Oracle Utilities Customer Care and Billing

Installation Guide

Release 2.5.0 Service Pack 2

E61797-03

June 2016

ORACLE

Oracle Utilities Customer Care and Billing Installation Guide

E61797-03

Contents

Contents

Preface

This guide describes how to install Oracle Utilities Customer Care and Billing.

Audience

Oracle Utilities Customer Care and Billing Installation Guide is intended for system administrators installing Oracle Utilities Customer Care and Billing.

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

For more information, refer to these Oracle documents:

Installation Guides and Release Notes

- *Oracle Utilities Customer Care and Billing V2.5.0.2 Release Notes*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 Quick Install Guide*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 Database Administrator's Guide*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 Optional Products Installation Guide*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 License Information User Guide*

Administrative and Business User Guides

- *Oracle Utilities Customer Care and Billing V2.5.0.2 Administrative User Guide*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 Business User Guide*

Supplemental Documents

- *Oracle Utilities Customer Care and Billing V2.5.0.2 Server Administration Guide*
- *Oracle Utilities Customer Care and Billing V2.5.0.2 Security Guide*

Updates to this Documentation

This documentation is provided with the version of the product indicated. Additional and updated information about the operations and configuration of the product is available from the Knowledge Base section of My Oracle Support (http://support.oracle.com). Please refer to My Oracle Support for more information.

Conventions

The following text conventions are used in this document:

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

Chapter 1

Overview

This chapter provides an overview of the installation of Oracle Utilities Customer Care and Billing, including:

Installation Overview

Installing Oracle Utilities Customer Care and Billing involves the following steps:

1. Review the different tiers of the application architecture as described in Chapter 2: Application Architecture Overview.
2. Understand the hardware requirements for installing the application and the supported platforms for the application and database servers as described in Chapter 3: Supported Platforms and Hardware Requirements.

   Note: The installation and administration of the database server tier is described in detail in the document *Oracle Utilities Customer Care and Billing Database Administrator's Guide*.
3. Install the database as described in the document *Oracle Utilities Customer Care and Billing Database Administrator's Guide*.
4. Plan your installation as described in Chapter 4: Planning the Installation.
5. Install all required third-party software as described in Chapter 5: Installing Application Server Prerequisite Software. The required software is listed for each supported combination of operating system and application server.
6. If you are using the WebSphere application server on AIX, configure your server as described in Chapter 6: Configuring WebSphere Application Server.
7. Install the framework for the application as described in Chapter 7: Installing the Application Server Component of Oracle Utilities Application Framework.
8. Install Oracle Utilities Customer Care and Billing as described in Chapter 8: Installing the Application Server Component of Oracle Utilities Customer Care and Billing.
9. Follow the installation guidelines described in Chapter 10: Additional Tasks.

Chapter 2

Application Architecture Overview

This section provides an overview of the Oracle Utilities Application Framework application architecture.

Application Architecture

The Oracle Utilities Application Framework application is deployed on multiple tiers.

Please see the *Oracle Utilities Customer Care and Billing 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 Customer Care and Billing application. Note also that a desktop machine running Microsoft Windows and the Oracle client is required to perform some of the Oracle Utilities Customer Care and Billing product installation steps.

Tier 2: Web Application / Business Application Server, or Business Logic 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 Application Framework 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 Customer Care and Billing 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.

Chapter 3

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 supported on. It includes:

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 Customer Care and Billing be deployed?
- Which web server product will Oracle Utilities Customer Care and Billing deploy on?
- Which database product will Oracle Utilities Customer Care and Billing deploy on?
- Do you plan to deploy multiple Oracle Utilities Customer Care and Billing instances on the same physical server?
- How do you plan to deploy Oracle Utilities Customer Care and Billing?

  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 the Oracle Utilities Customer Care and Billing product, as described in the rest of this chapter.

Requirements by Tier

The application is deployed on multiple Tiers:

- Tier 1, Desktop
- Tier 2, Web/Business Application Server
- Tier 3, Database Server

Tier 1, Desktop: Software and Hardware Requirements

Configuration	Processor	Memory (RAM)	Monitor Display
Minimum	1 GHz or faster 64-bit (x64) processor	2 GB	1280x1024
Recommended*	3 GHz or faster 64-bit (x64) processor	4 GB	1280X1024

Web Browser Requirements

The following operating system / web browser software is supported:

- Windows 7, 8.1 (64-bit) with Internet Explorer 11, Firefox 45 ESR

Tier 2, Web/Business Application Server: Software and Hardware Requirements

Please consult the Supported Platforms to determine which web application servers can be used with the operating system that will be hosting this tier.

The recommendations that follow are based on a standard installation with both the web application and business application servers on the same machine and the system running with the default values. The default values may not support a production environment. You should adjust these values according to your production needs. Refer to the Server Administration Guide on how to change the default values. The minimum resource requirements exclude third-party software installation requirements. Refer to the third- party vendors for specific requirements. The following sizing excludes the Oracle database server installation.

Memory Requirements

For each application server deployment, 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
$SPLEBASE	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.
$SPLAPP	2 GB minimum	This location is used for storing batch log files and output from batch jobs. The size of this space should be influenced by which batches are run and how often, and the amount of debugging information that is collected.
Location of the application web work files on the web servers	1.5 GB minimum	This location is used by the 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.

Tier 3, Database Server: Software and Hardware Requirements

See the section Supported Platforms for supported database servers.

Supported Platforms

The installation has been tested to operate on many operating system, application server, and database server combinations. For the software requirements for each of these combinations, see Chapter 5: Installing Application Server Prerequisite Software for more information. This section includes the following topics:

- Operating Systems and Application Servers
- Oracle Database Servers
- Oracle WebLogic Server Information

Operating Systems and Application Servers

The following table details the operating system and application server combinations on which this version of Oracle Utilities Customer Care and Billing is supported.

Operating System and Web Browser (Client)	Operating System (Server)	Chipset	Application Server	Database
Windows 7, 8.1 (Internet Explorer 11, Firefox 45 ESR	AIX 7.2 TL0 (64-bit)	POWER 64-bit	WebLogic 12.1.3.0+* WebSphere (Basic)/ WebSphere (ND) 8.5.5	Oracle 12.1.0.1+
	Oracle Linux 6.5+/7.x (64-bit) or Red Hat Enterprise Linux** 6.5+/7.x (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 (64-bit)	x86_64	WebLogic 12.1.3.0+*	Oracle 12.1.0.1+
	HP-UX 11.31 (64-bit)	ia64	WebLogic 12.1.3.0+*	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.

** Oracle Utilities Customer Care and Billing is tested and supported on the versions of Oracle Linux specified. Because Oracle Linux is 100% userspace-compatible with Red Hat Enterprise Linux, Oracle Utilities Customer Care and Billing also is supported on Red Hat Enterprise Linux for this release.

- 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).

Oracle Database Servers

This release of Oracle Utilities Customer Care and Billing is supported with Oracle Database Server 12.1.0.1+ on all of the operating systems listed above.

The following Oracle Database Server Editions are supported:

- Oracle Database Enterprise Edition
- Oracle Database Standard Edition

> **Note:** Oracle Database Enterprise Edition and the Partitioning and Advanced Compression options are not mandatory but are recommended. Standard Edition should only be considered suitable for very small, pilot projects or development environments where scalability, performance, and database size-on-disk are not important considerations. Oracle Database Enterprise Edition, including the Advanced Compression and Partitioning options, is strongly recommended in all other situations.

The Oracle 12.1.0.1 client is required for this version of the database server.

Oracle WebLogic Server Information

The following Oracle WebLogic Server Editions are supported:

- Oracle WebLogic Server Standard Edition 12.1.3.0+
- Oracle WebLogic Server Enterprise Edition 12.1.3.0+ (required if using application clustering)

Support for Software Patches and Upgrades

Due to the ongoing nature of software improvement, vendors will issue patches and service packs for the operating systems, application servers and database servers on top of specific versions that Oracle Utilities Application Framework has been tested with.

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 Oracle Utilities Customer Care and Billing production environment.

The exception from this rule is Hibernate software version 4.1.0. This version should not be upgraded.

Always contact Oracle Utilities Customer Care and Billing support prior to applying vendor updates that do not guarantee backward compatibility.

Chapter 4

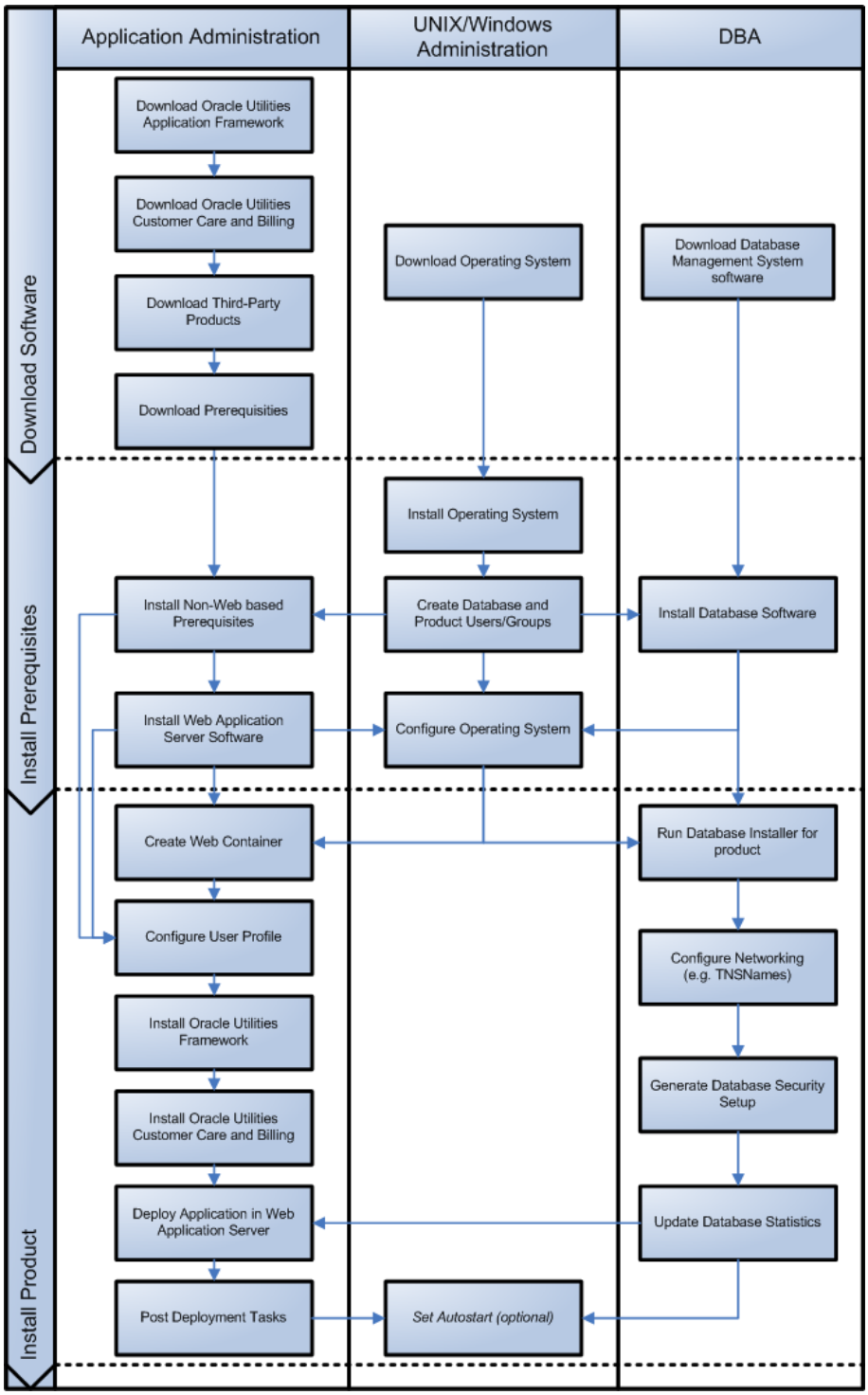
Planning the Installation

This chapter provides information for planning an Oracle Utilities Customer Care and Billing installation, including:

- Installation and Configuration Overview
- Before You Install
- Installation Checklist
- Installation and Configuration Worksheets

Installation and Configuration Overview

The following diagram provides an overview of the steps that need to be taken to install and configure Oracle Utilities Customer Care and Billing:



Before You Install

Refer to My Oracle Support for up-to-date additional information on installing Oracle Utilities Customer Care and Billing.

Embedded vs Native/Clustered Installation

By default, Oracle Utilities Application Framework uses Oracle WebLogic in embedded mode. This means the Oracle WebLogic installation is essentially pointed to the product installation and the executables of Oracle WebLogic are only used to execute the code. This has the advantage of being simple and quick to implement with the Oracle Utilities Application Framework generating a simple configuration for Oracle WebLogic to use.

If you want to take advantage of more advanced WebLogic features such as high performance (multiple managed servers) and high availability (clustering) configuration, do not use the embedded install. Rather, use the native/clustered installation which allows you to deploy the Oracle Utilities Application Framework J2EE components within Oracle WebLogic, as you would with other J2EE applications.

Application Server Clustering

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

- Implementing Oracle ExaLogic and/or Oracle WebLogic Clustering (Doc Id: 1334558.1)
- IBM WebSphere Clustering for Oracle Utilities Application Framework (Doc Id: 1359369.1)

Native Mode in WebLogic

If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "Native Installation Oracle Utilities Application Framework (Doc Id: 1544969.1)" on My Oracle Support.

Directory Names

Please note that directory names must not contain whitespace characters.

Installation Checklist

The following checklist will help guide you through the installation process of the application tier. The details for each step are presented in subsequent chapters.

1. Install the database as described in the *Oracle Utilities Customer Care and Billing Database Administrator's Guide.*
2. Create Group/User ID.
3. Install prerequisite software (for complete details about installing and configuring the prerequisite third-party software for your specific platform, see Chapter 5**:** Installing Application Server Prerequisite Software):
   - Oracle client 12.1.0.1.0
   - Java 7 Update 60 or Java 8 Update 51
   - Hibernate 4.1.0
4. Install web server.

- Oracle WebLogic 12.1.3.0+
- IBM WebSphere Basic 8.5.5 / IBM WebSphere Network Deployment 8.5.5

  Note: If you are upgrading and you are currently running Oracle Application Server please contact your Global Support Representative.

5. Verify that the software installed.
6. Set up environment variables.
7. Install Oracle Utilities Application Framework.
8. Install Oracle Utilities Application Framework prerequisite single fixes.
9. Install Oracle Utilities Customer Care and Billing.
10. Deploy Oracle Utilities Customer Care and Billing application.
11. Complete post-installation tasks.
12. Optional third-party product integration (such as web self service or reporting tools).

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 7: Installing the Application Server Component of Oracle Utilities Application Framework.

> **Note:** Some web application server information will not be available until the software installation steps have been completed as described in the Chapter 5: Installing Application Server Prerequisite Software.

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 password are entered in the command line but the inputted values are not reflected on the screen when performing the installation.

