Oracle® Banking Deposits and Lines of Credit Servicing

US Localization Installation Guide - Silent Installation

Release 2.7.0.0.0

F11759-01

March 2019

ORACLE®

Oracle Banking Deposits and Lines of Credit Servicing US Localization Installation Guide - Silent Installation, Release 2.7.0.0.0

F11759-01

Contents

List of Figures

List of Tables

Preface

The Oracle Banking Deposits and Lines of Credit Servicing US Localization Installation Guide - Silent Installation contains information on silent installation and configuration of Oracle Banking Deposits and Lines of Credit Servicing software and its associated products.

This preface contains the following topics:

Audience

This guide is primarily meant as a step-by-step installation manual for IT deployment teams and onshore implementations at client locations to install a complete Oracle Banking Deposits and Lines of Credit Servicing US localization system in a UNIX based environment.

The reader is expected to have an acquaintance with UNIX platform, Oracle WebLogic server and Oracle Fusion platform firmware such as Oracle JDeveloper, Oracle OID and Oracle SOA Suite.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/us/corporate/accessibility/index.html.

Access to Oracle Support:

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/us/corporate/accessibility/support/index.html#info or visit http://www.oracle.com/us/corporate/accessibility/support/index.html#trs if you are hearing impaired.

Organization of the Guide

This document contains:

Chapter 1 Getting Started

This chapter presents an overview of Oracle Banking Deposits and Lines of Credit Servicing and the installation guide. It also mentions the assumptions, limitations and exclusions that this document has been based upon.

Chapter 2 Pre-Installation Configurations

This chapter describes the pre-configuration activities that are to be completed successfully for proper installation and functioning of Oracle Banking Deposits and Lines of Credit Servicing.

Chapter 3 OBDLOCS US Localization SOA Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Deposits and Lines of Credit Servicing SOA (Integration Server) Media pack.

Chapter 4 OBDLOCS US Localization Host Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Deposits and Lines of Credit Servicing Host Media Pack.

Chapter 5 OBDLOCS US Localization Presentation Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Deposits and Lines of Credit Servicing Presentation (UI) Media Pack.

Chapter 6 Standalone Database Setup

This chapter explains the steps involved in Oracle Banking Deposits and Lines of Credit Servicing database.

Chapter 7 OBDLOCS and IPM Integration

This chapter explains the steps involved in the integration of Oracle Banking Deposits and Lines of Credit Servicing and Oracle Imaging and Process Management (IPM).

Chapter 8 BIP Datasource Creation

This chapter explains the steps required for Business Intelligence Publisher (BIP) datasource creation.

Chapter 9 ODI Configuration

This chapter explains the steps involved in the configuration of ODI using OBDLOCS HOST Media Pack.

Chapter 10 Monitoring Servers Using Oracle Enterprise Manager

This chapter explains the steps required to monitor servers using Oracle Enterprise Manager (OEM).

Chapter 11 Post Installation Verification

This chapter explains the steps required to verify the installation of Oracle Banking Deposits and Lines of Credit Servicing.

Chapter 12 Errors and Remedies

This chapter provides information on troubleshooting to help diagnose and remedy some of the problems encountered during installation of the Oracle Banking Deposits and Lines of Credit Servicing.

Chapter 13 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Deposits and Lines of Credit Servicing.

Related Documents

For more information, see the following documentation:

- For information necessary for the installation and configuration of integration components to create a complete solution using Oracle Banking Deposits and Lines of Credit Servicing and Oracle Documaker, see the installation and configuration guides at http://docs.oracle.com/cd/E22582_01/e22582_01_index.html.
- Information on Oracle Fusion Middleware Install-Config Checklist is available at http://aseng-wiki.us.oracle.com/asengwiki/display/ASMWArchPM/FMW+Install-Config+Checklist+Page.
- For a comprehensive overview of security, see the Oracle Banking Deposits and Lines of Credit Servicing Security Guide.

- For the complete list of licensed products and the third-party licenses included with the license, see the Oracle Banking Deposits and Lines of Credit Servicing Licensing Guide.
- For information related to setting up a bank or a branch, and other operational and administrative functions, see the Oracle Banking Deposits and Lines of Credit Servicing Administrator Guide.
- For information related to customization and extension, see the Oracle Banking Deposits and Lines of Credit Servicing Extensibility Guides for SOA, HOST, and UI.
- For information on the functionality and features, see the respective Oracle Banking Deposits and Lines of Credit Servicing Functional Overview document.
- For recommendations of secure usage of extensible components, see the Oracle Banking Deposits and Lines of Credit Servicing Secure Development Guide.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

The following acronyms are used in this document:

Acronym	Meaning
ADF	Application Development Framework
ATM	Automated Teller Machine
BIP	Business Intelligence Publisher
BPEL	Business Process Execution Language
DB or db	Oracle Database
FEPI	Front End Processing Interface
HOST	Middleware Host Tier
IAM	Identity and Access Management
IPM	Imaging and Process Management
LDAP	Lightweight Directory Access Protocol
OAAM	Oracle Adaptive Access Manager
OBDLOCS	Oracle Banking Deposits and Lines of Credit Servicing

Acronym	Meaning
ODI	Oracle Data Integrator
OEL	Oracle Enterprise Linux
OEM	Oracle Enterprise Manager
OID	Oracle Internet Directory
OIM	Oracle Identity Manager
OLTP	Online Transaction Processing
OPSS	Oracle Platform Security Services
OS	Operating System
POS	Point Of Sale
RCU	Repository Creation Utility
sh	Unix Shell file
SOA	Service Oriented Architecture Tier
SVN	Source Code Version Repository
UI	User Interface, that is Presentation Tier
VM	Virtual Machine
WLS	WebLogic Server

1 Getting Started

This chapter presents an overview of Oracle Banking Deposits and Lines of Credit Servicing and the installation guide. It also mentions the assumptions, limitations and exclusions that this document has been based upon.

1.1 About Oracle Banking Deposits and Lines of Credit Servicing

Transaction Accounts constitutes a crucial segment in banking business. Servicing transaction account customers is critical and depends on the target customer segment and geography. Oracle Banking Deposits and Lines of Credit Servicing supports the servicing of the following three significant segments in a bank's business offering - namely, Current and Savings Account, Term Deposits, and Retail and SME Lines of Credit.

