	NES endpoint URI	
The SOA partition to which the application is installed	SOA_PARTITION_D4	The SOA partition to which the application is installed: Default Value: Echelon	Echelon
The path to the NES EventManager web service on the head end system	HEADEND_EVENT-MANAGER_D4	The path to the NES EventManager web service on the head end system: Default Value: CoreServices/EventManager.asmx	
The path to the NES GatewayManager web service	HEADEND_GATEWAYMANAGER_D4	The path to the NES GatewayManager web service: Default Value: CoreServices/GatewayManager.asmx	
The path to the NES DeviceManager web service on the head end system	HEADEND_DEVICE-MANAGER_D4	The path to the NES DeviceManager web service on the head end system: Default Value: CoreServices/DeviceManager.asmx	
The path to the NES SettingManager web service on the head end system	HEADEND_SETTINGMANAGER_D4	The path to the NES SettingManager web service on the head end system: Default Value: CoreServices/SettingManager.asmx	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
The path to the NES UserManager web service on the head end system	HEADEND_USER-MANAGER_D4	The path to the NES UserManager web service on the head end system: Default Value: CoreServices/UserManager.asmx	
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 calls a head end system. Default Value: 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	D4_SOA_HE_SERVICE_POLICY	The name of the OWSM policy to use when SOA is called by a head end system. Default Value: oracle/http_basic_auth_over_ssl_service	

For the Adapter for Itron OpenWay

22. SOA Configuration Plan (Itron OpenWay)

Itron SOA Partition Name: Itron

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:

The name of the OWSM policy to use when SOA calls a head end system:

The name of the OWSM policy to use when SOA is called by a head end system:

Note: Replace localhost and port with respective host and port for the below mentioned Endpoint URLs.

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
Itron SOA Partition Name	SOA_PARTTTION_D8	Itron SOA Partition Name Default Value: Itron	Itron
Headend Http Read Timeout	HEADEND_HTTP_READ_TIMEOUT_D8	Headend Http Read Timeout Default Value: 500000	
Headend Http Connection Timeout	HEADEND_HTTP_CONNECTION_TIMEOUT_D8	Headend Http Connection Timeout Default Value: 50000	
DataSubscriberService Output Path	DATASUBSCRIBER_OUTPUT_PATH_D8	Directory path for DataSubscriberService Output	
ExceptionSubscriberService Output Path	EXCEPTIONSUBSCRIBER_OUTPUT_PATH_D8	Directory path for ExceptionSubscriberService For example: Output	
Itron Headend DataService Endpoint URI	Headend_DataService_D8	URL for Itron Headend DataService Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/DataService390	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
Itron Headend DiagnosticService Endpoint URI	Headend_DiagnosticService_D8	URL for Itron Headend DiagnosticService Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/DiagnosticService390	
Itron Headend UtilService Endpoint URI	Headend_UtilService_D8	URL for Itron Headend UtilService Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/UtilService	
Itron Headend ControlService Endpoint URI	Headend_ControlService_D8	URL for Itron Headend ControlService Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/ControlService39	
Itron Headend ProvisioningService Endpoint URI	Headend_ProvisioningService_D8	URL for Itron Headend ProvisioningService Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/ProvisioningService39	
Itron Headend ProvisioningService370 Endpoint URI	Headend_ProvisioningService370_D8	URL for Itron Headend ProvisioningService370 Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/ProvisioningService37	
Itron Headend ControlService370 Endpoint URI	Headend_ControlService370_D8	URL for Itron Headend ControlService370 Endpoint For Example: http://localhost:port/soa-infra/services/Itron_Test/ItronTestHarness/ControlService370	
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 calls a head end system Default Value: oracle/http_basic_auth_over_ssl_client_policy	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
The name of the OWSM policy to use when SOA is called by a head end system	D8_SOA_HE_SERVICE_POLICY	The name of the OWSM policy to use when SOA is called by a head end system Default Value: oracle/http_basic_auth_over_ssl_service_policy	