Application Framework Installation and Configuration Worksheets

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 server as part of the same environment. On a new installation, the default is a random 8 digit number.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
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 hibernate4 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 *Server Administration Guide* 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 WebSphere: /ouaf/IBM/WebSphere/AppServer WebSphere ND: /ouaf/IBM/WebSphereND/	
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 Options 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
```

The ons.jar should be copied to the Application Server. 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	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. 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) If this option is left empty, the install process creates a new keystore from scratch.	
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	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
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	Value used for keytool option -alias The following values are fixed: - HMAC Alias Key Algorithm: HmacSHA256 - HMAC Alias Key Size: 256 **Default value**: ouaf.system.hmac	
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>	The mount point into which the application is installed. For example: /ouaf for UNIX and C:\ouaf for Windows. 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. See <SPLENVIRON> below for more information on how this mount point is used.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Log File Mount Point	<SPLDIROUT>	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. 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). For each environment initialized, the application logs will be written to the directory <SPLDIROUT>/<SPLENVIRON> Note: Later in the installation the splenviron.sh (splenviron.cmd) script will set the $SPLOUTPUT (%SPLOUTPUT%) environment variable to point to:<SPLDIROUT>/<SPLENVIRON>	
Environment Name	<SPLENVIRON>	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. On installation a directory <SPLDIR>/<SPLENVIRON> is created, under which the Oracle Utilities Application Framework and <Product Name> software resides. When multiple environments are set up on the machine you will typically have directories such as: /ouaf/DEV01/.... /ouaf/CONV/.... Each of these contains a complete version of the Oracle Utilities Application Framework and <Product Name>. Note: Later in the installation process, the splenviron.sh (splenviron.cmd) script will set $SPLEBASE (%SPLEBASE%) environment variable to point to <SPLDIR>/<SPLENVIRON>	
Web Application Server Type	<SPLWAS>	A web application server for the environment to be used. The following value must be selected: **Valid values**: WLS: WebLogic WAS: WebSphere WASND: WebSphere ND Note: Not all web application servers are supported on all platforms; refer to Supported Platforms section for details.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Installation Application Viewer Module	<WEB_ ISAPPVIEWER>	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. **Valid values**: true: Application Viewer module will be installed. false: Application Viewer module will not be installed. **Default value**: true 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.	
Install Demo Generation Cert Script	CERT_INSTALL_ SCRIPT	You can install/uninstall later by executing the following script: perl [INSTALL_PACKAGE_FOLDER]/installAR.plx **Valid values**: true: Demo Generation Cert Script will be installed. false: Demo Generation Cert Script will not be installed. **Default value**: true	
Install Sample CM Source Code	CM_INSTALL_ SAMPLE	You can install/uninstall later by executing the following script: perl [INSTALL_PACKAGE_FOLDER]/installAR.plx **Valid values**: true: Sample CM Source Code will be installed. false: Sample CM Source Code will not be installed. **Default value**: true	

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	

WebSphere ND Business Application Server Configuration

The WebSphere Network Deployment parameters below and in the worksheet are for a WebSphere ND installation.

```
2. Business Application Server Configuration
       Business Server Host:                          <machine_name>
       Bootstrap Port:
       WebSphere Server Name:
       WebSphere Node Name:
       Business Server Application Name:               SPLService
       MPL Admin Port Number:
       MPL Automatic startup:
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Business Server Host	BSN_WLHOST	The host name on which business application server resides. **Default value**: <current server name>	
Bootstrap Port	BSN_WASBOOTSTRAP PORT	The boot strap port number allows the web module to communicate with the EJB module.	
WebSphere Server Name	BSN_SVRNAME	The WebSphere ND Application Server to host the OUAF application. Each OUAF must be installed in a unique WebSphere ND Application Server. **Default value**: server2	
WebSphere Node Name	BSN_NODENAME	The name of the WebSphere ND Node Name where the WebSphere ND Application Server is running.	
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	

WebSphere Basic Business Application Server Configuration

The WebSphere parameters below and in the worksheet are for a WebSphere installation.

```
2. Business Application Server Configuration
      Business Server Host:                                <machine_name>
       Bootstrap Port:
       WebSphere Server Name:
       WebSphere Node Name:
       Business Server Application Name:                     SPLService
       MPL Admin Port Number:
       MPL Automatic startup:
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Business Server Host	BSN_WLHOST	The host name on which business application server resides. **Default value**: <current server name>	
Bootstrap Port	BSN_WASBOOTSTRAPPORT	The boot strap port number allows the web module to communicate with the EJB module.	
WebSphere Server Name	BSN_SVRNAME	The WebSphere Application Server to host the OUAF application. Each OUAF must be installed in a unique WebSphere Application Server. **Default value**: server2	
WebSphere Node Name	BSN_NODENAME	The name of the WebSphere Node Name where the WebSphere Application Server is running. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.	
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	The password the application uses to connect to the EJB component through JNDI. Note: The required value for an initial installation is "jndiadmin". This value will be saved in encrypted format. This is a security value; it will be encrypted with the Oracle Application Framework Encryption Algorithm.	
WebLogic Admin System User ID	WLS_WEB_ WLSYSUSER	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 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". This is a security value; it will be encrypted with the Weblogic Encryption Algorithm.	
WebLogic Admin System Password	WLS_WEB_ WLSYSPASS	The password to login to Oracle WebLogic console and to administer Oracle WebLogic. The Oracle WebLogic startup and stop script also utilize this password. 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". This is a security value; it will be encrypted with the Weblogic Encryption Algorithm.	
WebLogic Server Name	WEB_WLS_ SVRNAME	The name of the WebLogic server where the web application resides. **Default value**: myserver Note: For an initial installation, use the default value of "myserver".	
Web Server Application Name	WEB_APP	The name of the web application server. **Default value**: SPLWeb Note: For an initial installation, use the default value of "SPLWeb".	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Deploy Using Archive Files	WEB_DEPLOY_EAR	When the value is "false" the web application will be deployed in exploded directory format (no WAR/EAR files). When the value is "true", the web application will be deployed in ear file format. Note: The expanded application folders will always exist under the application folder (<SPLEBASE>/splapp/applications), regardless of the setting of this option. **Valid values**: true (Deploy EAR files) false (Deploy expanded application folders **Default value**: true	
Deploy Application Viewer Module	WEB_DEPLOY_APPVIEWER	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. Note: With either value the application viewer module will still be managed by the upgrade process. 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. **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 **Default value**: true	
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	The application super users. Enter the super users separating them by commas.	

WebSphere ND Web Application Server Configuration

The WebSphere ND parameters below and in the worksheet are for a WebSphere ND installation.

```
3. Web Application Server Configuration
      Web Server Host:                                        <machine_name>
       WebSphere SSL Port Number:
       Web Context Root:
       WebSphere Server Name:
       WebSphere Node Name:
       Web Server Application Name:
       WebSphere JNDI System User ID:
       WebSphere JNDI System Password:
       Deploy Using Archive Files:
       Deploy Application Viewer Module:
       Enable The Unsecured Health Check Service:   false
       MDB RunAs User Ids:
       Super User Ids
```

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**: <machine_name>	
WebSphere SSL Port Number	WEB_WASSLPORT	The WC_defaulthost_secure number for your WebSphere ND server. This is the port number that is used as a part of the client URL request to connect to the host. Example value: 9081	
Web Context Root	WEB_CONTEXT_ ROOT	A context root name that allows customers to run multiple instances of web application on the same installation of WebSphere ND server. **Default value**: ouaf	
WebSphere Server Name	WEB_SVRNAME	The WebSphere Application Server to host the <Product Acronym> application. Each <Product Acronym> must be installed in a unique WebSphere Application Server. **Default value**: server2	
WebSphere Node Name	WEB_NODENAME	The name of the WebSphere Node Name where the WebSphere Application Server is running.	
Web Server Application Name	WEB_APP	The name of the web application server. **Default value**: SPLWeb	Web Server Application Name
WebSphere JNDI User ID:	WEB_WASUSER	User ID the application utilizes to connect to the EJB component through JNDI. This is the EJB container user ID. Note: This value must be a valid User in the WebSphere ND console.	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
WebSphere JNDI System Password:	WEB_WASPASS	The password the application utilizes to connect to the EJB component through JNDI. Note: This value will be saved in encrypted format.	
Deploy Using Archive Files	WEB_DEPLOY_EAR	When the value is "false" the web application will be deployed in exploded directory format (no WAR/EAR files). When the value is "true", the web application will be deployed in ear file format. Note: the expanded application folders will always exist as main depot under the application folder (<SPLEBASE>/splapp/applications), regardless of the setting of this option. **Valid values**: true: Environment expanded (no WAR files) false: Environment with WAR/EAR files **Default value**: true	
Deploy Application Viewer Module	WEB_DEPLOY_APPVIEWER	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. Note: With either value the application viewer module will still be managed by the upgrade process. **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) **Default value**: true	
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	The application super users. Enter the super users separating them by commas.	

WebSphere Basic Web Application Server Configuration

The WebSphere parameters below and in the worksheet are for a WebSphere installation.

```
3. Web Application Server Configuration
       Web Server Host:                                    <machine_name>
       Web Server SSL Port Number:
       Web Context Root:
       WebSphere Server Name:
       WebSphere Node Name:
       Web Server Application Name:
       WebSphere JNDI System User ID:
       WebSphere JNDI System Password:
       Deploy Using Archive Files:
       Deploy Application Viewer Module:
       Enable The Unsecured Health Check Service:   false
       MDB RunAs User Ids:
       Super User Ids
```

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**: <machine_name>	
Web Server SSL Port Number	WEB_WLPORT	The WC_defaulthost_secure number for your WebSphere Basic server. This is the port number that is used as a part of the client URL request to connect to the host. Example value: 9081	
Web Context Root	WEB_CONTEXT_ ROOT	A context root name that allows customers to run multiple instances of web application on the same installation of WebSphere server. **Default value**: ouaf	
WebSphere Server Name	WEB_SVRNAME	The WebSphere Basic Application Server to host the <Product Acronym> application. Each <Product Acronym> must be installed in a unique WebSphere Basic application server. **Default value**: server2	
WebSphere Node Name	WEB_NODENAME	The name of the WebSphere Basic Node Name where the WebSphere Basic application server is running. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.	
Web Server Application Name	WEB_APP	The name of the web application server. **Default value**: SPLWeb	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
WebSphere JNDI User ID:	WEB_WASUSER	User ID the application utilizes to connect to the EJB component through JNDI. This is the EJB container user ID. Note: This value must be a valid User in the WebSphere console. This is a security value.	
WebSphere JNDI System Password:	WEB_WASPASS	The password the application utilizes to connect to the EJB component through JNDI. Note: This is a security value. it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm.	
Deploy Using Archive Files	WEB_DEPLOY_EAR	When the value is "false" the web application will be deployed in exploded directory format (no WAR/EAR files). When the value is "true", the web application will be deployed in ear file format. Note: The expanded application folders will always exist as main depot under the application folder (<SPLEBASE>/ splapp/applications), regardless of the setting of this option. **Valid values**: true: Environment expanded (no WAR files) false: Environment with WAR/EAR files **Default value**: true	
Deploy Application Viewer Module	WEB_DEPLOY_ APPVIEWER	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. Note: With either value the application viewer module will still be managed by the upgrade process. **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) **Default value**: true	
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	The application super users. Enter the super users separating them by commas.	

Database Configuration

Note: If any of the database menu option items below are changed, the system displays the following warning next to the actual option that has been changed:

```
      This database option have been changed. Since the keystore and
encrypted data in the database must be compatible, you have two
options:
      - load the compatible keystore into the environment;
      - keep the current keystore, re-enter any encrypted information
online through the application, and re-generate the database hashes.
 Refer to the security guide for more information.


4. Database Configuration
       Application Database User ID:
       Application 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:
      Oracle Client Character Set NLS_LANG:  AMERICAN_AMERICA.AL32UTF8
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Application 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 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.	

Menu Option	Name Used in Documentation	Usage	Customer Install 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.	
XAI Database Password	XAI_DBPASS	The database password that has been configured on the database for the XAI 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.	
Batch Database User ID	BATCH_DBUSER	The database user ID that has been configured on the database for the batch connection. This is a security value.	
Batch Database Password	BATCH_DBPASS	The database password that has been configured on the database for the batch 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.	
Web JDBC DataSource Name	JDBC_NAME	Populate in order to activate JDBC datasource for online when on weblogic. Leave empty to use UCP connection pooling.	
JDBC Database User ID	DBUSER_WLS	The database user ID that has been configured for the JDBC connection. Set this to the proper value if the Web JDBC DataSource Name is entered.	
JDBC Database Password	DBPASS_WLS	The database user password that has been configured for the JDBC connection. Set this to the proper value if the Web JDBC DataSource Name is entered. This is a security value; it will be encrypted with the WebLogic Encryption Algorithm.	
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.	
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:                                dev
```

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.	
RMI Port number for JMX Web	WEB_JMX_RMI_PORT_PE RFORMANCE	Example value: 6570 Note: This is an optional value.	

Menu Option	Name Used in Documentation	Usage	Customer Install 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	If you choose DEMO you need to execute the following script at least once perl [SPLEBASE]/bin/demo_gen_cert.plx 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. **Default value**: CUSTOM **Valid values**: DEFAULT,DEMO,CUSTOM 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.	
Identify Keystore Type	CERT_IDENT_KS_ FILE	Mandatory if the type is CUSTOM. No need to populate if type is DEMO, it will use: [SPLEBASE]/splapp/certs/ouaf_demo_ident.jks	
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	Mandatory if the type is CUSTOM. No need to populate if type is DEMO, it will use: [SPLEBASE]/splapp/certs/ouaf_demo_trust.jks	
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	

OUAF TrustStore Options

Note: See the *Server Administration Guide* for additional details on this configuration.

The OUAF truststore configuration is required for IWS.