1.2 About This Document

This document guides you through the installation of the core banking application Oracle Banking Deposits and Lines of Credit Servicing along with localization. This document guides in deploying the following parts of the application:

- Presentation Server (ADF Presentation UI deployment on WebLogic)
- Application Server (Banking Services hosted on WebLogic)
- Integration Server (Oracle Banking Deposits and Lines of Credit Servicing Integration and Approval Processes hosted on Oracle SOA)
- Security Configuration (Seeding security to OID)
- Seed Data Configuration (Seeding data to Core banking OLTP Database Server)

There are multiple prerequisites that need to be done before the start of the installation. The prerequisites section lists down the requirements. This document does not attempt to guide you through the prerequisites installation. The readers are expected to see the appropriate platform documentation to install the prerequisites.

This document prescribes bare minimum hardware requirements to have a functional application configuration. The sizing for a production environment is not prescribed here.

Due care has been taken to make this document as complete as possible. In case of any anomalies please mail to obp-deployment-support@oracle.com.

There are certain steps in the installation that *may* not be optimal yet. Further releases will optimize the deployment further.

1.3 Assumptions

It is assumed that the reader is aware of the technologies involved and is capable of installing the prerequisite software products mentioned in Section 2.1.2 Software Environment.

The following are the assumptions regarding the environment and setup with regard to carrying out this installation:

- The Oracle Banking Deposits and Lines of Credit Servicing US localization installables are downloaded and copied onto a Linux machine or Linux VM.
- The reader has taken a remote connection to the Linux machine via Windows box.
- The reader is able to take an 'ssh' connection to the servers on which various OBDLOCS components have to be installed from the Linux machine.
- The user is aware of the process of creating required db schema using RCU prior to initiation of OBDLOCS US localization installation.

1.4 Limitations

Whenever the installation gets aborted or is served a timeout for various reasons, rerun the installation from the beginning with domain cleanup.

1.5 Exclusions

Though some of the software and products listed in prerequisites section may work on Windows, such qualification has not been carried out and shall not be the focus of this guide. It is advisable to use the mentioned Operating System (OS) for the best experience.

2 Pre-Installation Configurations

This chapter describes the pre-configuration activities that are to be completed successfully for proper installation and functioning of Oracle Banking Deposits and Lines of Credit Servicing.

2.1 Setup Prerequisites

This section lists down the requirements from an environment perspective including minimum hardware requirements with Operating System (OS) and the middleware software products, which the Oracle Banking Deposits and Lines of Credit Servicing solution depends and runs on (for example, Database or WebLogic) or interfaces with (for example, OID or IPM).

2.1.1 Hardware Environment

The minimum hardware requirements for Oracle Banking Deposits and Lines of Credit Servicing solution to install and function decently are listed below:

Table 2–1 Hardware and OS

Sr. No.	CPU (2+GHz)	RAM (GB)	Disk (GB)	OS Version	Purpose
1	4	16	200	OEL 6.8 or OEL 7.1 64 bit	Oracle Banking Deposits and Lines of Credit Servicing Oracle Database
2	4	32	200	OEL 6.8 or OEL 7.1 64 bit	Oracle Banking Deposits and Lines of Credit Servicing ADF UI Presentation Server
3	4	32	200	OEL 6.8 or OEL 7.1 64 bit	Oracle Banking Deposits and Lines of Credit Servicing Services Middleware Host Server
4	2	16	200	As per OID certification matrix.	Oracle OID Server
5	2	16	200	As per IPM certification matrix.	Oracle IPM Server
6	2	16	200	As per BIP certification matrix.	Oracle BIP Server
7	4	32	200	As per SOA certification matrix.	Oracle SOA Server
8	4	16	200	As per BAM certification matrix.	Oracle BAM Server

2.1.2 Software Environment

It is assumed that the following products are installed and are available on the server on which the Oracle Banking Deposits and Lines of Credit Servicing installation will be performed.

2.1.2.1 Certification Details

The following software are mandatory:

Table 2–2 List of Software

Sr. No.	Components	Zone	Software
1	OBDLOCS UI Presentation	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
2	SOA	Banking App	Oracle SOA Suite 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
3	OBDLOCS HOST	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
4	OID	Security	Oracle Internet Directory 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
5	BIP	Document	Oracle Business Intelligence 12c (12.2.1.3.0) Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
6	IPM	Document	Oracle WebCenter - Content 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
7	OSB	Integration	Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Oracle Service Bus 12c (12.2.1.3.0). Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
8	ODI	Integration	Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Oracle Data Integrator 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
9	OIM	Security	Oracle Identity Manager 12.2.1.3.0

Sr. No.	Components	Zone	Software
			Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
10	OAAM	Security	Oracle IAM 11.1.2.3 Suite Oracle Weblogic Server 10.3.6 Java Version jdk1.7.0_xx Oracle Linux 6.8 64-bit or Oracle Linux 7.0 64-bit
11	OAM	Security	Oracle Access Manager 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 6.8 / 7.1 64-bit
12	OEM	Management	Oracle Enterprise Manager 13.2.0.0.0 As per certification matrix of Oracle Enterprise Manager 13.2.0.0.0
13	EM Agent Installation	Management	Push from OEM Console
14	OBDLOCS Database	Database	Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 Oracle Linux 6.8 / 7.1 64-bit
15	HTTP Server	Web Server	Oracle HTTP Server 12.2.1.3.0.
16	BAM	Banking App	Oracle SOA Suite and Business Process Management 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172)

The following are some notes related to the software.

Table 2–3 Notes

Serial Number	Description
1	OBDLOCS release has been certified with OEL version 6.8 and above (7.1) during the release cycle. It is strongly recommended to use the versions on which the release is certified.
2	Oracle Business Intelligence Publisher is required at the time of OBDLOCS installation. It is required to use the actual BIP property values during the installation. This is required as the installer uploads the OBDLOCS reports as onto the BIP server as part of the middleware host installation process.
3	ODI_OUTBOUND_USERNAME and ODI_OUTBOUND_PASSWORD The OBDLOCS installer will not abort the installation if this component is not present. It can be installed later. However, it is strongly recommended to use the actual property values instead of default property values during the installation. Else, the actual values for ODI_OUTBOUND_USERNAME and ODI_OUTBOUND_