For the Adapter for Landis+Gyr

16. SOA Configuration Plan

LG SOA Partition Name:

LG SOA TestHarness Partition Name:

AMI Event Subscriber Output Path:

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:

Security policy attached to inbound web service calls from a CIM interface:

The name of the OWSM policy to use when SOA calls a head end system:

The name of the OWSM policy to use when SOA is called by a head end system:

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
LG SOA Partition Name	SOA_PARTITION_D3	SOA LG partition name. Default Value: LG	LG
LG SOA TestHarness Partition Name	SOA_PARTITION_TEST_D3	SOA LG Test Harness Partition Name Default Value: LG_Test	
AMI Event Subscriber Output Path	AMIEVENTSUBSCRIBER_OUTPUT_PATH_D3	Directory path for received events	
MR_Server endpoint URI	Headend_MR_Server_D3	URL for the head-end system running the MR_CB service. For Example: http://localhost:port/soa-infra/services/LG_Test/LGTestHarness/MR_CBService	
CD_Server endpoint URI	Headend_CD_Server_D3	URL for the head-end system running the CD_CB service. For Example: http://localhost:port/soa-infra/services/LG_Test/LGTestHarness/CD_CBService	
CIM endpoint URI	Headend_CIM_Server_D3	URL for the head-end system running the CIM service. For Example: http://localhost:port/soa-infra/services/LG_Test/LGTestHarness/LGCIMService	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
Metering Server end-point URI	Headend_Metering_Server_D3	URL for the head-end system running the Metering Service For Example: http://localhost:port/soa-infra/services/LG_Test/LGTestHarness/MeteringService	
Security policy attached to outbound web service calls to a CIM interface	SOA_HE_CIM_CLIENT_POLICY	Security policy attached to outbound web service calls to a CIM interface	
Security policy attached to inbound web service calls from a CIM interface	SOA_HE_CIM_SERVICE_POLICY	Security policy attached to inbound web service calls from a CIM interface	
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 calls a head end system	
The name of the OWSM policy to use when SOA is called by a head end system	D3_SOA_HE_SERVICE_POLICY	The name of the OWSM policy to use when SOA is called by a head end system	

For the Adapter for Sensus RNI

18. SOA Configuration Plan (Sensus)

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:

The name of the OWSM policy to use when SOA is called by a head end system:

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
Sensus SOA Partition Name	SOA_PARTITION_D6	Sensus SOA Partition Name Default Value: Sensus	Sensus
MR Server Endpoint URI	HEADEND_MR_D6	URL for the headend system running the MR service. For Example: http://host:port/multispeakv4-mr-ws	
CD Server Endpoint URI	HEADEND_CD_D6	URL for the headend system running CD service For Example: http://host:port/multispeakv4-cd-ws	
OD Server Endpoint URI	HEADEND_OD_D6	URL for the headend system running OD service For Example: http://host:port/multispeakv4-cd-ws	
Headend Http Read Timeout	Headend_http_read_timeout_D6	Headend http read timeout value Default Value: 500000	
Headend Http Connection Timeout	Headend_http_conn_timeout_D6	Headend Http Connection Timeout value Default Value: 50000	
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 calls a head end system Default Value: oracle/http_basic_auth_over_ssl_client_policy	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
The name of the OWSM policy to use when SOA is called by a head end system	D6_SOA_HE_SERVICE_POLICY	The name of the OWSM policy to use when SOA is called by a head end system Default Value: oracle/http_basic_auth_over_ssl_service_policy	

For the Adapter for Silver Spring Networks

SOA Configuration Plan (SSN)

19. SOA Configuration Plan (SSN)

SSN SOA Partition Name: SSN

SOA WebLogic User Name:

SOA Weblogic User Password:

SSN SOA Queue JNDI Name: queue/SSNODRQ

SSN Headend DataAggregation Endpoint URI:

The url for the SSN 4.7 DataAggregation service (DataAggregation.asmx):

The url for the SSN 4.10 DataAggregation service:

SSN Headend DeviceManager Endpoint URI:

The url for the SSN 4.7 DeviceManager service (DeviceManager.asmx):

The url for the SSN 4.10 DeviceManager service:

SSN Headend DeviceResults Endpoint URI:

The url for the SSN 4.7 DeviceResults service (DeviceResults.asmx):

The url for the SSN 4.10 DeviceResults service:

SSN Headend JobManager Endpoint URI:

The url for the SSN 4.7 JobManager service (JobManager.asmx):

The url for the SSN 4.10 JobManager service:

The name of the OWSM policy to use when SOA calls a head end system:

The name of the OWSM policy to use when SOA is called by a head end system:

Note: Replace localhost and port with your respective host and port for the Endpoint URLs listed below.

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
SOA Partition Name	SOA_PARTITION_D7	SOA SSN partition name. Default Value: SSN	
SOA Queue JNDI Name	SOA_QUEUE_D7	SOA queue JNDI name. Default Value: queue/SSNODRQ	
Headend DataAggregation Endpoint URI	Headend_DataAggregation_Server_D7	URL for headend DataAggregation Endpoint. Example: http://localhost:7001/soa-infra/services/SSN_Test/SSNTestHarness / DataAggregationService	
The url for the SSN 4.7 DataAggregation service (DataAggregation.asmx)	Headend_DataAggregation_47_Server_D7	URL for version 4.7 headend DataAggregation Endpoint. Example: http://127.0.0.1/CoreServices/DataAggregation.asmx	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
The url for the SSN 4.10 DataAggregation service	Headend_DataAggregation_410_Server_D7	URL for version 4.10 headend DataAggregation Endpoint. Example: https://ssn.ssns.gs.net:3000/amm/webservice/v2_1/DataAggregation-Port	
Headend DeviceManager Endpoint URI	Headend_DeviceManager_Server_D7	URL for headend DeviceManager Endpoint. Example: http://localhost:7001/soa-infra/services/SSN_Test/SSNTestHarness/DeviceManagerService	
The url for the SSN 4.7 DeviceManager service (DeviceManager.asmx)	Headend_DeviceManager_47_Server_D7	URL for version 4.7 headend DeviceManager Endpoint. Example: http://127.0.0.1/CoreServices/DeviceManager.asmx	
The url for the SSN 4.10 DeviceManager service	Headend_DeviceManager_410_Server_D7	URL for version 4.10 headend DeviceManager Endpoint Example: https://ssn.ssns.gs.net:3000/amm/webservice/v2_1/DeviceManagerPort	
Headend DeviceResults Endpoint URI	Headend_DeviceResults_Server_D7	URL for headend DeviceResults Endpoint. Example: http://localhost:7001/soa-infra/services/SSN_Test/SSNTestHarness/DeviceResultsService	
The url for the SSN 4.7 DeviceResults service (DeviceResults.asmx)	Headend_DeviceResults_47_Server_D7	URL for version 4.7 headend DeviceResults Endpoint. Example: http://127.0.0.1/CoreServices/DeviceResults.asmx	
The url for the SSN 4.10 DeviceResults service	Headend_DeviceResults_410_Server_D7	URL for version 4.10 headend DeviceResults Endpoint Example: https://ssn.ssns.gs.net:3000/amm/webservice/v2_1/DeviceResults	
Headend JobManager Endpoint URI	Headend_JobManager_Server_D7	URL for headend JobManager endpoint. Example: http://localhost:7001/soa-infra/services/SSN_Test/SSNTestHarness /JobManagerService	
The url for the SSN 4.7 JobManager service (JobManager.asmx)	Headend_JobManager_47_Server_D7	URL for version 4.7 headend JobManager endpoint. Example: http://127.0.0.1/CoreServices/JobManager.asmx	