```
7. OUAF 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
       Weblogic Cluster Name:
       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:
       Cloud Restriction URLs Enable:
       Cloud White List Full Path:
       Cloud Custom White List Full Path:
```

Menu Option	Name Used in Documentation	Usage	Customer Value Install
Online JVM Batch Server Enabled	BATCHENABLED	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. **Default value**: false Note: This functionality should only be used in low volume environments.	
Online JVM Batch Number of Threads	BATCHTHREADS	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). **Default value**: 5 Note: This will be only used and activated when BATCHENABLED is set to true.	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
Online JVM Batch Scheduler Daemon Enabled	BATCHDAEMON	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. **Valid values**: true, false **Default value**: false Note: This will be only used and activated when BATCHENABLED is set to true.	
Enable Batch Edit Funtionality	BATCHEDIT_ ENABLED	Enable Batch Edit Functionality If enabled, use the bedit.sh|cmd script in order to configure the batch **Valid values**: true, false **Default value**: false	
Batch Online Log Directory	BATCH_ONLINE_LOG _DIR	This is required for the online batch retrieval feature.	
Enable Web Services Functionality	WEBSERVICES_ ENABLED	If enabled, execute the following commands in oder to allow the application to re-deploy the Webservices without prompting for the user and password: - Add weblogic.jar to the CLASSPATH - Execute: java weblogic.Admin -username [USER NAME] -password [PASSWORD] STOREUSERCONFIG -userconfigfile [SPLEBASE]/etc/.wlsuserconfig -userkeyfile [SPLEBASE]/etc/.wlsuserkey **Valid values**: true, false **Default value**: false	
GIS Service Running on the same Web Server	GIS	Geographical information (GEOCODING) - GIS Service running on the same web application server **Valid values**: true, false This value is optional. This value will only appear for WebLogic.	
GIS Service URL	GIS_URL	This is the URL of the external web server. Note: This value will be only be used when GIS is set to true. This value is optional. This value will only appear for WebLogic.	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
GIS WebLogic System User ID	GIS_WLSYSUSER	GIS WebLogic System User ID Note: This value will be only be used when GIS is set to true. This value is optional. This value will only appear for WebLogic.	
GIS WebLogic System Password	GIS_WLSYSPASS	GIS WebLogic System Password. Note: This value will be only be used when GIS is set to true. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm. This value will only appear for WebLogic.	
Online Display Software Home	ONLINE_DISPLAY_HOME	The location of the Online Display Software installation directory. This value is optional.	
Max Queries To Hold In Cache Across All Threads	XQUERIES_TO_CACHE	Max number of queries to hold in the cache across all threads 0 = no cache -1 or [empty] = unlimited	
Seconds Timeout Flush Cache Completely	XQUERY_CACHE_FLUSH_TIMEOUT	Number of seconds before cache is flushed Completely 0 or [empty] = never auto-flush	
Cloud Restriction URLs Enable	CLOUD_RESTRICTION_URLS_ENABLE	Enables restriction of urls that the application can communicate with based on a whitelist file. Default is false.	
Cloud White List Full Path	CLOUD_WHITE_LIST_PATH	Fully qualified filename to whitelist.xml	
Cloud Custom White List Full Path	CLOUD_CUSTOM_WHITE_LIST_PATH	Fully qualified filename to cuistom cm_whitelist.xml	

WebSphere ND Advanced Environment Miscellaneous Configuration

```
50. Advanced Environment Miscellaneous Configuration
       WebSphere Web Server SOAP Port Number:
       WebSphere Business Server SOAP Port Number:
       WebSphere Profile Name Home Directory:
       WebSphere Deployment Manager Host Name:
       Online JVM Batch Server Enabled:               false
       Online JVM Batch Number of Threads:                5
       Online JVM Batch Scheduler Daemon Enabled:    false
       Enable Batch Edit Functionality:            false
       Batch Online Log Directory:
       Enable Web Services Functionality:         false
       Weblogic Cluster Name:
       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:
       Cloud Restriction URLs Enable:
       Cloud White List Full Path:
       Cloud Custom White List Full Path:
```

Menu Option	Name Used in Documentation	Usage	Customer Value Install
WebSphere Web Server SOAP Port Number	WAS_WEB_SOAP_PORT	WebSphere Web Server SOAP Port Number This is the SOAP port used for WebSphere when executing wsadmin.sh commands. **Note**: This value will only appear for WebSphere Basic and WebSphere ND	
WebSphere Business Server SOAP Port Number	WAS_BSN_SOAP_PORT	WebSphere Business Server SOAP Port Number. This is the SOAP port used for WebSphere when executing wsadmin.sh commands. **Note**: This value will only appear for WebSphere Basic and WebSphere ND	
Enter the location of the Application Server Profile Home	WAS_PROFILE_NAME_HOME	The profile home will be used when tracking log files, under websphere home. **Note**: This value will only appear for WebSphere Basic and WebSphere ND	
WebSphere Deployment Manager Host Name	WASND_DMGR_HOST	WebSphere Deployment Manager Host name, this value is used for WebSphere ND, when connecting to the WebSphere Deployment Manager. **Note**: This value will only appear for WebSphere ND.	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
Online JVM Batch Server Enabled	BATCHENABLED	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. **Default value**: false Note: This functionality should only be used in low volume environments.	
Online JVM Batch Number of Threads	BATCHTHREADS	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). **Default value**: 5 Note: This will be only used and activated when BATCHENABLED is set to true.	
Online JVM Batch Scheduler Daemon Enabled	BATCHDAEMON	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. **Valid values**: true, false **Default value**: false Note: This will be only used and activated when BATCHENABLED is set to true.	
Enable Batch Edit Funtionality	BATCHEDIT_ ENABLED	Enable Batch Edit Functionality If enabled, use the bedit.sh|cmd script in order to configure the batch **Valid values**: true, false **Default value**: false	
Batch Online Log Directory	BATCH_ONLINE_LOG _DIR	This is required for the online batch retrieval feature.	
Enable Web Services Functionality	WEBSERVICES_ ENABLED	If enabled, execute the following commands in oder to allow the application to re-deploy the Webservices without prompting for the user and password: - Add weblogic.jar to the CLASSPATH - Execute: java weblogic.Admin -username [USER NAME] -password [PASSWORD] STOREUSERCONFIG -userconfigfile [SPLEBASE]/etc/.wlsuserconfig -userkeyfile [SPLEBASE]/etc/.wlsuserkey **Valid values**: true, false **Default value**: false	

Menu Option	Name Used in Documentation	Usage	Customer Value Install
GIS Service Running on the same Web Server	GIS	Geographical information (GEOCODING) - GIS Service running on the same web application server **Valid values**: true, false This value is optional. This value will only appear for WebLogic.	
GIS Service URL	GIS_URL	This is the URL of the external web server. Note: This value will be only be used when GIS is set to true. This value is optional. This value will only appear for WebLogic.	
GIS WebLogic System User ID	GIS_WLSYSUSER	GIS WebLogic System User ID Note: This value will be only be used when GIS is set to true. This value is optional. This value will only appear for WebLogic.	
GIS WebLogic System Password	GIS_WLSYSPASS	GIS WebLogic System Password. Note: This value will be only be used when GIS is set to true. This is a security value; it will be encrypted with the Oracle Utilities Application Framework Encryption Algorithm. This value will only appear for WebLogic.	
Online Display Software Home	ONLINE_DISPLAY_HOME	The location of the Online Display Software installation directory. This value is optional.	
Max Queries To Hold In Cache Across All Threads	XQUERIES_TO_CACHE	Max number of queries to hold in the cache across all threads 0 = no cache -1 or [empty] = unlimited	
Seconds Timeout Flush Cache Completely	XQUERY_CACHE_FLUSH_TIMEOUT	Number of seconds before cache is flushed Completely 0 or [empty] = never auto-flush	
Cloud Restriction URLs Enable	CLOUD_RESTRICTION_URLS_ENABLE	Enables restriction of urls that the application can communicate with based on a whitelist file. Default is false.	
Cloud White List Full Path	CLOUD_WHITE_LIST_PATH	Fully qualified filename to whitelist.xml	
Cloud Custom White List Full Path	CLOUD_CUSTOM_WHITE_LIST_PATH	Fully qualified filename to cuistom cm_whitelist.xml	

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_O PT	Additional options that will be passed in to the web application server JVM. This is optional.	
Global JVM Arguments	GLOBAL_JVMARGS	JVM arguments that are passed to all Java server processes such as Weblogic Server, Threadpoolworkers and jobs. Arguments added to all jvms Defaults to -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=<TEMPDIR>	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Ant Min Heap Size	ANT_OPT_MIN	Minimum Heap Size passed to ANT JVM. **Default value**: 200	
Ant Max Heap Size	ANT_OPT_MAX	Maximum Heap Size passed to ANT JVM. **Default value**: 800	
Ant Additional Options	ANT_ADDITIONAL_OPT	Additional options that are passed into the ANT JVM.	
Thread Pool Worker Java Min Heap Size	BATCH_MEMORY_OPT_MIN	Minimum heap size passed to the Thread Pool Worker. **Default value**: 512	
Thread Pool Worker Java Max Heap Size	BATCH_MEMORY_OPT_MAX	Maximum heap size passed to the Thread Pool Worker. **Default value**: 1024	
Thread Pool Worker Java Max Perm Size	BATCH_MEMORY_OPT_MAXPERMSIZE	Maximum perm size passed to the Thread Pool Worker **Default value**: 768	
Thread Pool Worker Additional Options	BATCH_MEMORY_ADDITIONAL_OPT	Additional Memory Options passed into the Thread Pool Worker. For non-AIX only.	
Additional Runtime Classpath	ADDITIONAL_RUNTIME_CLASSPATH	Additional Classpath Options passed in when starting the WebLogic JVM Note: For WebLogic installation only. This is an optional value.	

WebSphere ND Advanced Environment Memory Configuration

```
51. Advanced Environment Memory Configuration
       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:
```

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Web Application Additional Options	WEB_ADDITIONAL_OPT	Additional options that will be passed in to the web application server JVM. This is optional.	
Global JVM Arguments	GLOBAL_JVMARGS	JVM arguments that are passed to all Java server processes such as Weblogic Server, Threadpoolworkers and jobs. Arguments added to all jvms Defaults to -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=<TEMPDIR>	
Ant Min Heap Size	ANT_OPT_MIN	Minimum Heap Size passed to ANT JVM. **Default value**: 200	
Ant Max Heap Size	ANT_OPT_MAX	Maximum Heap Size passed to ANT JVM. **Default value**: 800	
Ant Additional Options	ANT_ADDITIONAL_OPT	Additional options that are passed into the ANT JVM.	
Thread Pool Worker Java Min Heap Size	BATCH_MEMORY_OPT_MIN	Minimum heap size passed to the Thread Pool Worker. **Default value**: 512	
Thread Pool Worker Java Max Heap Size	BATCH_MEMORY_OPT_MAX	Maximum heap size passed to the Thread Pool Worker. **Default value**: 1024	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
Thread Pool Worker Additional Options	BATCH_MEMORY_ ADDITIONAL_OPT	Additional Memory Options passed into the Thread Pool Worker. For non-AIX only.	
Additional Runtime Classpath	ADDITIONAL_ RUNTIME_ CLASSPATH	Additional Classpath Options passed in when starting the WebLogic JVM Note: For WebLogic installation only. This is an optional value.	

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_L2_CACHE_ MODE	**Default value**: off **Valid values**: off read_write read_only	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
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.	
Domain Home Location	WLS_DOMAIN_ HOME	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). Note: For WebLogic installation only This value is optional	
Batch Cluster URL	WEB_BATCH_ CLUSTER_URL	Example: service:jmx:rmi:///jndi/rmi://[host]:[TPW JMX port]/oracle/ouaf/batchConnector	
StripHTMLComments: false	STRIP_HTML_ COMMENTS	Stripping HTML (and JavaScript) comments will increase the security of the system. **Default value**: false **Valid values**: true, false	
Authentication Login Page Type	WEB_WLAUTHMETHOD	Specifies which authentication mode should be used. To switch off OUAF Login Page enter: BASIC **Valid values**: FORM, BASIC **Default value**: FORM	
Web Form Login Page	WEB_FORM_ LOGIN_PAGE	Specify the jsp file used to login into the application. **Default value**: /loginPage.jsp	
Web Form Login Error Page	WEB_FORM_LOGIN _ERROR_PAGE	Specify the jsp file used when there is an error when logging into the application. **Default value**: /formLoginError.jsp	
Application Viewer Form Login Page	WEB_APPVIEWER_ FORM_LOGIN_ PAGE	Specify the jsp file used to login into the application viewer application. **Default value**: /loginPage.jsp	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
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 viwer application.	
Help Form Login Page	WEB_HELP_FORM_ LOGIN_PAGE	Specify the jsp file used to login into the help application. **Default value**: /loginPage.jsp	
Help Form Login Error Page	WEB_HELP_FORM_ LOGIN_ERROR_ PAGE	Specify the jsp file used when there is an error when logging into the help application. **Default value**: /formLoginError.jsp	
Web Security Role	WEB_PRINCIPAL_ NAME	Specify the name of the security role. **Default value**: cisusers	
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	

Menu Option	Name Used in Documentation	Usage	Customer Install Value
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:                           sOAPElement
```

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 Defautlt 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	
SPML OIM Enclosing Element	OIM_SPML_SOAP_ ELEMENT	Default top level SOAP Element name for Oracle Identity Manager integration **Default value**: sOAPElement	

Chapter 5

Installing Application Server 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 7.2 TL0 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 7.2 (64-bit) TL0	POWER 64-bit	Oracle WebLogic (12.1.3.0+) 64-bit version/ WebSphere 8.5.5 64-bit version

Web/Application Server Tier

AIX 7.2 TL0 Operating System Running on Power5 and Power6 Architecture

UNIX Administrator Userid

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

Description	Default Value	Customer Defined Value
CCB Administrator UserID	cissys	
CCB 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 userid 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 exists 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 077 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 and 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

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.

You must use the same user for starting and stopping a process. For example, if cissys is used to start the application server, the use cissys to stop it as well.

Oracle 12.1.0.1.0 Client

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 7.0 or 7.1 (64-bit)

Installation of Java as a prerequisite is only needed if you are using Oracle WebLogic as a Web application server. If you use WebSphere, the Java runtime engine from the Web application server is used.

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 userid (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

You must install Hibernate 4.1.0 before installing Oracle Utilities Customer Care and Billing.

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:

```
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
  jboss-transaction-api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
```

Oracle WebLogic Server 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 12.1.3.0+ .

> **Note**: If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "*Native Installation Oracle Utilities Application Framework*" (Doc Id: 1544969.1) on My Oracle Support.

IBM WebSphere Application Server 8.5.5.x 64-bit

WebSphere must be purchased and downloaded from IBM. It must be installed and configured prior to the Oracle Utilities Customer Care and Billing installation. This Web application server will run as a 64-bit application.

IBM WebSphere Application Server 8.5 supports SDK 1.6 as the basic configuration but with SDK 1.7 or 1.7.1_64 as an optional configuration. For Oracle Utilities Customer Care and Billing, the implementation requires SDK 1.7 or 1.7.1_64 as the default run-time configuration for WebSphere Application Server 8.5. Therefore, after WebSphere Application Server is installed with the basic configuration, you MUST change the default SDK to 1.7 or 1.7.1_64.

A single WebSphere server represents a single Oracle Utilities Customer Care and Billing environment. You can install multiple environments on a single WebSphere Installation by creating additional WebSphere servers. Refer to Chapter 5: Configuring WebSphere Application Server for the configuration steps.

IBM WebSphereND Application Server 8.5.5.x 64-bit

WebSphere must be purchased and downloaded from IBM. It must be installed and configured prior to the Oracle Utilities Customer Care and Billing installation. This Web application server will run as a 64-bit application.