Serial Number	Description
	PASSWORD once available have to be manually updated in the 'ra/FCRJConnectorODI' jndi property of com.ofss.fc.app.connector.ear application inside middleware host server after the entire installation completes.
4	The OBDLOCS installer will not abort the installation if this component is not present. It can be installed later. It is strongly recommended to use the actual property values instead of default property values during the installation. Else, these properties have to be manually updated in Host Database after the entire installation completes.
5	OIM_OUTBOUND_USERNAME and OIM_OUTBOUND_PASSWORD The OBDLOCS installer will not abort the installation if this component is not present. It can be installed later. It is recommended to use the actual property values instead of default property values during the installation. Else, these properties have to be manually updated in Host Database. Also, actual values for OIM_OUTBOUND_USERNAME and OIM_OUTBOUND_PASSWORD once available have to be manually updated in the 'ra/FCRJConnectorOIM' jndi property of com.ofss.fc.app.connector.ear application inside middleware host server after the entire installation completes.
6	Oracle Access Manager can be installed later.
7	During installation, password of unix user will be asked multiple times for "scp" "ssh". There is a time limit for entering password. If not entered within specified limit, the installation is likely to exit. User should take care of this.
8	It is mandatory for machine nodes on which OBDLOCS UI, Host, and SOA Media pack installation is planned, to install the Java Cryptography Extensions Unlimited Strength Jurisdiction Policy Files, to enable additional encryption strengths.
9	Download the jce_policy.zip from Oracle website for the current Java version being used. For jdk1.8.0_xx, download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 jce_policy-8.zip from the following link: http://www.oracle.com/technetwork/java/javase/downloads/jce-all-download-5170447.html Copy "local_policy.jar" and "US_export_policy.jar" from this zip file in the path mentioned below: JAVA_HOME/jre/lib/security/
10	It is mandatory that the team installing OBDLOCS reads and understands the system requirements and specifications for the fusion middleware specified in the following link: https://docs.oracle.com/html/E82037_01/toc.htm The url details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.3.0) products. Changes necessary at a system level for the fusion middleware should be made prior to executing OBDLOCS media packs. For example, the number of open files should be increased from the default value as specified in the following link: https://docs.oracle.com/html/E82037_01/toc.htm#GUID-95BCDEF2-F2FC-4E30-A8EF-B966F817B1D4
11	SOA managed servers may need the default value raised at operating system level to run, as it needs to load a large number of OBDLOCS application binaries.

Serial Number	Description
12	The value of property SOA_SERVER_NAME in installer properties should not be changed. The default value of soa_server1, that is shipped along with media pack, should be retained AS IS. Managed servers, that are required inside the cluster as per the naming onsite conventions, should be added after the media pack installation is complete.
13	Oracle SOA Suite 12.2.1.3.0 patch - p27651368_122130_Generic.zip has to be applied on SOA machine only. This can be downloaded from the following link: http://aru.us.oracle.com:8080/ARU/ViewPatchRequest/process_form?aru=22513715

2.1.2.2 Optional

The following software is optional:

- Oracle VM server release 2.2.0

2.1.2.3 Patching

OPatch is a patching utility in OBDLOCS Installer. The following is required to run OPatch.

The Python packages need to be installed in the same order as mentioned below. They have to be installed as root user in UI, Host, and SOA Machines.

- Suds-0.4 (to create webservice client)
- docutils-0.12 (prerequisite for SOAPpy)
- wstools-0.4.3 (prerequisite for SOAPpy)
- SOAPpy0.12.5 (to make SOAP webservice call)
- PyYAML-3.11 (to read yaml file)
- Jypye1-0.5.7 (to call java code from Python)

The above mentioned packages are available in the form of .tar.gz files in the media pack.

The installation steps are as follows:

1. Extract each file so that the above Python packages get installed in the same order.
2. Run setup.py file inside extracted folder. (command:python install).

   tar -xvzf suds-0.4.tar.gz

   tar -xvzf docutils-0.12.tar.gz

   tar -xvzf wstools-0.4.3.tar.gz

   tar -xvzf SOAPpy-0.12.5.tar.gz

   tar -xvzf PyYAML-3.11.tar.gz

   tar -xvzf JPype1-0.5.7.tar.gz

   chmod -R 777 *

   cd suds-0.4

   python setup.py install

```
cd ../docutils-0.12
python setup.py install
cd ../wstools-0.4.3
python setup.py install
cd ../SOAPpy-0.12.5
python setup.py install
cd ../PyYAML-3.11
python setup.py install
cd ../JPype1-0.5.7
python setup.py install
```

Please note that the above step is only required to run OPatch (a patching utility available with OBP Installer).

2.2 Configure Variables

Perform the following steps to configure the variables:

1. Modify the TargetDefinition.yaml located at the location <installDir>/patching/config.
2. The IP and port of the target should be of Admin Server and the destination location is the path where the zip will be extracted which is the patch Stage Path.
3. Modify the PatchConfig.yaml located at the location <installDir>/patching/config.
4. The Session context details such as Bank Code, Channel, TargetUnit, Transaction Branch, UserId has to be entered.

   The wsdl details will be as follows:

   ${Protocol}://${hostadmin_ip}:${hostadmin_port}/${path_to_ TransactionBlackoutApplicationServiceSpi}?wsdl

   For example, url: http://<Ip>:<Port>/com.ofss.fc.webservice/services/sms/TransactionBlackoutApplicationServiceSpi ?wsdl

5. Modify the PatchConstants.py located at the location <installDir>patching/constants.
   a. The PATCH_HOME should point to the Patching Utility.
   b. The Deployables Path should point to obp.
   c. The FMW_HOME should point to the path till fmw.
   d. The WLST_SCRIPT_LOCATION should point to the wlst.sh (weblogic scripting tool).
   e. The JVM_PATH should point to the libjvm.so.
   f. The PATCH_TEMP_LOCATION should be the path where the zips are to be stored.
   g. The FCServerWithPort is '${protocol}://${hostmanagedserver_ip}:${hostManagedServer_port}'.

h. The SOAServerWithPort is '${protocol}://${uimanagedserver _ip}:${ uiManagedServer _port}'.