Menu Option	Name Used in this Documentation	Usage	Customer Install Value
The url for the SSN 4.10 JobManager service	Headend_JobManager_410_Server_D7	URL for version 4.10 headend Job Manager End-Point Example: https://ssn.ssns.gs.net:3000/amm/webservice/v2_1/JobManagerPort	
The name of the OWSM policy to use when SOA calls a head end system	D7_SOA_HE_CLIENT_POLICY	The name of the OWSM policy to use when SOA calls a head end system	
The name of the OWSM policy to use when SOA is called by a head end system	D7_SOA_HE_SERVICE_POLICY	The name of the OWSM policy to use when SOA is called by a head end system	

SSN JMS Source Destination Bridge Configuration

20. SSN JMS Source Destination Bridge Configuration

```

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:
SSN Destination Bridge Password:

```

Parameter Description	Name Used in this Documentation	Usage	Customer Install Value
Source Bridge Destination Name	SRC_BRG_NAME_D7	Source bridge Destination name. Default Value: SSNTestHarness-BridgeDestination	
Classpath	SRC_BRG_CLASS-PATH_D7	Source bridge destination classpath. Default Value: empty	
Connection URL	SRC_BRG_CONN-URL_D7	Source bridge destination connection URL. Example: t3://JMS_PROVIDER_HOST:JMS_PORT_NUMBER	
Initial Context Factory	SRC_BRG_INITIAL_CONTEXT_D7	Source bridge destination initial context factory. Default: weblogic.jndi.WLInitialContextFactory	
Connection Factory JNDI Name	SRC_BRG_CONN_FACTORY_D7	SSN bridge connection factory JNDI Name. Default: jms/SSNTestHarnessConnectionFactory	
Destination Queue JNDI Name	SRC_BRG_QUEUE_JNDI_D7	SSN bridge destination queue JNDI name. Default: queue/SSNTestSSNODRQ	
JMS Provider User Name	SRC_BRD_WLS_USER_D7	Source destination bridge username.	
JMS Provider User Password	SRC_BRD_WLS_PASS_D7	Source destination bridge password.	

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
```

70. SSN SOA TestHarness Configurations

SSN TestHarness SOA Host Server:

SSN TestHarness SOA Port Number:

SSN SOA TestHarness Partition Name:

SSN SOA TestHarness Queue JNDI Name:

SSN_Test
queue/SSNTestSSNODRQ

Parameter Description	Name used in this Document	Usage	Customer Install Value
TestHarness SOA Host Server	SOA_HOST_TEST_D7	TestHarness SOA Host Server	
TestHarness SOA Port Server	SOA_PORT_NUMBER_TEST_D7	TestHarness SOA Port Server	
SOA TestHarness Partition Name	SOA_PARTITION_TEST_D7	TestHarness SOA partition name. Default Value: SSN_Test	
SOA TestHarness Queue JNDI Name	SOA_QUEUE_TEST_D7	TestHarness SOA Queue JNDI Name. Default Value: queue/SSNTestSSNODRQ	

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 these common tasks:

To Initialize the Environment

1. Go the directory <install_dir>/bin.
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. Run the following command:

UNIX:

```
./spl.sh start
```

Windows:

```
spl.cmd start
```

To Stop the WebLogic Server

1. Initialize the environment.
2. Run the following command:

UNIX:

```
./spl.sh stop
```

Windows:

```
spl.cmd stop
```

To Start the Thread Pool Worker

1. Initialize the environment.
2. Run the following command:

UNIX:

```
./spl.sh -b start
```

Windows:

```
spl.cmd -b start
```

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:

```
initialSetup.sh
```

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 initial setup script:

```
initialSetup.sh
```


Appendix D

Oracle Utilities Application Framework 4.3.0 Service Pack 3 (4.3.0.3.0) Fixes

The following table lists the Oracle Utilities Application Framework 4.3.0 Service Pack 3 (4.3.0.3.0) fixes included in this release.

Bug	Description