IBM WebSphere Application Server 8.5 supports SDK 1.6 as the basic configuration but with SDK 1.7 or 1.7.1_64 as an optional configuration. For Oracle Utilities Customer Care and Billing, the implementation requires SDK 1.7 or 1.7.1_64 as the default run-time configuration for WebSphere Application Server 8.5. Therefore, after WebSphere Application Server is installed with the basic configuration, you MUST change the default SDK to 1.7 or 1.7.1_64.

A single WebSphere server represents a single Oracle Utilities Customer Care and Billing environment. You can install multiple environments on a single WebSphere Installation by creating additional WebSphere servers. Refer to Chapter 5: Configuring WebSphere Application Server for the configuration steps.

Oracle Linux 6.5+/7.x and Red Hat Linux 6.5+/7.x Application Server

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) Red Hat Enterprise Linux 6.5+/7.x (64-bit))	x86_64	Oracle WebLogic 12.1.3.0+ (64-bit) version

Web/Application Server Tier

Oracle Enterprise Linux 6.5+/7.x or Red Hat Enterprise Linux 6.5+/7.x Operating System Running on x86_64 64-bit Architecture

UNIX Administrator Userid

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

Description	Default Value	Customer Defined Value
CCB Administrator UserID	cissys	
CCB 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 userid 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 exists 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 077 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 and 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

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.

You must use the same user for starting and stopping a process. For example, if cissys is used to start the application server, the use cissys to stop it as well.

Oracle 12.1.0.1.0 Client

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 7.0 Update 60 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.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.

Oracle Java Development Kit Version 8.0 Update 51 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.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

You must install Hibernate 4.1.0 before installing Oracle Utilities Customer Care and Billing.

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:

   ```
   cp hibernate-release-4.1.0.Final/lib/optional/
      ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/optional/
      ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/required/
      hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/required/
      hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/required/
      hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/required/
      javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
   cp hibernate-release-4.1.0.Final/lib/required/
      jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
  jboss-transaction-api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
   ```

Oracle WebLogic Server 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 12.1.3.0+

  Note: If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "*Native Installation Oracle Utilities Application Framework*" (Doc Id: 1544969.1) on My Oracle Support.

Solaris 11 Application Server

This section describes the software requirements for operating the application using the Sun Solaris 11 application server.

Supported Application Servers

Operating System	Chipsets	Application Server
Solaris 11 (64-bit)	SPARC	Oracle WebLogic 12.1.3.0+ (64-bit) version

Web/Application Server Tier

Solaris 11 Operating System Running on SPARC-based 64-bit Architecture

UNIX Administrator Userid

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

Description	Default Value	Customer Defined Value
CCB Administrator UserID	cissys	
CCB 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 userid 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 exists 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 077 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 and 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

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.

You must use the same user for starting and stopping a process. For example, if cissys is used to start the application server, the use cissys to stop it as well.

Oracle 12.1.0.1.0 Client

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 7.0 Update 60 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.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.

Oracle Java Development Kit Version 8.0 Update 51 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.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

You must install Hibernate 4.1.0 before installing Oracle Utilities Customer Care and Billing.

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:

```
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
  jboss-transaction-api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
```

Oracle WebLogic Server 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 12.1.3.0+

  Note: If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "*Native Installation Oracle Utilities Application Framework*" (Doc Id: 1544969.1) on My Oracle Support.

Windows 2012 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
Window Server 2012	x86_64	Oracle WebLogic 12.1.3.0+ (64-bit) version

Web/Application Server Tier

Oracle Client 12.1.0.1.0

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 7.0 Update 60 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.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.

Oracle Java Development Kit Version 8.0 Update 51 or Later, 64-Bit

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

http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.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

You must install Hibernate 4.1.0 before installing Oracle Utilities Customer Care and Billing.

To install Hibernate:

1. Create a Hibernate jar external depot:

   ```
   SET 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:

```
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
  jboss-transaction-api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
```

Oracle WebLogic Server 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 12.1.3.0+

Note: If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "*Native Installation Oracle Utilities Application Framework*" (Doc Id: 1544969.1) on My Oracle Support.

HP-UX 11.31 Application Server

This section describes the software requirements for operating the application using the HP-UX application server.

Supported Application Servers

Operating System	Chipsets	Application Server
HP-UX ia (64-bit)	ia64	Oracle WebLogic 12.1.3.0+ (64-bit) version

Web/Application Server Tier

HP-UX Operating System Running on Itanium 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
CCB Administrator UserID	cissys	
CCB 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 userid 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 exists 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 077 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 and 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

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.

You must use the same user for starting and stopping a process. For example, if cissys is used to start the application server, the use cissys to stop it as well.

Oracle 12.1.0.1.0 Client

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.

HP-Ux Java Development Kit Version 7.0 Update 12 or Later (64-Bit)

This software is only required for Oracle WebLogic installations. At the time of release, the Java packages used in the test cycle were downloaded from the HP website.

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

You must install Hibernate 4.1.0 before installing Oracle Utilities Customer Care and Billing.

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:

```
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/ehcache-core-2.4.3.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/optional/
   ehcache/hibernate-ehcache-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-commons-annotations-4.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-core-4.1.0.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   hibernate-jpa-2.0-api-1.0.1.Final.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   javassist-3.15.0-GA.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
   jboss-logging-3.1.0.CR2.jar $HIBERNATE_JAR_DIR
cp hibernate-release-4.1.0.Final/lib/required/
  jboss-transaction-api_1.1_spec-1.0.0.Final.jar $HIBERNATE_JAR_DIR
```

Oracle WebLogic Server 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 12.1.3.0+

Note: If you plan on using the Oracle Utilities Application Framework in native mode within Oracle WebLogic (as opposed to embedded mode), refer to the whitepaper "*Native Installation Oracle Utilities Application Framework*" (Doc Id: 1544969.1) on My Oracle Support.

Chapter 6

Configuring WebSphere Application Server

This section describes tasks that you should complete before you install the Oracle Utilities Application Framework. It also describes configuration tasks you should complete after installing Oracle Utilities Customer Care and Billing. It includes the following:

- Configuring WebSphere Basic
- Configuring WebSphere Network Deployment

Configuring WebSphere Basic

Pre-Installation Tasks

This section describes tasks that you should complete to configure a WebSphere Basic application server before you install the Oracle Utilities Application Framework.

> **Note:** When working within the WebSphere console make sure to apply and save your changes to the Master Configuration when appropriate.

Setting of WebSphere Security

There are several security configuration options within WebSphere. In a production environment you must use the security implementation appropriate for your security requirements. During the Release cycle we used the User account repository of the Federated repository. The following procedures describe how to apply these security settings.

> **Note:** Refer to the WebSphere Application Server documentation for more details.

1. Start the WebSphere Administrative Console and log in.
2. Go to **Security, Global security.**
   - Check **Enable administrative security.**
   - Check **Enable application security.**
   - Select **Federated repositories** from the Available realm definitions
3. Click **Apply.**

Setting WebSphere Application Groups

1. Start the WebSphere Administrative Console and log in.
2. Go to **Users and Groups - Manage Groups**.

   Create the group name of cisusers (default group).
3. Click **Create.**

Setting WebSphere Application Users

1. Start the WebSphere Administrative Console and log in.
2. Go to **Users and Groups - Manage Users.**
   - Create the user Id of SYSUSER (example user)
   - Add the Group Membership of cisusers (created in the previous step) to the user.
3. Click **Create.**

Setting WebSphere JNDI Users

1. Start the WebSphere Administrative Console and log in.
2. Go to **Users and Groups, Manage Users**.
   - Create the user id of JNDI (example user).
   - Add the Group Membership of cisusers (created in the previous step) to the JNDI user, created in this step.
3. Click **Create.**

Setting WebSphere JNDI Users - CORBA Naming Service Users

1. Start the WebSphere Administrative Console and log in.

2. Go to **Environment, Naming, CORBA Naming Service Users**.

- Add the user id of JNDI (example user).
- Highlight all of the Roles (Cos Naming Read, Cos Naming Write, Cos Naming Create, Cos Naming Delete)

3. Click **Apply.**

   Note: Prior to this step you will need to restart the server1 since when adding CORBA Naming Service Users, the User is not recognized.

4. Note the values for JNDI User and Password. The Oracle Utilities Application Framework will prompt you for this information during the installation.

Creation of Additional Servers in WebSphere - Sample Script

You must also provide the name of servers during OUAF installation. You can use the following sample script to create additional servers using the wsadmin.sh tool.

Note: There are several other ways to accomplish this task.

1. Initialize a wsadmin.sh session:

```
<$WAS_HOME>/bin/wsadmin.sh -host localhost -port
 <SoapConnectorPort> -conntype SOAP -username
 <webSphereUserName> -password <webSphereUserPassword>
```

   Note: Substitute $WAS_HOME, webSphereUserName, SoapConnectorPort, webSphereUserPassword, with values that are appropriate for your installation:

   For example:

```
/ouaf/IBM/WebSphere85/AppServer/bin/wsadmin.sh -host
localhost -port
8889 -conntype SOAP
```

2. Create the server instance:

```
<wsadmin> $AdminTask createApplicationServer
<nodeName> {-name <serverName>}
```

Setting General Server Properties

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers,** and then select **Application Servers.**
3. Select your server name.
4. Under the section General Properties.
   - Deselect **Parallel start**.
   - Deselect **Run in development mode.**
5. Click **OK.**
6. Click **Save** to commit the setting.

Enabling SOAP Communication with WebSphere

The OUAF configuration scripts communicate with WebSphere as a SOAP client by using Jython commands to perform environment maintenance (for example, stop, start, deploy, undeploy).

To enable SOAP communication with WebSphere:

1. In a text editor, open the following file:

$WAS_HOME/profiles/<PROFILE_NAME>/properties/soap.client.props

Edit the property lines as follows:

- com.ibm.SOAP.requestTimeout=0
- com.ibm.SOAP.loginUserid=< WebSphere_User_Id >
- com.ibm.SOAP.loginPassword=< WebSphere_Password >

Note: Refer to IBM WebSphere Application Server documentation for more details.

1. If you want to encode the password in the soap.client.props file, then run the PropFilePasswordEncoder command from the $WAS_HOME/profiles/<PROFILE_NAME>/bin directory.

   This command is specific to IBM WebSphere Application Server. It encodes passwords located in plain-text property files.

2. Save and close the file.

Enabling RMI Communication with WebSphere (Webservices Enable Environment)

The IWS (Inbound Web Services Deployment) configuration scripts communicate with WebSphere using RMI for IWS commands to perform actions for IWS (for example, deploy, undeploy of the WebService.war file. When the following items are not completed, the deployment run would appear to "hang", most importantly if submitted from the OUAF online Inbound Web Services Deployment page.

To allow the deployment tasks to no RMI communication with WebSphere:

1. In a text editor, open the following file:

$WAS_HOME/profiles/<PROFILE_NAME>/properties/sas.client.props

2. Edit the property lines as follows:

```
com.ibm.CORBA.loginSource=properties
com.ibm.CORBA.loginUserid=< websphere user id>
com.ibm.CORBA.loginPassword=< websphere user password>
```

Note: Refer to IBM WebSphere Application Server documentation for more details. If you want to encode the password in the sas.client.props file, then run the PropFilePasswordEncoder command from the $WAS_HOME/profiles/<PROFILE_NAME>/bin directory.

This command is specific to IBM WebSphere Application Server. It encodes passwords located in plain-text property files.

3. Save and close the file.

Creation of Additional Servers in WebSphere - Sample Script

You must also provide the name of servers during the installation. You can use the following sample script to create additional servers using the wsadmin.sh tool.

Note: There are several other ways to accomplish this task.

1. Initialize a wsadmin.sh session:

   <$WAS_HOME>/bin/wsadmin.sh -host localhost -port <SoapConnectorPort> -conntype SOAP -username <webSphereUserName> -password <webSphereUserPassword>

   Note: Substitute $WAS_HOME, webSphereUserName, SoapConnectorPort, webSphereUserPassword, with values that are appropriate for your installation:

For example: /ouaf/IBM/WebSphere85/AppServer/bin/wsadmin.sh -host localhost -port 8889 -conntype SOAP

2. Create the server instance:

   wsadmin> $AdminTask createApplicationServer <nodeName> {-name <serverName>}

Obtaining the Bootstrap Port and WC_defaulthost_secure

You must also provide these port numbers during Oracle Utilities Application Framework installation. Obtain the bootstrap port number and the WC_defaulthost_secure by using the WebSphere administrative console.

> **Note:** The WebSphere application server1 must be running to obtain the bootstrap port number and the WC_defaulthost_secure port number.

To view the bootstrap port number and the WC_defaulthost_secure:

1. Log on to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers, <server_name>** and then select **Ports** under **Communications.**

   The bootstrap port is displayed as BOOTSTRAP_ADDRESS.

   The WC_defaulthost_secure is displayed as WC_defaulthost._secure

3. Note the values for WC_defaulthost_secure and BOOTSTRAP_ADDRESS. The Oracle Utilities Application Framework will prompt you for this information during the installation.

Set Up a Virtual Host for the Server

1. Select **Environment, Virtual Host, default_host,** and then select **Host Alias.**
2. Click **New.**

   Enter the following:

   - **Host Name:** *
   - **Port:** WC_defaulthost_secure Port Number

Obtaining the WebSphere Node Name

You must also provide the node name during the installation. Obtain the node name by using the WebSphere administrative console.

> **Note:** The WebSphere application server must be running to obtain the bootstrap port number.

To obtain the node name:

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers, <server_name>.**

   Note: Take note of the value for the Node Name.

Installing Oracle Utilities Application Framework as a Non-Root User with IBM WebSphere Installed as Root

Installing Oracle Utilities Application Framework as a non-root user on a WebSphere application server running on AIX requires certain permissions. Prior to the installation, verify that the operating system user account installing the framework has write and execute permissions on the directories in which WebSphere will be installed.

Post-Installation Tasks

This sections describes tasks that you should complete after you have installed Oracle Utilities Customer Care and Billing on a WebSphere application server.

Setting Environment Entries.

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers.**
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to Environment Entries.
7. Click **New** and add the following Environment Entries:

   Name: SPLENVIRON

   Value: <$SPLENVIRON>

   Note: Substitute $SPLENVIRON with appropriate values for your installation.

   Name: SPLEBASE

   Value: < $SPLEBASE >

   Note: Substitute $SPLEBASE with appropriate values for your installation.

   Name: LIBPATH

   Value: <$SPLEBASE >/runtime

   Note: Substitute $SPLEBASE with appropriate values for your installation.

   Note: You will need to restart the server_name before you attempt to start the application on the server.
8. Click **OK.**
9. Click **Save** to commit the setting.

Setting JVM Memory and Arguments

For Oracle Utilities Application Framework, JVM memory settings must be changed for production environments and/or when processing large volume in a nonproduction environment.

Perform the following steps to set the JVM memory size. The WebSphere application server must be running to set the memory size.

To set the JVM memory size:

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers.**
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to **Additional Properties,** and then click **Java Virtual Machine.**
7. Enter 2048 for **Minimum Heap Size.**
8. Enter 2048 for **Maximum Heap Size.**

Note: Modify the memory settings based on your production installation needs.

9. Enter -Djava.security.auth.login.config=<$SPLEBASE>/splapp/config/java.login.config for Generic JVM arguments.

   Note: Substitute $SPLEBASE with appropriate values for your installation.

   You will need to restart the server_name before you attempt to start the application on the server.

10. Click **OK.**
11. Click **Save** to commit the setting.

Setting Server Custom Properties.

The following custom properties have been need in the past to enable WebSphere Classloader to load the correct xalan.jar file.

To set the Custom Properties:

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers.**
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to **Additional Properties,** and then click **Java Virtual Machine.**
7. Go to **Additional Properties,** and then click **Custom Properties.**
8. Click **New.**

   Enter the following information:

   - **Name**: javax.xml.transform.TransformerFactory
   - **Value:** org.apache.xalan.processor.TransformerFactoryImpl

9. Click **OK.**
10. Click **Save** to commit the setting.

Setting the Web Container Custom Properties.

To set the Web Container Custom Properties:

1. Connect to the WebSphere administrative console.
2. Select **Servers, Server Types, WebSphere application servers.**
3. Select the server name.
4. Go to **Container Settings,** and then click **Web Container Settings.**
5. Select **Web container.**
6. Go to **Additional Properties,** and then click **Custom properties.**
7. Click **New.**

   Enter the following information:

   - **Name:** com.ibm.ws.webcontainer.invokefilterscompatibility
   - **Value:** true

8. Click **OK.**

9. Click **Save** to commit the setting.

Starting and Stopping WebSphere Servers

To start WebSphere use the $WAS_HOME/profiles/<profile_name>/bin/startServer.sh script. For example, run:

```
$WAS_HOME/profiles/<profile_name>/bin/startServer.sh <server_name>
```

To stop WebSphere, use the $WAS_HOME/profiles/<profile_name>/bin/stopServer.sh script. For example, run:

```
$WAS_HOME/profiles/<profile_name>/bin/stopServer.sh <server_name
```

> **Note:** The Oracle Utilities Application Framework script **spl.sh** does not stop or start the WebSphere servers. It only stops and starts the Oracle Utilities Application Framework-based applications.

Deployment Using Supplied Script

The application deployment script is initialSetup.sh.-d, located in $SPLEBASE/bin (this script deploys both the SPLService.ear and SPLWeb.ear)

> **Note:** Before running the script ensure you have initialized the environment by running splenviron.sh

Deployment via the Admin Console

Follow these steps to deploy the application using the Admin Console:

Deployment Overview

The application needs to be deployed in the following order:

1. SPLService.ear
2. SPLWeb.ear

> **Note:** The SPLService.ear must be successfully deployed before deploying SPLWeb.ear

Deploy SPLService.ear

1. Select the ear file to deploy.
   - Select **Applications, Install New Application.**
   - Select **Remote file system.**
   - Browse to the SPLService.ear or enter the full path to the file.
   - The ear files can be found under $SPLEBASE/splapp/applications.
   - Click **Next.**
2. Select **Option Fast Path - Prompt only when additional information is required.** Click **Next.**
3. On the **Select Installation Options** page ensure that **Deploy enterprise beans** is checked. Click **Next.**
4. Assign the module to the WebSphere server instance.

   When deploying an application from the console make sure you select the correct server and click **Apply.**
5. Review the summary page. Review the installation options.
6. Click **Finish**. The application will then deploy. The deployment process takes about 5 minutes.

7. Click **Save.** The save process may take more than 20 minutes.

Deploying SPLWeb.ear

1. Select the ear file to deploy.
   - Select **Applications, Install New Application.**
   - Select **Remote file system.**
   - Browse to the SPLWeb.ear or enter the full path to the file.
   - The ear files can be found under $SPLEBASE/splapp/applications.
   - Click **Next.**
2. Select **Option Fast Path - Prompt only when additional information is required.** Click **Next.**
3. Assign the module to the WebSphere server instance.

   When deploying an application from the console make sure you select the correct server and click Apply.
4. Review the summary page. Review the installation options.
5. Click **Finish.** The application will then deploy. The deployment process takes about 5 minutes.
6. Click **Save.** The save process may take about more than 20 minutes.

Configure the Applications

You need to apply these steps to both the SPLWeb and SPLService applications unless specified.

1. Set the startup order of the applications (this applies only to SPLWeb):
   - Select the SPLWeb application from **Applications, Enterprise Applications.**
   - Select **Startup behavior.**
   - Change the startup order to 2.
   - Click **OK.**
   - Click **OK** and Save directly to master configuration.
2. Set the class loading order (for both SPLService.ear and SPLWeb.ear): Select Class loading and update detection.
   - Set Polling interval to 0.
   - Under Class loader order select Classes loaded with application class loader first. Click **OK** and Save to master configuration.
3. Set the module starting weight:
   - **SPLService only:** Set the Starting weight to 1.
   - **SPLWeb only:** For each module (.war) set the Starting weight to 10000 and change the Class loader order to Classes loaded with application class loader first
4. Set EJB JNDI names (this applies only to SPLService). Select Enterprise Java Bean Properties and enter the following values:
   - **EJB module:** SPLServiceBean
   - JNDI name for all interfaces
   - **Target Resource JNDI Name:** [Web Context Root]/servicebean
   - **EJB module:** TUGBULiteServiceBean
   - JNDI name for all interfaces
   - **Target Resource JNDI Name:** [Web Context Root]/liteservicebean
5. Click **Ok.**

Configure Application Security

After using the supplied script to deploy the application to WebSphere you will need to configure each application's security before starting the application.

Using the WebSphere administration console select **Applications, Application Types, WebSphere enterprise applications, <Business Server Application Name>, <server name>** (for example, SPLService-server2)**, Security role to user/group mapping.**

For role cisusers:

- Check **Select** and the click **Map Users:**
- Search for SYSUSER and add to the Selected users list.
- Click **OK.**

Note: Repeat the process for <Web Server Application Name>-<server name> (for example, SPLWeb-server2).

Restart the WebSphere Server

It is recommended to stop and then restart the WebSphere server.

If the application is deployed in server1 you can use the admin console to stop and start the server. If the application is deployed in another server you will need to use the scripts that are supplied with WebSphere (stopServer.sh, startServer.sh).

Note: WebSphere admin console runs under server1.

Application URL

The Web link to the WebSphere application will be:

```
http://<hostname>:<WC_defaulthost_secure>/<context_root>/loginPage.jsp
```

For example, http://oracle:9081/ouaf/loginPage.jsp

Configuring WebSphere Network Deployment

Pre-Installation Tasks

This section describes tasks that you should complete to configure a WebSphere ND application server before you install the Oracle Utilities Application Framework.

When working within the WebSphere Network Deployment (WebSphere ND) console make sure to apply and save your changes to the Master Configuration when appropriate.

Setting of WebSphere ND Security

There are several security configuration options within WebSphere ND. In a production environment you must use the security implementation appropriate for your security requirements. During the Release cycle we used the User account repository of the Federated repository. The following procedures describe how to apply these security settings.

> **Note:** Refer to WebSphere ND Application Server documentation for more details.

1. Start the WebSphere ND DPMGR Administrative Console and log in.
2. Go to S**ecurity, Global security.**
   - Check **Enable administrative security.**
   - Check **Enable application security.**
   - Select **Federated repositories** from the Available realm definitions.
3. Click **Apply.**

Setting WebSphere ND Application Groups

1. Start the WebSphere ND Administrative Console and log in.
2. Go to **Users and Groups - Manage Groups.**

   Create the group name of cisusers (default group).
3. Click **Create.**

Setting WebSphere ND Application Users

1. Start the WebSphere ND Administrative Console and log in.
2. Go to **Users and Groups - Manage Users**.
   - Create the user Id of SYSUSER (example user).
   - Add the Group Membership of cisusers (created in the previous step) to the user.
3. Click **Create.**

Setting WebSphere ND JNDI Users

1. Start the WebSphere Administrative Console and log in.
2. Go to **Users and Groups - Manage Users.**

   Create the user id of JNDI (example user).

   Add the Group Membership of cisusers to the user id of JNDI (created above)
3. Click **Create.**

Setting WebSphere ND JNDI Users - CORBA Naming Service Users

1. Start the WebSphere ND Administrative Console and log in.
2. Go to **Environment, Naming - CORBA Naming Service Users.**

- Add the user id of JNDI (example user).
- Highlight all of the Roles (Cos Naming Read, Cos Naming Write, Cos Naming Create, Cos Naming Delete).

3. Click **Apply.**

   Note: the values for JNDI User and Password. The Oracle Utilities Application Framework will prompt you for this information during the installation.

Setting General Server Properties.

1. Connect to the WebSphere ND DPMGR administrative console
2. Select **Servers, Server Types, WebSphere application servers.**
3. Select the your server name.
4. Under the section General Properties.
   - Deselect **Parallel start.**
   - Deselect **Run in development mode.**
5. Click **OK.**
6. Click **Save** to commit the setting.

Enabling SOAP Communication with WebSphere ND

The OUAF configuration scripts communicates with WebSphere ND Deployment Manager as a SOAP client by using Jython commands to perform environment maintenance (e.g. stop, start, deploy, undeploy).

To enable SOAP communication with WebSphere ND:

1. In a text editor, open the following file:

   ```
   $WAS_HOME/profiles/<PROFILE_NAME>/properties/soap.client.props
   ```

   Edit the property lines as follows:

   - com.ibm.SOAP.requestTimeout=0
   - com.ibm.SOAP.loginUserid=< WebSphere_User_Id >
   - com.ibm.SOAP.loginPassword=< WebSphere_Password >

     Note: Refer to IBM WebSphere Application Server documentation for more details,

2. If you want to encode the password in the soap.client.props file, then run the PropFilePasswordEncoder command from the $WAS_HOME/profiles/<PROFILE_NAME>/bin directory.

   This command is specific to IBM WebSphere ND Application Server, and it encodes passwords located in plain-text property files.

3. Save and close the file.

Enabling RMI Communication with WebSphere (Webservices Enable Environment)

The IWS (Inbound Web Services Deployment) configuration scripts communicate with WebSphere using RMI for IWS commands to perform actions for IWS (for example, deploy, undeploy of the WebService.war file. When the following items are not completed, the deployment run would appear to "hang", most importantly if submitted from the OUAF online Inbound Web Services Deployment page.

To allow the deployment tasks to no RMI communication with WebSphere:

1. In a text editor, open the following file:

$WAS_HOME/profiles/<PROFILE_NAME>/properties/sas.client.props

2. Edit the property lines as follows:

```
com.ibm.CORBA.loginSource=properties
com.ibm.CORBA.loginUserid=< websphere user id>
com.ibm.CORBA.loginPassword=< websphere user password>
```

Note: Refer to IBM WebSphere Application Server documentation for more details. If you want to encode the password in the sas.client.props file, then run the PropFilePasswordEncoder command from the $WAS_HOME/profiles/<PROFILE_NAME>/bin directory.

This command is specific to IBM WebSphere Application Server. It encodes passwords located in plain-text property files.

3. Save and close the file.

Creation of Additional Servers in WebSphere ND

You must also provide the server names during the installation.

Note: There are several other ways to accomplish this task.

1. Select **Servers, New Servers.**

   This will lead you through a list of steps for creating a new server.

2. Select server type from the drop down list: WebSphere application server. Click **N.ext**

3. Select node from the drop down list that has been created for to host the WebSphere server.

   Enter the Server name

   Note: Both the Node Name and Server Name will be needed for during the OUAF installation process.

4. Select a server template of default

   Click Next

5. Check the box to Generate Unique Ports. Click Next

6. Confirm new server. Click Finished

Obtaining the Bootstrap Port and WC_defaulthost_secure

You must also provide these port numbers during Oracle Utilities Application Framework installation. Obtain the bootstrap port number and the WC_defaulthost_secure by using the WebSphere ND administrative console.

Note: The WebSphere ND Deployment Manager server must be running to obtain the bootstrap port number and the WC_defaulthost_secure port number

To view the bootstrap port number and the WC_defaulthost_secure:

1. Log on to the WebSphere ND administrative console.

2. Select Servers, Application Servers, <server_name>, and then select **Ports** under Communication.

   The bootstrap port is displayed as BOOTSTRAP_ADDRESS. The WC_defaulthost_secure is displayed as WC_defaulthost_secure.

3. Note the values for WC_defaulthost_secure and BOOTSTRAP_ADDRESS. The Oracle Utilities Application Framework will prompt you for this information during the installation.

Set up a New Virtual Host for your Server

1. Select **Environment, Virtual Host, default_host,** and then select **Host Alias.**
2. Click **New.**
3. Enter the following:
   - Host Name:
   - Port: WC_defaulthost_secure Port Number

Obtaining the WebSphere ND Node Name

You must also provide the node name during OUAF installation. Obtain the node name by using the WebSphere ND administrative console.

> **Note:** The IBM WebSphere ND application server must be running to obtain the bootstrap port number.

To obtain the node name:

1. Connect to the WebSphere ND administrative console
2. In the left pane, click **Servers.**
3. Click **Application Servers** under Servers.
4. Click the server instance (server_name, default) on the right section.
5. Click the **Runtime** tab.

   Note: The value for the Node Name.

   Note: If the value of State is not started, then restart the server instance.

Installing Oracle Utilities Application Framework as a Non-Root User with IBM WebSphere Installed as Root

Prior to attempting to install Oracle Utilities Application Framework as a non-root user on a IBM WebSphere ND application server running on Unix, verify that the operating system user account installing Oracle Utilities Application Framework has write and execute permissions on the directories in which IBM WebSphere ND will be installed.

Post-Installation Tasks

This sections describes tasks that you should complete after you have installed the Oracle Utilities Application Framework and Oracle Utilities Customer Care and Billing on a WebSphere application server.

Setting Environment Entries.

1. Connect to the IBM WebSphere ND administrative console.
2. Select **Servers** and then select **Application Servers.**
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to **Environment Entries.**
7. Click **New** and add the following Environment Entries:

   Add the following entries:

   Name: SPLENVIRON

   Value: <$SPLENVIRON>

Note: Substitute $SPLENVIRON with appropriate values for your installation.

Name: SPLEBASE

Value: < $SPLEBASE >

Note: Substitute $SPLEBASE with appropriate values for your installation.

Name: LIBPATH

Value: <$SPLEBASE >/runtime

Note: Substitute $SPLEBASE with appropriate values for your installation.

Note: You will need to restart the server_name before you attempt to start the application on the server.

8. Click **OK.**
9. Click **Save** to commit the setting.

Setting JVM Memory and Arguments

For Oracle Utilities Application Framework, JVM memory settings must be changed for production environments and/or when processing large volume in a nonproduction environment.

Perform the following steps to set the JVM memory size. The IBM WebSphere ND application server must be running to set the memory size.

To set the JVM memory size:

1. Connect to the IBM WebSphere ND administrative console.
2. Select **Servers,** and then select **Application Servers.**
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to **Additional Properties,** and then click **Java Virtual Machine.**
7. Enter 2048 for **Minimum Heap Size.**
8. Enter 2048 for **Maximum Heap Size.**

   Note: Modify the memory settings based on your production installation needs.
9. Enter -Djava.security.auth.login.config=<$SPLEBASE>/splapp/config/java.login.config for Generic JVM arguments.

   Note: Substitute $SPLEBASE with appropriate values for your installation.

   You will need to restart the server_name before you attempt to start the application on the server.
10. Click **OK.**
11. Click **Save** to commit the setting.

Setting Server Custom Properties.

The following custom properties have been need in the past to enable WebSphere ND Classloader to load the correct xalan.jar file.

To set the Custom Properties:

1. Connect to the WebSphere ND administrative console.
2. Select **Servers,** and then select Application Servers.
3. Select the server name.
4. Go to **Server Infrastructure,** and then click **Java and Process Management.**
5. Select **Process Definition.**
6. Go to **Additional Properties,** and then click **Java Virtual Machine.**
7. Go to **Additional Properties,** and then click **Custom Properties.**
8. Click **New.**

   Enter the following information:

   Name: javax.xml.transform.TransformerFactory

   Value: org.apache.xalan.processor.TransformerFactoryImpl
9. Click **OK.**
10. Click **Save** to commit the setting.

Setting Up the Web Container Custom Properties.

To set the Web Container Custom Properties:

1. Connect to the WebSphere ND administrative console.
2. Select **Servers,** and then select **Application Servers.**
3. Select the server name.
4. Go to **Container Settings,** and then click **Web Container Settings.**
5. Select Web container
6. Go to **Additional Properties,** and then click **Custom properties.**
7. Click **New.**

   Enter the following information:

   Name: com.ibm.ws.webcontainer.invokefilterscompatibility

   Value: true
8. Click **OK.**
9. Click **Save** to commit the setting.

Starting and Stopping WebSphere ND servers

You can use the WebSphere ND console to stop and start the servers. You can also use the command line scripts supplied with WebSphere ND.

> **Note:** The Oracle Utilities Application Framework utility **spl.sh** does not stop or start the IBM WebSphere ND servers. It only stops and starts the Oracle Utilities Customer Care and Billing applications.

Deployment Using Supplied Script

The application deployment script is initialSetup.sh.-d, located in $SPLEBASE/bin (this deploys both the SPLService.ear and SPLWeb.ear).

> **Note:** Before running the script ensure you have initialized the environment by running splenviron.sh

Deployment via the Admin Console

Follow these steps to deploy the application using the Admin Console:

Deployment Overview

The application needs to be deployed in the following order:

1. SPLService.ear
2. SPLWeb.ear

   Note: The SPLService.ear must be successfully deployed before deploying SPLWeb.ear

Deploy SPLService.ear

1. Select the ear file to deploy.
   - Select **Applications, Install New Application.**
   - Select **Remote file system.**
   - Browse to the SPLService.ear or enter the full path to the file.
   - The ear files can be found under $SPLEBASE/splapp/applications.

   Click **Next.**
2. Select **Option Fast Path - Prompt only when additional information is required.**

   Click **Next.**
3. On the Select installation options page

   Ensure **Deploy enterprise beans** is selected.

   Click **Next.**
4. Assign the module to the IBM WebSphere ND server instance.

   When deploying an application from the console make sure you select the correct server and click **Apply.**
5. Review the summary page. Review the installation options
6. Click **Finish**. The application will then deploy. The deployment process takes about 5 minutes.
7. Click **Save.** The save process can take about more than 20 minutes.

Deploying SPLWeb.ear

1. Select the ear file to deploy.
   - Select **Applications, Install New Application.**
   - Select **Remote file system.**
   - Browse to the SPLWeb.ear or enter the full path to the file.
   - The ear files can be found under $SPLEBASE/splapp/applications.

   Click **Next.**
2. Select **Option Fast Path - Prompt only when additional information is required.**

   Click **Next.**
3. Assign the module to the IBM WebSphere ND server instance.

   When deploying an application from the console make sure you select the correct server and click **Apply.**
4. Review the summary page. Review the installation options

5. Click **Finish**. The application will then deploy. The deployment process takes about 5 minutes.
6. Click **Save.** The save process can take about more than 20 minutes.

Configure the Applications

You need to apply these steps to both the SPLWeb and SPLService applications unless specified.

1. Set the startup order of the applications (this applies only to SPLWeb):
   - Select the SPLWeb application from **Applications, Enterprise Applications.**
   - Select **Startup behavior.**
   - Change the startup order to 2.

   Click **OK.**

   Click **OK** and Save directly to master configuration.
2. Set the class loading order (for both SPLService.ear and SPLWeb.ear): Select Class loading and update detection.
   - Set Polling interval to 0.
   - Under Class loader order select Classes loaded with application class loader first. Click OK and Save to master configuration.
3. Set the module starting weight:
   - SPLService only - set the Starting weight to 1.
   - SPLWeb only - for each module (.war) set the Starting weight to 10000 and change the Class loader order to Classes loaded with application class loader first
4. Set EJB JNDI names (this applies only to SPLService). Select Enterprise Java Bean Properties and enter the following values:
   - **EJB module:** SPLServiceBean
   - JNDI name for all interfaces
   - **Target Resource JNDI Name:** [Web Context Root]/servicebean
   - **EJB module:** TUGBULiteServiceBean
   - JNDI name for all interfaces
   - **Target Resource JNDI Name:** [Web Context Root]/liteservicebean
5. Click **Ok.**

Configure Application Security

After using the supplied script to deploy the application to IBM WebSphere ND you will need to configure each application's security before starting the application.

Using the IBM WebSphere ND administration console select **Applications, Enterprise Applications, Business-<server name>** (for example, SPLService-server2), **Security role to user/group mapping.**

For role cisusers:

- Check **All Authenticated.**
- Check **Select** and click **Look up users:**
- Search for SYSUSER and add to the Selected users list.
- Click **OK.**

Note: Repeat the process for <Web Server Application Name>-<server name>(for example, SPLWeb-server2).

Restart the IBM WebSphere ND Server

It is recommended to stop and then restart the WebSphere ND server.

Application URL

The Web link to the IBM WebSphere ND application will be:

```
   http://<hostname>:<WC_defaulthost_secure>/<context_root>/
loginPage.jsp
```

For example, http://oracle:9085/ouaf/loginPage.jsp

Chapter 7

Installing the Application Server Component of Oracle Utilities Application Framework

Installing the Oracle Utilities Application Framework ("the framework") is the prerequisite and foundation for installing a framework-based application such as Oracle Utilities Customer Care and Billing. This section describes the process for installing the Oracle Utilities Application Framework, including:

- Installation Overview
- Pre-Installation Tasks
- Installing Oracle Utilities Application Framework

Installation Overview

The installation packages for your Oracle Utilities Application Framework-based application must be downloaded from the Oracle Software Delivery Cloud.

Application server installations are new, you cannot upgrade an existing application server. The database installation can be an initial install or an upgrade install.

Before you proceed with the installation process:

1. Complete the database installation/upgrade process. Refer to the *Oracle Utilities Customer Care and Billing Database Administrator's Guide*.
2. Make sure that you have installed all the required third-party software as described in Chapter 5**:** Installing Application Server Prerequisite Software.

Once the Oracle Utilities Application Framework installation is successfully completed and the framework application environment is created, Oracle Utilities Customer Care and Billing can be installed on top of the framework environment.

You can download the installation packages from the Oracle Software Delivery Cloud.

This section describes how to install a working Oracle Utilities Application Framework Server, which can then be further configured manually to allow for production performance levels.

Application server installation packages delivered for this version are multi-platform and are ready to install on any supported platform (as described in the section Supported Platforms).

Pre-Installation Tasks

Hardware and Software Version Prerequisites

The section Supported Platforms contains all of the available platforms that are required with this release of the product.

Database Installation

Verify that the database has been installed and is operational. See *Oracle Utilities Customer Care and Billing Database Administrator's Guide* for more information.

Installation Prerequisites

Chapter 5: Installing Application Server Prerequisite Software describes all preparations that need to be done on the server prior to installing the application server. Please read carefully the server setup requirements and make sure that all prerequisite software is installed and that all required environment variables are set. Correct server setup and proper environment variable settings are an essential prerequisite for successful environment installation.

System Architecture Overview

Oracle Utilities Application Framework V4.3.0.2.0 is a decoupled system architecture involving a business service application tier and a web application tier. Typically both will run on the same server, but the design does allow each tier to be installed on separate servers.

The design implements a stateless session bean (EJB technology, under Java EE 7), to provide remote access to service invocations. The root web app and XAI web apps can be configured to access service processing locally (as in previous versions), or to make a remote EJB call to perform the service request. In the latter case, the served containers, effectively, run as very thin servlet wrappers around the remote call.

For all supported application servers except for WebLogic expanded configuration (SDK environment), the deployment is in the form of two Enterprise Archive (ear) Files: SPLService.ear and SPLWeb.ear. Web Archive (war) files are created during the installation process but are not deployed.

Copying and Decompressing Install Media

The Oracle Utilities Application Framework V4.3.0.2.0 installation file is delivered in jar format for both UNIX and Windows platforms. If you are planning to install multiple Oracle Utilities Application Framework V4.3.0.2.0 environments operated by different Oracle Utilities administrator user IDs, you must complete each of the following installation steps for each administrator user ID.

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 V4.3.0.2.0 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-V4.3.0.2.0-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-V4.3.0.2.0-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-V4.3.0.2.0-SP2" is created. It contains the installation software for the Oracle Utilities framework application server.

Set 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-V4.3.0.2.0-SP2 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 Application 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 Application 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.

Installing Oracle Utilities Application Framework

This section outlines the steps for installing the Application Framework.

Installation Process (Brief Description)

1. Log on as the Oracle Utilities Framework administrator (the default is cissys on UNIX) or as a user with Administrator privileges (on Windows).
2. Configure your application server and any third-party software required for your platform, as outlined in Chapter 5**:** Installing Application Server Prerequisite Software
3. Change directory to the <*TEMPDIR*>/FW-V4.3.0.2.0-SP2 directory.
4. Set the following path:

   ```
   export PATH=/<JAVA_HOME>/bin:/<JAVA_HOME>/lib:$PATH
   ```

   Note: The above command is only applicable on a Unix platform. <JAVA_HOME> is the location where the JDK has been installed.
5. Start the application installation utility by executing the appropriate script:

   UNIX: ksh ./install.sh

   Windows: install.cmd
6. Follow the messages and instructions that are produced by the application installation utility. Use the completed worksheets in the section Installation and Configuration Worksheets to assist you.
7. Installation of Oracle Utilities Framework Application Server is complete if no errors occurred during installation.

Installation Process (Detailed Description)

1. Log on to the host server as Oracle Utilities Application Framework administrator.

   Logon as cissys (on UNIX) or as a user with Administrator privileges (on Windows).
2. Configure application server and third-party software.

   Complete all steps outlined in Installing Application Server Prerequisite Software You will need to obtain specific information for the install.
3. Change directory to the <*TEMPDIR*>/FW-V4.3.0.2.0-SP2 directory and start the application installation utility by executing the appropriate script:

   UNIX: ksh ./install.sh

   Windows: install.cmd
4. On the Environment Installation Options menu, select item 1: Environment ID, Roles, Third Party Software Configuration.

   Use the completed Environment ID, Roles, Third Party Software Configuration worksheet in Installation and Configuration Worksheets to complete this step.
5. Select menu item 2: Keystore Options.

   Use the completed Keystore Options Worksheet to complete this step. See Installation and Configuration Worksheets.
6. Select menu item 50: Environment Installation Options.

   Use the completed Environment Installation Options Worksheet to complete this step. See Installation and Configuration Worksheets.

Note: You must create the directory for output (the Log Mount Point). The installation process fails if this directory does not exist.

- Specify the environment mount point, log files mount point, name and the environment directory names for a new installation on a menu screen.
- Specify the web application server type your environment will run with (the default will be WebLogic).
- Specify if you want to install the application viewer module
- Specify if you want to install the demo certificate generation scripts
- Specify if you want to install sample custom code
- Enter P to accept the selected options.
- During this step, the specification of a new environment is checked for validity against /etc/cistab and the permissions on mount points and directories.

7. Configure environment parameters.
   - During this step you will configure environment parameters such as web server hosts and ports, database name, and user ID.
   - The application installation utility shows default values for some configuration options.
   - Use the completed Environment Configuration Worksheet to assist you.
   - Note: Some options require a value for a successful install. It is important to provide these values as described in the previous sections.
   - When you are done with the parameters setup, proceed with the option P.
   - All of the options will be written in the following File: $ SPLEBASE/etc/ ENVIRON.INI.
   - You will be warned if you did not edit a section. You may proceed if you want to keep the default settings.
   - The application installation utility copies the installation media to a new environment.
   - The application installation utility generates environment configuration parameters:
     - The application installation utility automatically executes the script initialSetup.sh (on UNIX) or initialSetup.cmd (on Windows), located in $SPLEBASE/bin (%SPLEBASE%\bin on Windows) directory. This script populates different application template configuration files with the new environment variables values and completes the rest of the installation steps.
8. Set up environment variables.

   Once the ENVIRON.INI file is created and contains the correct environment parameters, the application installation utility starts a sub shell to the current process by executing the splenviron.sh (on UNIX) or splenviron.cmd (on Windows) script, located in $SPLEBASE/bin (or *%SPLEBSE%\etc for Windows)* directory. This script sets up all the necessary environment variables and shell settings for the application server to function correctly.

   From this point, a number of environment variables have been set up. Some key ones are:

   - $PATH - an adjustment to $PATH is made so that all of the environment scripts and objects will be in the path.
   - $SPLEBASE (%SPLEBASE%) - stands for <SPLDIR>/<SPLENVIRON> directory
   - $SPLOUTPUT (%SPLOUTPUT%) - stands for <SPLDIROUT>/<SPLENVIRON> directory
   - $SPLENVIRON (%SPLENVIRON%) - environment name

For future operations or any post installation steps, you need to first execute the following command to setup your session to the new environment:

UNIX: $SPLEBASE/bin/splenviron.sh -e <SPLENVIRON>

Windows:%SPLEBASE%\bin\splenviron.cmd -e <SPLENVIRON>

You need to execute this script each time you want to be connected to the specific environment before performing manual operations such as shutdown, startup or performing an additional application product installation.

When you have finished the install process, your current online session will be connected to the new environment.

See the Planning the Installation for settings and configuration.

Detailed Description for Configuring the OUAF Keystore

The following section details the steps required to configure the OUAF keystore.

OUAF Keystore

The OUAF Keystore feature secures sensitive data such as passwords and prevents tampering of long login IDs via direct updates to the database. The application server uses an external keystore to store keys for system password and other sensitive system data including user "hashes" that are used to verify the validity of email long login IDs. In order to run the application correctly, the keystore used by the application server must match the data encrypted in the database. If they do not match, the application will not be able to decrypt passwords correct, nor will users be able to log on due to a mismatch of user security hashes.

To help manage the keystore and ensure that the keystore matches the database-encypted data, there is a system check at startup of the application that display warning messages when the system detects that the keystore in use does not match the encrypted data in the database. Thus after any keystore operation, fresh installation of the application, or reconfiguration to point to a different database, the keystore will need to be synchronized with the database. Synchronization of the keystore happens any time ChangeCryptographyKey or ResetCryptography key programs are run.

After running the cryptography programs, it is necessary to reset the database credentials used by the database patching utility with the nvokeDBUpdatePatch.sh|cmd script.

> **Note**: The database utility ORADBI does not require the keystore files. Please refer to the database documentation for more details.

The following lists the common administrative activities related to the keystore.

Determining keystore in use

You can determine if an existing application server uses a keystore through the existence of the files in the following location. (Use the ls -a option in Unix systems to list all files):

<SPLEBASE>/ks/.ouaf_keystore

<SPLEBASE>/ks/.ouaf_storepass

If there are no files in this location, then the system is not using a keystore. Starting from 4.2.0.2.0, a keystore should be in use.

Configuring the keystore options

If you would like to customize the keystore options, the Install Menu includes a section for keystore options as shown below. You can access the Install Menu later through (execute configureEnv.sh|cmd -i):

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
```

Importing an existing keystore

This will import a keystore from an existing environment to the current one. Use this when upgrading from 4.2.0.2.0 or when reconfiguring environments using different keystores and you want them to point to the same database schema (e.g. you want to have more than one application server pointing to the same database schema).