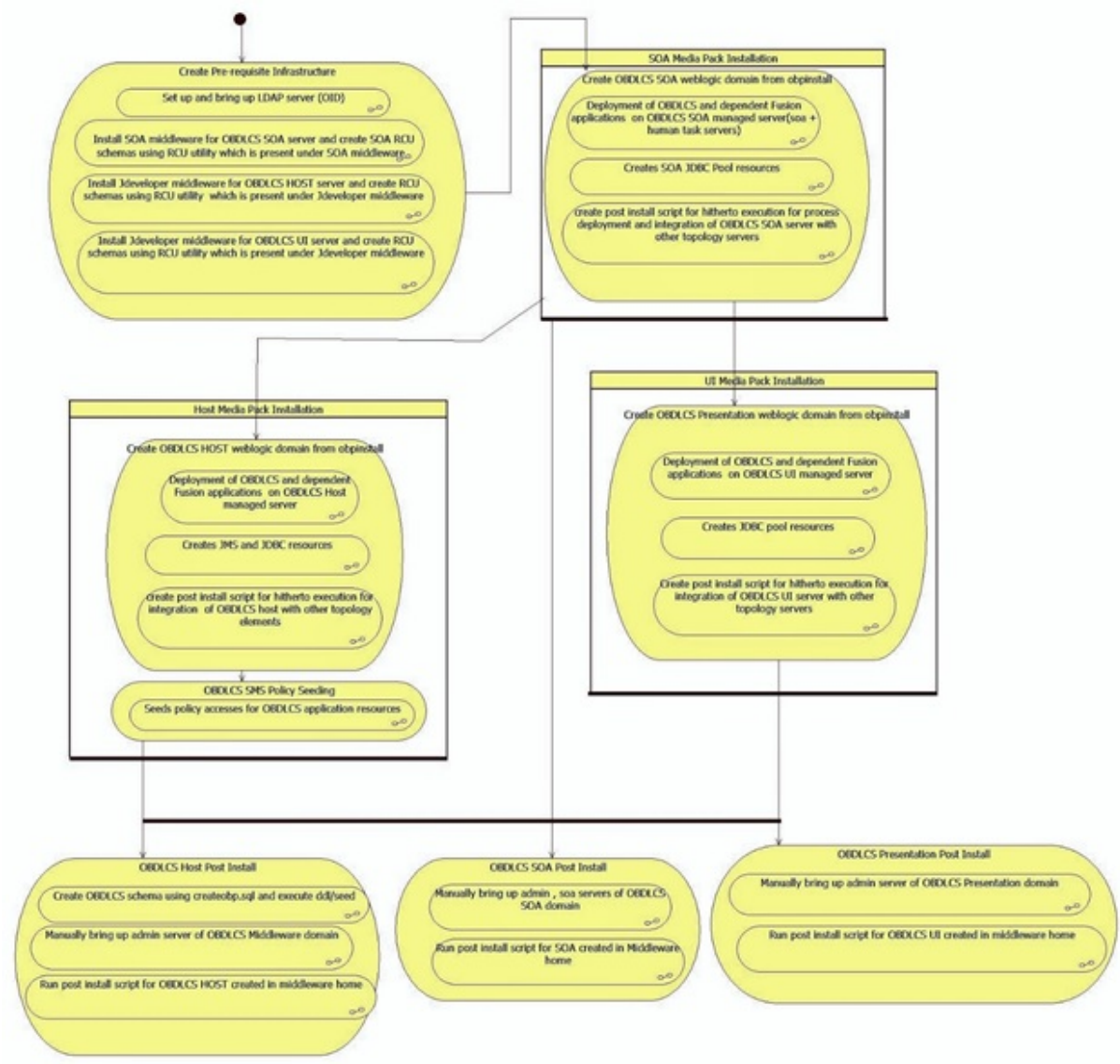
i. The CENTRAL_PATCH_STAGE_PATH should point to the central patch Staging path.

6. Create folder patchStage and centralPatchStage in location <installDir>/.

2.3 Installation Process Overview

The following diagram provides an overview of the steps that need to be followed to install and configure Oracle Banking Deposits and Lines of Credit Servicing:

Figure 2–1 Installation Overview



2.4 Installation Checklist

It is mandatory that the team installing OBDLOCS US Localization reads and understands the system requirements and specifications for the fusion middleware specified in the following link:

https://docs.oracle.com/html/E82037_01/toc.htm

The link details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.3.0) products.

Changes necessary at a system level for the fusion middleware should be made prior to executing OBDLOCS US Localization media packs.

For example, the number of open files should be increased from the default value as specified in the following link:

https://docs.oracle.com/html/E82037_01/toc.htm#GUID-95BCDEF2-F2FC-4E30-A8EF-B966F817B1D4

To make the installation experience quick and easy, a checklist of information is provided, which should be filled and kept handy. The checklist has been made more intuitive and relevant by ensuring that the Key for properties defined in the installation property file is same as the Name column in the first table of the checklist.

2.4.1 XD Components

The following table provides a list of XD components.

Table 2–4 XD Components

Sr. No.	Name	Value	Description
1	XD_COMPONENT_NAME	batchhost	Value for batch host sever, Policy seeding and BIP reports upload will be done with this batch host server installation
2	XD_COMPONENT_NAME	obepmhost	Value for obepm server (Product Manufacturing)
3	XD_COMPONENT_NAME	obcsdshost	Value for obcsds server (Deposits)
4	XD_COMPONENT_NAME	obpmhost	Value for obpm server (Party)
5	XD_COMPONENT_NAME	obeprhost	Value for obpr server (Pricing)
6	XD_COMPONENT_NAME	obccmhost	Value for obccm server (LCM)
7	XD_COMPONENT_NAME	obpui	Value for obcsds UI server
8	XD_COMPONENT_NAME	obpsoa	Value for obcsds SOA

2.4.2 Updating installobp***.properties

The following checklist provides values for updating installobp***.properties.

Table 2–5 Values for updating installobp.properties***

Sr. No	Name	Description	Example Value	Value
1	SILENT_INSTALL	Flag for installing silent or interactive mode	y	
2	IPM_INSTALLED	Flag to make sure IPM is installed	y	
3	BIP_INSTALLED	Flag to make sure BIP is installed	y	
4	OID_FARM_AND_POLICY_SEEDING_FLAG	Flag for policy seeding	Y	This value must be 'Y' for batch host installation and for other XD host installation value must be 'N'
5	BIP_REPORTS_UPLOADING_FLAG	Flag for BIP reports uploading	Y	This value must be 'Y' for batch host installation and for other XD host installation value must be 'N'
6	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
7	SECURITY_ENABLED	Flag for security enable	Y	
8	XD_COMPONENT_NAME	Flag for XD Component name	batchhost	Refer XD components table

Sr. No	Name	Description	Example Value	Value
				above
9	LOCAL_IP	I/P of the local machine which could be a windows machine on which software like XManager is installed for rendering UI of a utility executing on a remote Linux server.	10.180.84.110	
10	LOCAL_ DISPLAY_VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0.0	
11	DOMAIN_NAME	Weblogic Domain name	host_domain or ui_domain or base_domain	
12	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_ NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
13	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
14	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
15	ADMIN_ SERVER_ LISTEN_ ADDRESS	Admin server listen address	10.180.84.110 (Always use ip , do not use localhost)	
16	ADMIN_ SERVER_ LISTEN_PORT	Admin server listen port	7001	
17	ADMIN_ SERVER_SSL_ LISTEN_PORT	Admin server SSL listen port	7002	
18	MANAGED_ SERVER_ LISTEN_ ADDRESS	Managed server listen address	10.180.84.110	
19	MANAGED_ SERVER_	Managed server listen port	8001	

Sr. No	Name	Description	Example Value	Value
	LISTEN_PORT			
20	MANAGED_ SERVER_SSL_ LISTEN_PORT	SSL listen port for managed server	8002	
21	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
22	OID_IP	I/P address of the OID server.	10.180.84.113	
23	OID_PORT	Port of the OID process instance.	389	
24	OID_ADMIN_ USER	Admin user id which can be used to login of the OID as administrator.	cn= orcladmin	
25	OID_ADMIN_ PWD	Refers to the password of admin user of the OID	welcome1	
26	OID_GROUP_ DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
27	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	ou=obp,cn=Users,dc=in,dc=oracle,dc=com	
28	NODE_MGR_ PORT	Refers to the port number to be used for the weblogic node manager. This port should either be free on the UI Presentation server or an existing weblogic node manager should be installed to listen on this port when the same is started.	5556	

Sr. No	Name	Description	Example Value	Value
29	HOST_ CLUSTER_NAME	Refers to HOST cluster name	obphost_cluster1	
30	HOST_SERVER_ NAME	Refers to HOST server name	obphost_server1	
31	HOST_JAVA_ HOME	Refers to the home directory of java installation of the host machine.	/scratch/app/product/jdk1.8.0_172	
32	OUI_JAVA_HOME	Refers to the home directory of java installation.	/scratch/app/product/jdk1.8.0_172	
33	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
34	HOST_IP	I/P address of the server on which the OBDLOCS host or middleware layer should be installed.	10.180.84.110 (Always use ip , do not use localhost)	
35	HOST_TARGET	Refers to a location on the Host server where the installable can be transferred. The user id used for installation of OBDLOCS should have read, write and execute privileges on this directory.	/scratch/install/target	
36	HOST_MW_ HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
37	UI_ADMIN_ SERVER_ LISTEN_	Listen address of UI Admin server	10.180.84.111	

Sr. No	Name	Description	Example Value	Value
	ADDRESS			
38	UI_ADMIN_ SERVER_ LISTEN_PORT	Listen port of UI Admin server	7001	
39	UI_MANAGED_ SERVER_ LISTEN_ ADDRESS	Listen address of UI managed server	10.180.84.111	
40	UI_MANAGED_ SERVER_ LISTEN_PORT	Listen port of UI managed server	8001	
41	UI_MANAGED_ SERVER_SSL_ LISTEN_PORT	Listen ssl port of UI managed server	8002	
42	SOA_ORACLE_ HOME	Name of Oracle SOA which is present in fusion middleware.	soa	
43	SOA_IP	i/p address of SOA machine	10.180.84.112	
44	SOA_UNIX_USER	Unix username of SOA machine	ofssobp	
45	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
46	SOA_DOMAIN_ NAME	Refers to the middleware home of the weblogic installation on the SOA server.	base_domain	
47	SOA_MANAGED_ SERVER_ LISTEN_ ADDRESS	Listen address of SOA server	10.180.84.112	
48	SOA_ADMIN_ SERVER_ LISTEN_PORT	Listen port of SOA Admin server	7001	
49	SOA_MANAGED_ SERVER_ LISTEN_PORT	Listen port of SOA server	8001	
50	SOA_	Username of the	weblogic	

Sr. No	Name	Description	Example Value	Value
	WEBLOGIC_ USERNAME	server of SOA domain		
51	SOA_ WEBLOGIC_ PASSWORD	Password of the server of SOA domain	weblogic1	
52	UI_IP	I/P address of the server on which the OBDLOCS presentation or UI layer should be installed.	10.180.84.111	
53	UI_UNIX_USER	Linux login user id used to install the OBDLOCS UI solution.	ofssobp	
54	UI_DOMAIN_ HOME	Refers to the domain name to be used for the weblogic domain of the OBDLOCS Presentation server	/scratch/app/ product /fmw/user_projects /domains /ui_domain	
55	INSTALL_AS	Linux login user id used to install the OBDLOCS solution.	ofssobp	
56	BIP_SERVER_IP	I/P of the BIP server to host OBDLOCS reports	10.180.84.115	
57	BIP_SERVER_ PORT	Port of the BIP server that hosts OBDLOCS reports	9502	
58	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
59	BIP_MW_HOME	Oracle BIP Middleware directory on BIP server	/scratch/app/product/fmw	
60	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
61	BIP_INSTANCE_ PATH	Oracle BIP Instance	/scratch/app/product/fmw/user_ projects/domains/bi_domain/bidata/service_	

Sr. No	Name	Description	Example Value	Value
		directory on BIP server	instances/ssi/metadata/content/catalog/root/users/weblogic	
62	BIP_SERVER_USER	Oracle BIP server user id	weblogic	
63	BIP_SERVER_PSWD	Oracle BIP server user password	weblogic1	
64	BIP_REPORT_BASE_PATH	Logical Base Path on Oracle BIP server under which OBDLOCS reports would be hosted	OBDLOCS27/R27INSTALLER	
65	BIP_DATASOURCE_NAME	OBDLOCS Host database user used by OBDLOCS report to fetch data for reports	OBDLOCS27	
66	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
67	IPM_SERVER_IP	IP of Oracle Image and Processing Server for OBDLOCS Content Management	10.180.84.114	
68	IPM_SERVER_PORT	Port of Oracle Image and Processing Server for OBDLOCS Content Management	16000	
69	IPM_MW_HOME	Oracle Middleware Home directory on IPM server	/scratch/app/product/fmw	
70	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/wccontent	
71	OBP_HOST_DB_USER	OBDLOCS Host database user	OBDLOCS27	

Sr. No	Name	Description	Example Value	Value
72	OBP_HOST_DB_PASSWORD	OBDLOCS Host database password	welcome1	
73	OBP_HOST_DB_IP	OBDLOCS Host database i/p address	10.180.84.113	
74	OBP_HOST_DB_PORT	OBDLOCS Host database port	1521	
75	OBP_HOST_DB_SERVICE_NAME	OBDLOCS Host database service name	P84113A	
76	ONS_NODE	i/p address of ONS service	10.180.84.113	
77	ONS_PORT	Listen port of ONS service	6250	
78	OPSS_HOST_SCHEMA_USER	OPSS Host schema user	PRDHOST_OPSS	
79	OPSS_HOST_SCHEMA_PASSWORD	OPSS Host schema password	welcome1	
80	OPSS_HOST_DB_IP	OPSS Host DB IP	10.180.84.113	
81	OPSS_HOST_DB_PORT	OPSS Host DB Port	1521	
82	OPSS_HOST_DB_SERVICE_NAME	OPSS Host database service name	P84113A	
83	LOCAL_DATASOURCE	STB datasource schema name	PRDHOST_STB	
84	WLS_RUNTIME_SCHEMA_USER	WLS RNTIME datasource schema name	PRDHOST_WLS_RUNTIME	
85	MDS_HOST_DB_USER	MDS data source schema user name	PRDHOST _MDS	
86	MDS_HOST_DB_PASSWORD	MDS schema Password	welcome1	
87	MDS_HOST_DB_IP	MDS DB IP	10.180.84.113	
88	MDS_HOST_DB_PORT	MDS db port	1521	
89	MDS_HOST_DB_	MDS db service	P84113A	