Follow these steps:

1. Enter the keystore options from the the install menu or from the configureEnv.sh|cmd –i as above.
2. Run initialSetup.sh|cmd –s so that the keystore is imported and appropriate property files are updated.
3. Run configureEnv.sh|cmd and re-enter the passwords so they are encrypted with the imported keystore.
4. Run initialSetup.sh|cmd again to update property files with the encrypted data.
5. Run:

```
•perl $SPLEBASE/bin/run_java_standalone.plx
com.splwg.shared.common.ChangeCryptographyKeRun $SPLEBASE/bin/
nvokeDBUpdatePatch.sh|cmd and follow the prompts.
```

You can use the –h option to obtain help.

Upgrading from the Legacy Keystore

This will:

- synchronize the keystore to the database
- regenerate the user hashes
- reencrypt any passwords (from the legacy-encrypted passwords) using the current keystore.
- Use this only when upgrading from a framework prior to version 4.2.0.2.0.

Follow these steps:

1. Run:

```
perl $SPLEBASE/bin/run_java_standalone.plx
com.splwg.shared.common.ChangeCryptographyKey -l -h
```

2. Run $SPLEBASE/bin/nvokeDBUpdatePatch.sh|cmd and follow the prompts. You can use the –h option to obtain help.

Forcing the environment to use the current keystore

This process will:

- prompt for and encrypt application server-stored passwords
- synchronize the keystore to the database
- regenerate the user hashes

- invalidate any database-stored passwords
- Use this option when, for example, a keystore has been lost, and thus, the system will not be able to decypt the passwords stored in the configuration files or database. All passwords will need to be reentered.

Follow these steps:

1. Using configureEnv.sh|cmd, re-enter the menu passwords to encrypt the data.
2. Run initialSetup.sh|cmd to update property files with the encrypted data.
3. Run:

```
perl $SPLEBASE/bin/run_java_standalone.plx
com.splwg.shared.common.ResetCryptographyKey
```

4. Run $SPLEBASE/bin/nvokeDBUpdatePatch.sh|cmd and follow the prompts. You can use the –h option to obtain help.
5. Re-enter stored password information using the application (e.g. passwords for reports)

Synchronizing the Keystore

This will

- synchronize the keystore to the database
- regenerate the user hashes
- Follow these instructions only when you are sure the data in the database is encrypted with the current keystore. This is used to synchronize the keystore to the database.

Follow these steps:

1. Run:

```
perl $SPLEBASE/bin/run_java_standalone.plx
com.splwg.shared.common.ResetCryptographyKey
```

2. Run $SPLEBASE/bin/nvokeDBUpdatePatch.sh|cmd and follow the prompts. You can use the –h option to obtain help.

Creating a new keystore

This will

- prompt for and encyrpt new application server-stored passwords
- synchonize the keystore to the database
- regenerate user hashes
- decrypt the passwords using the old keystore and encrypt them using the new keystore.

Follow these steps:

1. Copy the old keystore to a temporary directory as a backup measure.
2. Run initialSetup.sh|cmd –k to generate the new keystore.
3. Using configureEnv.sh|cmd, re-enter the menu passwords to encrypt the data.
4. Run initialSetup.sh|cmd to update property files with the encrypted data.
5. Run:

```
perl $SPLEBASE/bin/run_ java_standalone.plx
-Dcom.oracle.ouaf.system.old.keystore.file={property-value}
-Dcom.oracle.ouaf.system.old.keystore.passwordFileName={property-
value}
-Dcom.oracle.ouaf.system.old.keystore.type={property-value}
-Dcom.oracle.ouaf.system.old.keystore.alias={property-value}
-Dcom.oracle.ouaf.system.old.keystore.padding={property-value}
```

```
-Dcom.oracle.ouaf.system.old.keystore.mode={property-value}
 com.splwg.shared.common.ChangeCryptographyKey
```

where {property-value}is related to the old keystore

6. Run $SPLEBASE/bin/nvokeDBUpdatePatch.sh|cmd and follow the prompts. You can use the –h option to obtain help.

Chapter 8

Installing the Application Server Component of Oracle Utilities Customer Care and Billing

This section describes the procedure for installing Oracle Utilities Customer Care and Billing on top of the previously created Oracle Utilities Application Framework environment. This section includes:

- Pre-installation Tasks
- Installing the Application
- Integrating Customer Modifications into This Release
- Operating the Application
- Installing Service Packs and Patches

You can download the installation package from the Oracle Software Delivery Cloud. If the Framework installation was processed on previously existing Oracle Utilities Customer Care and Billing environment, then customer modifications relevant for this version and compliant with the proper naming conventions (as described in the *Oracle Utilities Customer Care and Billing Database Administrator's Guide)* have been preserved in the new environment by the Framework installation process.

To proceed with the Oracle Utilities Customer Care and Billing installation you need to be connected to the target framework application environment. See the detailed installation instructions in the following section.

You *must* initialize the Framework environment along with the required Patch Set prior to proceeding with Oracle Utilities Customer Care and Billing Application product installation. For detailed instructions see Preparing for the Installation.

Pre-installation Tasks

This section describes the steps that should be taken before installing Oracle Utilities Customer Care and Billing.

Installing Prerequisite Patches

Oracle Utilities Application Framework patches must be installed prior to installing Oracle Utilities Customer Care and Billing.

The patches are available as a convenience rollup inside the zip file, CCB-V2.5.0.2.0-FW-PREREQ-MultiPlatform.zip, which is part of the downloaded Media Pack.

For a list of the patches that are included in this rollup, refer to Appendix Application Framework Prerequisite Patches.

Follow these steps for installing the application and database patches on top of Oracle Utilities Application Framework 4.3.0.2.0:

1. Copy the file CCB-V25020-FW-PREREQ-MultiPlatform.jar in the delivered package to a <TEMPDIR>. Unjar using below command:

   ```
   jar -xvf CCB-V25020-FW-PREREQ-MultiPlatform.jar
   ```

2. Initialize the Framework environment that you want to install the Framework patch rollup into:

   UNIX:

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

   Windows:

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

3. Install application patches:

   3a. Navigate to the <temp location>/ FW-V4.3.0.2.0-Rollup/Application folder

   3b. Execute the group installation script:

   Unix /Linux:

   ```
   chmod a+x installSFgroup.sh
   chmod a+x FW*/*.sh
   ./installSFgroup.sh
   ```

   Windows:

   ```
   installSFgroup.cmd
   ```

Copying and Decompressing Install Media

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

Oracle Utilities Customer Care and Billing is delivered in a separate installation package for each supported Operating System. Please refer to the Supported Platforms for version and installation details regarding the database and operating system versions. Also see Chapter 5**:** Installing Application Server Prerequisite Software for prerequisite third-party software installation instructions.

Download the installation package for your operating system and proceed with the following instructions.

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 host server, which is independent of any current or other working Oracle Utilities Customer Care and Billing application environment. This can be the same <TEMPDIR> used during the installation of the Oracle Utilities Application Framework.
3. Copy the file CCB-V2.5.0.2.0-MultiPlatform.jar in the delivered package to a <TEMPDIR>. 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 CCB-V2.5.0.2.0-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://java.sun.com/products/archive/index.html

For Windows installs, 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 CCB.V2.5.0.2.0 is created. The contents of the installation directory are identical for both platforms. The directory contains the install software for the application product.

Preparing for the Installation

1. Log on as Oracle Utilities Customer Care and Billing Administrator (default cissys).
2. Initialize the Framework 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 Application

1. Change to the <TEMPDIR>/CCB.V2.5.0.2.0 Directory.
2. Set the following path:

   ```
   export PATH=<JAVA_HOME>/bin:$PATH
   ```

   Note: The above command is only applicable on a Linux platform. <JAVA_HOME> is the location where the JDK has been installed.

3. Execute the script:

   UNIX:

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

Windows:

```
install.cmd
```

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

4. Follow the messages and instructions that are produced by the install utility. Please note that some of the steps may take some time to complete.
5. If the install utility execution was not stopped due to errors and you did not interrupt the execution, you have finished the installation of the Oracle Utilities Customer Care and Billing Application product.
6. Execute the following commands:

Unix:

```
splenviron.sh -e <ENV_NAME>
configureEnv.sh
```

Type **P** and <ENTER> (you don't need to change anything)

```
splenviron.sh -e <ENV_NAME>
initialSetup.sh
```

Windows:

```
splenviron.cmd -e <ENV_NAME>
configureEnv.cmd -e <ENV_NAME>
```

Type **P** and <ENTER> (you don't need to change anything)

```
splenviron.cmd -e <ENV_NAME>
initialSetup.cmd
```

Notes.

- In case you are using demo certificates, please execute the below command before starting the environment:

```
cd $SPLEBASE/bin
perl demo_gen_cert.plx
```

- **For WebSphere environment installations:** at the end of the installation process you will be prompted whether to deploy the application into WebSphere server. If you reply **Y** the installation script will deploy the application into WebSphere using wsadmin tool. If you reply **N** you may deploy the application into WebSphere manually using WebSphere admin console, or by executing the genwasdeploy utility.

7. Start up the environment.

The final step of the installation process is the environment startup. The install utility executes the command spl.sh start (for UNIX) or spl.cmd start (for Windows) to start up the environment. You may start the environment by this command any time. Follow the messages on the screen and check the logs in $SPLSYSTEMLOGS (%SPLSYSTEMLOGS% on Windows) directory to ensure that the environment was started successfully. If the startup failed, identify the problem by reviewing the logs, and start up the environment manually while you are connected to the new environment in your online session.

Note:

- **For WebSphere environment installations:** because the WebSphere server usually runs under root user id, it needs to be restarted with the new environment variable settings after Oracle Utilities Customer Care and Billing environment installation and deployment into

WebSphere. To do this switch to root user id, setup $WAS_HOME environment variable (and the rest of environment variables as described in Chapter 5: Installing Application Server Prerequisite Software), initialize the newly installed environment by executing the command: $SPLEBASE/bin/splenviron.sh -e $SPLENVIRON and after that shutdown and startup WebSphere server using WebSphere commands, e.g. $WAS_HOME/bin/startServer.sh server1. After the initial server restart you may start the application by the environment startup/shutdown commands or through WebSphere Admin console.

Integrating Customer Modifications into This Release

In order to integrate customer modifications from previous releases into this version of the Oracle Utilities Customer Care and Billing, the customer modifications have to be re-applied to a new environment using the source code and database utilities provided with the software development kit. Please refer to the Oracle Utilities Customer Care and Billing Software Development Kit product documentation for instructions on this process.

Operating the Application

At this point your installation and custom integration process is complete.

Be sure to read the *Oracle Utilities Customer Care and Billing Server Administration Guide* for more information on further configuring and operating the Oracle Utilities Customer Care and Billing system.

Installing Service Packs and Patches

Periodically, Oracle Utilities releases a service pack of single fixes for its products. A service pack is an update to an existing release that includes solutions to known problems and other product enhancements. A service pack is not a replacement for an installation, but a pack consisting of a collection of changes and additions for it. The service pack may include changes to be applied to the application server, the database, or both. The service pack includes all files necessary for installing the collection of changes, including installation instructions.

Between services packs, Oracle Utilities releases patches to fix individual bugs. For information on installing patches, see knowledge base article ID 974985.1 on My Oracle Support.

Service packs and patches can be downloaded from My Oracle Support (https://support.oracle.com/).

Chapter 9

Installing Version 2.5.0 Service Pack 2

This section provides instructions for installing Oracle Utilities Customer Care and Billing 2.5.0 Service Pack 2. This section includes:

- Prerequisites
- Upgrading the Database
- Upgrading the Application

For fixes included in this service pack, see Appendix A: Application Framework Prerequisite Patches.

For known issues in this service pack, see the Release Notes included with this service pack.

Prerequisites

There are no prerequisites.

Upgrading the Database

For instructions on upgrading the database component, please refer to the *Oracle Utilities Customer Care and Billing Database Administrator's Guide*. This guide is included in the Oracle Utilities Customer Care and Billing V2.5.0.2.0 zip file delivered with the package.

Upgrading the Application

Note: This upgrade process is only applicable if the existing product version is 2.5.0 and 2.5.0.1.0.

For all other supported upgrade paths, please follow instructions listed in Chapter 7 and Chapter 8 of this document.

To upgrade to this service pack, you must install the following components in the order mentioned below:

- Oracle Utilities Application Framework v4.3.0.2.0
- Oracle Utilities Customer Care and Billing v2.5.0.2.0 Single Fix Prerequisites
- Oracle Utilities Customer Care and Billing v2.5.0 Service Pack 2

This section includes information on the following:

Upgrading to Oracle Utilities Application Framework v4.3.0.2.0

Ensure that the database component is successfully installed before proceeding with the steps below:

1. Create a <TEMPDIR> directory on the host server that is independent of any current or other working application environment.
2. Copy the delivered package zip file to <TEMPDIR> and unzip it. For example, the Linux copy for Framework V4.3.0.2.0 is "FW-V4.3.0.2.0-Multiplatform.zip".

   Note: If you are using FTP to transfer this file, remember to use the BINARY option for the FTP transfer.
3. Log in to the application server host server as the administrator user ID (default cissys).
4. Change directory:

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

   where <install_dir> is the location where the Oracle Utilities Customer Care and Billing application component is installed.
5. Initialize the Oracle Utilities Customer Care and Billing environment by running the appropriate command:

   UNIX:

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

   Windows:

   ```
   splenviron.cmd -e <ENV NAME>
   ```
6. If the environment is running, stop it by running the appropriate command:

   UNIX:

   ```
   ./spl.sh stop
   ```

   Windows:

```
spl.cmd stop
```

7. Ensure that you have executed splenviron.sh -e <$SPLENVIRON> prior to the installation process.

   Note: The installation utility DOES NOT create backup of installed files. You must backup <$SPLEBASE> before continuing with the rest of the installation utility.