Sr. No	Name	Description	Example Value	Value
	SERVICE_NAME	name		
90	OPSS_SOA_ SCHEMA_USER	SOA OPSS schema name	SOA27_OPSS	
91	OPSS_SOA_ AUDIT_DBDS	SOA OPSS Audit schema name	SOA27_IAU_APPEND	
92	OPSS_SOA_ AUDIT_VIEWDS	SOA OPSS Audit View schema name	SOA27_IAU_VIEWER	
93	OPSS_SOA_ SCHEMA_ PASSWORD	Password of SOA OPSS schema name	welcome1	
94	OPSS_SOA_DB_ IP	IP address of SOA OPSS DB machine	10.180.84.113	
95	OPSS_SOA_DB_ PORT	Port of SOA OPSS DB	1521	
96	OPSS_SOA_DB_ SERVICE_NAME	Service name of SOA OPSS DB	P84113A	
97	HOST_ADMIN_ JVM_PARAMS	Host domain admin JVM startup parameters	-Xms1024m -Xmx4096m	
98	HOST_ MANAGED_JVM_ PARAMS	Host domain managed JVM startup parameters	-Xms8g -Xmx8g -XX:NewSize=2048m -XX:MaxNewSize=4096m -XX:+UseParNewGC -XX: +CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75	
99	KEYSTORE_ PASSWORD	Password for generating certificate	welcome1	
100	IPM_ OUTBOUND_ USERNAME	IPM Username created in connector	weblogic	
101	IPM_ OUTBOUND_ PASSWORD	Password for the IPM user in connector	weblogic1	
102	BIP_OUTBOUND_ USERNAME	BIP Username created in connector	weblogic	
103	BIP_OUTBOUND_	Password for	weblogic1	

Sr. No	Name	Description	Example Value	Value
	PASSWORD	the BIP user in connector		
104	ODI_ OUTBOUND_ USERNAME	ODI Username created in connector	weblogic	
105	ODI_ OUTBOUND_ PASSWORD	Password for the ODI user in connector	weblogic1	
106	OIM_ OUTBOUND_ USERNAME	OIM Username created in connector	weblogic	
107	OIM_ OUTBOUND_ PASSWORD	Password for the OIM user in connector	weblogic1	
108	WCM_ OUTBOUND_ USERNAME	WCM Username created in connector	weblogic	
109	WCM_ OUTBOUND_ PASSWORD	Password for the WCM user in connector	weblogic1	
110	OFFLINE_ CHANNEL_ OUTBOUND_ USERNAME	Offline Username created in connector	offlineuser	
111	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password for the Offline user in connector	welcome1	
112	SAML_ISSUER_ OUTBOUND_ USERNAME	SAML ISSUER Username created in connector	weblogic	
113	SAML_ISSUER_ OUTBOUND_ PASSWORD	Password for the SAML ISSUER user in connector	weblogic1	
114	BPEL_ ENCRYPTION_ OUTBOUND_ USERNAME	BPEL_ ENCRYPTION Username created in connector	weblogic	
115	BPEL_ ENCRYPTION_ OUTBOUND_ PASSWORD	Password for the BPEL_ ENCRYPTION user in	weblogic1	

Sr. No	Name	Description	Example Value	Value
		connector		
116	FTP_IPM_ OUTBOUND_ USERNAME	FTP IPM Username created in connector	weblogic	
117	FTP_IPM_ OUTBOUND_ PASSWORD	Password for the FTP IPM user in connector	weblogic1	
118	FTP_BIP_ OUTBOUND_ USERNAME	FTP BIP Username created in connector	weblogic	
119	FTP_BIP_ OUTBOUND_ PASSWORD	Password for the FTP BIP user in connector	weblogic1	
120	BIP_USR_ OUTBOUND_ USERNAME	BIP Username created in connector	weblogic	
121	BIP_USR_ OUTBOUND_ PASSWORD	Password for the BIP user in connector	weblogic1	
122	SOA_PURGING_ OUTBOUND_ USERNAME	SOA Username created in connector	weblogic	
123	SOA_PURGING_ OUTBOUND_ PASSWORD	Password for the SOA user in connector	weblogic1	
124	SOA_ OUTBOUND_ USERNAME	SOA Username created in connector	weblogic	
125	SOA_ OUTBOUND_ PASSWORD	Password for the SOA user in connector	weblogic1	
126	ATMUSER_ OUTBOUND_ USERNAME	ATM Username created in connector	ATMUser	
127	ATMUSER_ OUTBOUND_ PASSWORD	Password for the ATM user in connector	welcome1	
128	POSUSER_ OUTBOUND_ USERNAME	POS Username created in connector	POSUser	

Sr. No	Name	Description	Example Value	Value
129	POSUSER_ OUTBOUND_ PASSWORD	Password for the POS user in connector	welcome1	
130	DMSHOST_ OUTBOUND_ USERNAME	DMS HOST Username created in connector	weblogic	
131	DMSHOST_ OUTBOUND_ PASSWORD	Password for the DMS HOST user in connector	weblogic1	
132	DMSUI_ OUTBOUND_ USERNAME	DMS UI Username created in connector	weblogic	
133	DMSUI_ OUTBOUND_ PASSWORD	Password for the DMS UI user in connector	weblogic1	
134	OCH_ OUTBOUND_ USERNAME	OCH Username created in connector	weblogic	
135	OCH_ OUTBOUND_ PASSWORD	Password for the OCH user in connector	weblogic1	
136	WS_MFT_ OUTBOUND_ USERNAME	WS_MFT Username created in connector	weblogic	
137	WS_MFT_ OUTBOUND_ PASSWORD	Password for the WS_MFT user in connector	weblogic1	
138	OP_OUTBOUND_ USERNAME	OP Username created in connector	weblogic	
139	OP_OUTBOUND_ PASSWORD	Password for the OP user in connector	weblogic1	
140	ICS_ OUTBOUND_ USERNAME	Username for ICS connector	weblogic	
141	ICS_ OUTBOUND_ PASSWORD	Password for ICS connector	Weblogic1	
142	OBDX_	Username for	1518675030085dean.white@test.com	

Sr. No	Name	Description	Example Value	Value
	OUTBOUND_ USERNAME	OBDX connector		
143	OBDX_ OUTBOUND_ PASSWORD	Password for OBDX connector	Welcome@1	
144	EDN_ OUTBOUND_ USERNAME	Username for EDN connector	weblogic	
145	EDN_ OUTBOUND_ PASSWORD	Password for EDN Connector	weblogic1	
146	COMMON_ OUTBOUND_ USERNAME	Username for COMMON connector	weblogic	
147	COMMON_ OUTBOUND_ PASSWORD	Password for COMMON Connector	weblogic1	
148	PM_OUTBOUND_ USERNAME	Username for PM connector	weblogic	
149	PM_OUTBOUND_ PASSWORD	Password for PM Connector	weblogic1	
150	LENDING_ OUTBOUND_ USERNAME	Username for LENDING connector	weblogic	
151	LENDING_ OUTBOUND_ PASSWORD	Password for LENDING Connector	weblogic1	
152	DEPOSITS_ OUTBOUND_ USERNAME	Username for DEPOSITS connector	weblogic	
153	DEPOSITS_ OUTBOUND_ PASSWORD	Password for DEPOSITS Connector	weblogic1	
154	FW_OUTBOUND_ USERNAME	Username for FW connector	weblogic	
155	FW_OUTBOUND_ PASSWORD	Password for FW Connector	weblogic1	
156	COLLECTION_ OUTBOUND_ USERNAME	Username for COLLECTION connector	weblogic	
157	COLLECTION_ OUTBOUND_ PASSWORD	Password for COLLECTION Connector	weblogic1	

Sr. No	Name	Description	Example Value	Value
158	OR_OUTBOUND_USERNAME	Username for OR connector	weblogic	
159	OR_OUTBOUND_PASSWORD	Password for OR Connector	weblogic1	
160	PARTY_OUTBOUND_USERNAME	Username for PARTY connector	weblogic	
161	PARTY_OUTBOUND_PASSWORD	Password for PARTY Connector	weblogic1	
162	PRODPROC_OUTBOUND_USERNAME	Username for PRODPROC connector	weblogic	
163	PRODPROC_OUTBOUND_PASSWORD	Password for PRODPROC Connector	weblogic1	
164	RECOVERY_OUTBOUND_USERNAME	Username for RECOVERY connector	weblogic	
165	RECOVERY_OUTBOUND_PASSWORD	Password for RECOVERY Connector	weblogic1	
166	PRICING_OUTBOUND_USERNAME	Username for PRICING connector	weblogic	
167	PRICING_OUTBOUND_PASSWORD	Password for PRICING Connector	weblogic1	
168	LCM_OUTBOUND_USERNAME	Username for LCM connector	weblogic	
169	LCM_OUTBOUND_PASSWORD	Password for LCM Connector	weblogic1	
170	MDM_OUTBOUND_USERNAME	Username for MDM connector	weblogic	
171	MDM_OUTBOUND_PASSWORD	Password for MDM Connector	weblogic1	
172	COMMUNICATIONS_OUTBOUND_USERNAME	Username for COMMUNICATIONS connector	weblogic	

Sr. No	Name	Description	Example Value	Value
173	COMMUNICATIONS_OUTBOUND_PASSWORD	Password for COMMUNICATIONS Connector	weblogic1	
174	APPCAPTURE_OUTBOUND_USERNAME	Username for APPCAPTURE connector	weblogic l	
175	APPCAPTURE_OUTBOUND_PASSWORD	Password for APPCAPTURE Connector	weblogic1	
176	CARD_USERNAME	Username of Card connector	weblogic1	
177	CARD_PASSWORD	Password of Card connector	welcome1	
178	RULE_USERNAME	Username of Rule connector	orakey	
179	RULE_PASSWORD	Password of Rule connector	welcome1	
180	BAM_USERNAME	Username of BAM connector	weblogic	
181	BAM_PASSWORD	Password of BAM connector	weblogic1	
182	USER_TIMEZONE	Time zone entry	+5:30	
183	HOST_SSL_PASSWORD	Password for configuring SSL in HOST domain	welcome1	
184	SILENT_INSTALL	Flag for executing installer remotely	y	
185	SECURITY_ENABLED	Flag for security enable	Y	
186	IPM_INSTALLED	Flag for if IPM is installed	Y	
187	BIP_INSTALLED	Flag for if BIP is installed	Y	
188	LOCAL_IP	I/P address of the local machine which could be a windows machine on	10.180.84.111	

Sr. No	Name	Description	Example Value	Value
		which software like XManager is installed for rendering UI of a utility executing on a remote Linux server.		
189	LOCAL_ DISPLAY_VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0.0	
190	DOMAIN_NAME	Weblogic Domain name	Host_domain or ui_domain or base_domain	
191	XD_ COMPONENT_ NAME	XD Component value	obpui	
192	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_ NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
193	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
194	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
195	LOCAL_ DATASOURCE	Username of LOCAL_ DATASOURCE	PRDUI_STB	
196	WLS_RUNTIME_ SCHEMA_USER	WLS RUNTIME Data source	PRDUI_WLS_RUNTIME	
197	OPSS_UI_ SCHEMA_USER	OPSS UI schema name	PRDUI_OPSS	
198	OPSS_UI_ SCHEMA_ PASSWORD	OPSS UI schema password	Welcome1	
199	OPSS_UI_DB_IP	OPSS UI DB IP	10.180.84.113	
200	OPSS_UI_DB_ PORT	OPSS UI DB PORT	1521	
201	OPSS_UI_DB_ SERVICE_NAME	OPSS UI DB SERIVICE NAME	P84113A	

Sr. No	Name	Description	Example Value	Value
202	MDS_SCHEMA_ USER	MDS schema name	PRDUI _MDS	
203	MDS_SCHEMA_ PASSWORD	Password of MDS schema	welcome1	
204	MDS_DB_IP	MDS DB IP	10.180.84.113	
205	MDS_DB_PORT	MDS DB PORT	1521	
206	MDS_DB_ SERVICE_NAME	MDS DB SERVIVE NAME	P84113A	
207	OPSS_SOA_ SCHEMA_USER	SOA OPSS Schema name	PRDSOA _OPSS	
208	OPSS_SOA_ AUDIT_DBDS	SOA OPSS AUDIT schema name	PRDSOA_IAU_APPEND	
209	OPSS_SOA_ AUDIT_VIEWDS	SOA OPSS AUDIT VIEWDB Schema name	PRDSOA_IAU_VIEWER	
210	OPSS_SOA_ SCHEMA_ PASSWORD	SOA OPSS password for above three OPSS schema	welcome1	
211	OPSS_SOA_DB_ IP	Service name of UI OPSS DB	10.180.84.113	
212	OPSS_SOA_DB_ PORT	SOA OPSS DB PORT	1521	
213	OPSS_SOA_DB_ SERVICE_NAME	SOA OPSS DB SERVICE NAME	P84113A	
214	HOST_SCHEMA_ USER	OBDLOCS Host Database username	OBDLOCS27	
215	HOST_SCHEMA_ PASSWORD	OBDLOCS Host Database password	welcome1	
216	HOST_DB_IP	OBDLOCS Host Database i/p address	10.180.84.113	
217	HOST_DB_PORT	OBDLOCS Host Database listen port	1521	
218	HOST_DB_ SERVICE_NAME	OBDLOCS Host Database	P84113A	