8. Change directory to the <TEMPDIR>/FW-V4.3.0.2.0-SP2 directory and run the below script.

   UNIX:

   ```
   ./installSP.sh
   ```

   Windows:

   ```
   installSP.cmd
   ```

9. The installation utility informs that the Service Pack (v4.3.0.2.0) is about to be installed into the environment <$SPLENVIRON>.

10. The utility prompts you to press Enter to continue with the rest of the installation process of Oracle Utilities Application Framework v4.3.0 Service Pack 2 (v4.3.0.2.0).

Applying Oracle Utilities Customer Care and Billing v2.5.0.2.0 Single Fix Prerequisite

Note: The Oracle Utilities Application Framework V4.3.0.2.0 Application Server must be installed prior to installing this Single Fix Prerequisite.

You must install the corresponding database component of this Single Fix Prerequisite. See the *Oracle Utilities Customer Care and Billing Database Administrators Guide* section "Installing Prerequisite Database Single Fixes" for instructions.

To install the Oracle Utilities Customer Care and Billing v2.5.0.2.0 Single Fix Prerequisite:

1. Unzip the CCB-V2.5.0.2.0-FW-PREREQ-MultiPlatform.zip file to a temporary location <temp location>.

2. Navigate to the <temp location> and unjar the CCB-V25020-FW-PREREQ-MultiPlatform.jar using the following command:

   ```
   jar -xvf CCB-V25020-FW-PREREQ-MultiPlatform.jar
   ```

3. Navigate to the <temp location>/FW-V4.3.0.2.0-Rollup/Application folder.

4. Execute the group installation script:

   On Unix / Linux:

   ```
   chmod a+x installSFgroup.sh
   chmod a+x FW*/*.sh
   ./installSFgroup.sh
   ```

   On Windows:

   ```
   installSFgroup.cmd
   ```

Upgrading Oracle Utilities Customer Care and Billing

1. Log in to the application server host server as the administrator user ID (default cissys).

2. Change directory:

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

where <install_dir> is the location where the Oracle Utilities Application Framework application component is installed.

3. Initialize the Oracle Utilities Application Framework environment by running the appropriate command:

   UNIX:

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

   Windows:

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

4. If the environment is running, stop it by running the appropriate command:

   UNIX:

   ```
   ./spl.sh stop
   ```

   Windows:

   ```
   spl.cmd stop
   ```

5. Go to the <TEMP>/CCB.V2.5.0.2.0 folder

6. Execute the install script:

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

   UNIX:

   ```
   ./install.sh
   ```

   Windows:

   ```
   install.cmd
   ```

7. The utility displays a message that you are about to install the product Customer Care and Billing into the environment <$SPLENVIRON> located at <$SPLEBASE>.

   Note: Ensure that you have executed splenviron.sh -e <$SPLENVIRON> prior to the installation process.

8. The installation utility asks you to confirm that you want to proceed with the installation process. Enter Y.

9. The installation process begins. The utility displays a warning that the product Customer Care and Billing is already installed in the environment. You are asked to confirm whether you want to reinstall the product. Enter Y.

10. When you are done with the confirmation, proceed with the option P.

This completes the installation of Oracle Utilities Customer Care and Billing v2.5.0 Service Pack 2.

Post-Upgrade Steps

1. Log in to the application server host server as the administrator User ID (default cissys).
2. Change directory:

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

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

   UNIX:

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

   Windows:

   ```
   splenviron.cmd -e <ENV NAME>
   ```
4. Navigate to $SPLEBASE/bin.
5. Perform the post-installation steps as described below:

   UNIX:

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

   Windows:

   ```
   configureEnv.cmd
   ```

   Note: On UNIX, ensure that you have the proper execute permission on configureEnv.sh.
6. Generate the appviewer by following the steps in Generating the Application Viewer.
7. Verify and review the log files to ensure that there are no errors during the upgrade process.

Generating Demo certificates

In case you are using demo certificates, please execute the below command before starting the environment:

```
cd $SPLEBASE/bin
perl demo_gen_cert.plx
```

Forcing the Environment to Use the Current Keystore

This process does the following:

- Prompts for and encyrpts new application-stored passwords.
- Synchronizes the keystore to the database.
- Regenerates the user hashes.
- Invalidates any database-stored passwords.

Use this option when, for example, a keystore has been lost, preventing the system from decrypting the passwords stored in the configuration files or database. In such a case, all passwords will need to be reentered.

For Oracle Utilities Application Framework, perform the following steps:

- Using configureEnv.sh|cmd, re-enter the menu passwords to encrypt the data.
- Run initialSetup.sh|cmd to update property files with the encrypted data.

- Run the following command:

```
Perl   $SPLEBASE/bin/run_java_standalone.plx
com.splwg.shared.common.ResetCryptographyKey
```

Operating the Application

At this point your installation of this service pack is complete. Be sure to read the *Oracle Utilities Customer Care and Billing Server Administration Guide* for more information on further configuring and operating the system.

Chapter 10

Additional Tasks

This section describes tasks that should be completed after installing Oracle Utilities Customer Care and Billing, 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
- Deploying Inbound WebServices (IWS)
- 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/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:

```
$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 user exit instead. 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. Use the following procedure:

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 $SPLEBASE/etc/conf/root/cm and create a

new “External” Navigation Key called CM_logoImage. To do that, run the Oracle Utilities application from the browser with the parameters: http://<hostname>:<port>/cis.jsp?utilities=true&tools=true. From the Admin menu, select Navigation Key. Add the above Navigation Key with its corresponding URL Override path. The syntax for the URL path is:

Windows:

http://<host name>:<port>/<Web Context>/cm/<customer_logo_file>.png

UNIX:

http://<host name>:<port>/<Web Context>/cm/<customer_logo_file>.png

The root directory may be deployed in war file format for runtime environment (SPLApp.war). Use provided utilities to incorporate your cm directory into SPLApp.war 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 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.XAIApp.template
- spl.properties.standalone.template

3. Re-initialize the environment to propagate these changes by executing the initialSetup.sh/cmd.
4. Restart the environment.

Deploying Inbound WebServices (IWS)

All existing XAI Inbound Services have been duplicated as Inbound Web Services as the application moves toward deprecation of XAI and full transition to IWS in the next release. The duplicated services are designed to work seamlessly in this release, and customers providing custom services are encouraged to migrate to IWS to take full advantage of the new, more efficient Web service technology.

For more information on migrating from XAI to IWS, please refer to Migrating from XAI to IWS Oracle Utilities Application Framework (Doc ID 1644914.1) on My Oracle Support.

Note: This is an optional step for customers using IWS instead of XAI services.

For deploying IWS, please follow the steps below:

UNIX:

1. Enable the Web Services Functionality as shown below:
   a. cd $SPLEBASE/bin
   b. Execute configureEnv.sh –a

   Select option 50 and set the option “Enable Web Services Functionality” to true. Enter "P" to process.
2. Execute initialSetup.sh as shown below:

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

3. Set the classpath as shown below:

```
$ CLASSPATH=$WL_HOME/server/lib/weblogic.jar:$CLASSPATH
$ export CLASSPATH
$ cd $SPLEBASE/bin
```

4. Execute the following command:

```
$ java weblogic.Admin -username <username> -password <password>
STOREUSERCONFIG -userconfigfile $SPLEBASE/etc/.wlsuserconfig -
userkeyfile $SPLEBASE/etc/.wlsuserkey
```

Select y

5. Execute the below step in $SPLEBASE/bin. Please note that the application server should be up before running the below command.

```
ksh ./iwsdeploy.sh
```

WINDOWS:

1. Enable the Web Services Functionality as shown below:

```
cd %SPLEBASE%\bin
```

2. Execute configureEnv.cmd –a

Select option 50 and set the option "Enable Web Services Functionality" to true. Enter "P" to process.

3. Execute initialSetup.cmd as shown below:

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

4. Set the classpath as shown below:

```
set CLASSPATH=%WL_HOME%\server\lib\weblogic.jar;%CLASSPATH%
```

5. Execute the following command:

```
java weblogic.Admin -username system -password ouafadmin
STOREUSERCONFIG -userconfigfile %SPLEBASE%\etc\.wlsuserconfig -
userkeyfile %SPLEBASE%\etc\.wlsuserkey
```

Select y

6. Execute the below step in %SPLEBASE%\bin. Please note that the application server should be up before running the below command.

```
iwsdeploy.cmd
```

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
- 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.

You are able to create a custom domain template from the existing domain by using the Domain Template Builder or the pack command. By using the Domain Template Builder, you can also create a custom domain template from an existing template.

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 updated in production configuration with the proper values based on your configuration.

Configure setDomainEnv.sh Script

You will need to set the value of SPLEBASE with the proper value for your implementation. Under the following location, DOMAIN_HOME/bin, update the setDomainEnv.sh file and add the following

```
SPLEBASE="${SPLEBASE}"
```

Note: You will need to update ${SPLEBASE} with appropriate value based on your configuration.

Update SPLEBASE

The following update in the configuration indicates if the embedded configuration is being utilized or if the environment is a native installation to Weblogic. When this item is populated in the environment, the delivered base tools will be able to identify that the starting and stopping of the environment are being done under the domain home.

1. Initialize the Environment: splenviron.sh –e <Environment_Name>
2. Execute: configureEnv.sh –a
3. Select Menu Item: 52. Advanced Web Application Configuration

```
================================================
```

4. 02. Configuration Option: Domain Home Location

   Current Value <ENTER>:

   The Weblogic Domain Home location, when this parameter is populated you will need to use the native Weblogic tools for maintenance (starting, stopping, deployment, and undeployment).

   Enter Value: <Enter your domain home location>

5. Once the Domain Home location has been completed, Enter <P> Process

Update setDomainEnv.sh

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 splenviron script provided with the system.

UNIX:

Log on to your UNIX box as the Oracle Utilities Administrator (default cissys) and open a shell prompt.

In the following example, replace the variables

- $SPLEBASE with the Full directory name that you installed the application into
- $SPLENVIRON with the name you gave to the environment at installation time

To initialize the environment enter:

```
$SPLEBASE/bin/splenviron.sh -e $SPLENVIRON
```
For example:

```
/ouaf/DEMO/bin/splenviron.sh -e DEMO
```

Windows:

The command window should be opened on the Windows server that you installed the application on.

In the below example you should replace the following variables:

- %SPLEBASE%: The Full directory name that you installed the application into
- %SPLENVIRON%: The name you gave to the environment at installation time

To initialize the environment, type the following in your command prompt:

```
%SPLEBASE%\bin\splenviron.cmd -e %SPLENVIRON%
```
For example:

```
D:\ouaf\DEMO\bin\splenviron.cmd -e DEMO
```

2. Execute the following script to generate the jar file.

   UNIX:

   ```
   ksh $SPLEBASE/bin/createDBStandlone.sh
   ```

   Windows:

   ```
   %SPLEBASE%\bin\createDBStandlone.cmd
   ```

   Note: By default, the output jar db_patch_standalone.jar is created in SPLEBASE/tools/dbstandalone. You can use the –l option to change the default directory.

3. Transfer the generated jar (db_patch_standalone.jar) to the Windows/Unix machine where you want to run the database patching utility.
4. Extract the contents of the archive file:

   ```
   jar xvf db_patch_standalone.jar
   ```

   Note: You must have Java 7 JDK installed on the machine to use the jar command. Be sure to install the JDK that is supported for your platform.

Overview of Database Patching Application

The database patching utility requires you have Java 7 JDK installed on the machine to execute the database patch application process.

The patch application process will perform following items to account for executing patch application under SPLEBASE or on a standalone server.

The database patch application utility will look do the following when it is executed:

- Checks to see if the environment variable $SPLEBASE is set.

If the $SPLEBASE variable is set, the utility uses the libraries under $SPLEBASE to apply the patch.

- When the $SPLEBASE is not set, the utility checks to see if the TOOLSBIN environment variable is set.

If the TOOLSBIN is set, the utility uses the libraries under the TOOLSBIN location.

- When both SPLEBASE and TOOLSBIN environment are not set, the utility prompts for the location of the TOOLSBIN.

The TOOLSBIN is the location of the of the application scripts ouafDatabasePatch.sh[cmd]

Unix Example: - The TOOLSBIN location would be set to /ouaf/dbpatch/bin

```
export TOOLSBIN=/ouaf/dbpatch/bin
```

Unix Sample - Database Patch Application (ouafDatabasePatch.sh)

> **Note**: The default permissions (ouafDatabasePatch.sh), may need to be adjusted to be executed by your user and group, when applying database fixes.

- Sample Execution – Passing a Password

```
./ouafDatabasePatch.sh -x ouafadm -p "-t O -d
CISADM_Z1_12C_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

Application Framework Prerequisite Patches

Oracle Utilities Application Framework patches must be installed prior to installing Oracle Utilities Customer Care and Billing. The patches listed below are available as a convenience rollup, CCB-V2.5.0.2.0-FW-PREREQ-MultiPlatform.zip, which is included in the downloaded Media Pack. Please refer to the instructions contained inside the rollup directory for steps to install the patches. The rollup contains the following patches:

Bug Fix	Description
18091888	UIHINTS: ISSUE WITH DEPENDENT DROPDOWN INSIDE A LIST NOT BEING POPULATED
23000202	ADHOC CHAR VAL INPUT FOR CHAR PAGES DEFINED IN PRECOMMON.XSL
23229887	VIEW WSDL FOR XAI INBOUND SERVICE DEPLOYMENT IN IWS DEPLOYMENT INCORRECT FOR SOM
23240036	UNABLE TO SCROLL LEFT TO VIEW TABS ON THE LEFT
23258902	UIHINTS - SERVICE SCRIPT BUILT DROPDOWN CRITERIA NOT POPULATE
23271541	BILL SEGMENT CALC LINE UI HIDING 1ST ROW OF CALC LINES - IE11 ONLY, FF OK
23300372	SCHEMA EDITOR: MAPFIELD IS BLANKING OUT ON SCHEMA ELEMENTS
23301784	CORRECT THE ORACHART CODE TO EXPECT AMOUNT IN INTERNAL FORMAT
23304123	ERROR SENDING OUTBOUND MESSAGE.
23311455	ACCOUNT MANAGEMENT - MISSING FIELD DESCRIPTION
23495244	ISSUE WITH BS/ZONE F1-RTCHRENT WHEN LOOKUP FIELD NAME IS
23537661	ADDING THE OPTION WEB_ADMIN_SERVER NEEDED FOR WEBLOGIC NATIVE INSTALL
23571679	COLLAPSING THE DASHBOARD CAUSES A SCROLLBAR TO APPEAR