Sr. No	Name	Description	Example Value	Value
		service name		
219	ONS_NODE	i/p address of ONS service	10.180.84.113	
220	ONS_PORT	Listen port of ONS service	6250	
221	ADMIN_ SERVER_ LISTEN_ ADDRESS	Admin server listen address	10.180.84.111	
222	ADMIN_ SERVER_ LISTEN_PORT	Admin server listen port	7001	
223	ADMIN_ SERVER_SSL_ LISTEN_PORT	Admin server SSL listen port	7002	
224	MANAGED_ SERVER_ LISTEN_ ADDRESS	Managed server listen address	10.180.84.111	
225	MANAGED_ SERVER_ LISTEN_PORT	Managed server listen port	8001	
226	MANAGED_ SERVER_SSL_ LISTEN_PORT	Managed server SSL listen port	8002	
227	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
228	OID_IP	I/P address of the OID server	10.180.84.113	
229	OID_PORT	Port of the OID process instance.	3060	
230	OID_ADMIN_ USER	Admin user id which can be used to login of the OID as administrator.	cn=orcladmin	
231	OID_ADMIN_ PWD	Refers to the password of admin user of the OID	welcome1	
232	OID_GROUP_	The DSN used	cn=Groups,dc=in,dc=oracle,dc=com	

Sr. No	Name	Description	Example Value	Value
	DSN	for object class Groups in the OID ldap.		
233	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	ou=obp,cn=Users,dc=in,dc=oracle,dc=com	
234	NODE_MGR_ PORT	Refers to the port number to be used for the weblogic node manager. This port should either be free on the UI Presentation server or an existing weblogic node manager should be installed to listen on this port when the same is started	5556	
235	UI_IP	I/P address of the server on which the OBDLOCS presentation or UI layer should be installed.	10.180.84.111	
236	UI_CLUSTER_ NAME	Name of UI Managed Cluster	obpui_cluster1	
237	UI_SERVER_ NAME	Name of UI Managed Server	obpui_server1	
238	UI_TARGET	Refers to a location on the UI server where the installables can be transferred. The user id of the use used for installation of OBDLOCS should have read, write and execute privileges on this directory.	/scratch/install/target	

Sr. No	Name	Description	Example Value	Value
239	UI_MW_HOME	Refers to the middleware home of the weblogic installation on the UI server.	/scratch/app/product/fmw	
240	UI_JAVA_HOME	Refers to the home directory of java installation. The version of java installed should be 1.8.0 or above. This is used to execute the OBDLOCS security policies policy seeding utility at the end of the installation.	/scratch/app/product/jdk1.8.0_101	
241	OUI_JAVA_HOME	Refers to the home directory of java installation.	/scratch/app/product/jdk1.8.0_101	
242	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
243	INSTALL_AS	Linux login user id used to install the OBDLOCS solution.	ofssobp	
244	IPM_UNIX_USER	Linux login user id of IPM server	ofssobp	
245	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
246	IPM_SERVER_ PORT	Listen port of IPM server	16000	
247	IPM_MW_HOME	Oracle IPM Middleware Home directory on IPM server	/scratch/app/product/fmw	
248	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/wccontent	

Sr. No	Name	Description	Example Value	Value
249	BIP_SERVER_IP	i/p address of BIP server	10.180.84.115	
250	BIP_SERVER_ PORT	Listen port of BIP server	9502	
251	BIP_UNIX_USER	Linux login user id of BIP server	ofssobp	
252	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
253	OAAM_SERVER_ IP	OAAM server IP for 2FA. OAAM_ SERVER_IP refers to the ip address of OAAM Server (i.e. the IP of default server name as oaam_server_ server1)	oaam-ofss.com	
254	OAAM_SERVER_ PORT	OAAM server Port for 2FA. OAAM_ SERVER_ PORT refers to the port of OAAM Server (default server name as oaam_ server_server1)	14000	
255	OIM_SERVER_IP	Oracle Identity Manager i/p address	oim-ofss.com	
256	OIM_SERVER_ PORT	Oracle Identity Manager Listen Port	16000	
257	OFSAA_ SERVER_IP	OFSAA Server i/p address	ofsaa-ofss.com	
258	OFSAA_ SERVER_PORT	OFSAA Server listen port	17000	
259	UI_ADMIN_JVM_ PARAMS	UI domain admin JVM startup parameters	-Xms2048m -Xmx4096m	

Sr. No	Name	Description	Example Value	Value
260	HOST_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of HOST admin server	10.180.84.110	
261	HOST_ADMIN_SERVER_LISTEN_PORT	Listen port of HOST admin server	7001	
262	HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of host managed server	10.180.84.110	
263	HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of host managed server	8001	
264	SOA_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
265	SOA_MANAGED_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
266	SOA_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of Admin SOA server	10.180.84.112	
267	SOA_ADMIN_SERVER_LISTEN_PORT	Listen port of Admin SOA server	7001	
268	KEYSTORE_PASSWORD	Password for generating certificate	welcome1	
269	UI_SSL_PASSWORD	Password for configuring SSL in UI domain	welcome1	
270	UCM_READ_FROM_URL	Flag for getting UCM URL from properties file. These values are used by the Webcenter Portal application for internet banking.	true/false	

Sr. No	Name	Description	Example Value	Value
		Hence values for UCM_ READ_FROM_ URL and UCM_ IP, UCM_PORT below can be left as is for installations, which do not use the Webcenter portal for hosting their internet banking application. However, as a best practice, it is recommended that we configure values for UCP_IP and UCM_PORT correctly from day 1		
271	UCM_IP	UCM_IP the IP address of the UCM WebLogic managed server.	ofss.ucm.com	
272	UCM_PORT	Port of UCM.	4444	
273	OFFLINE_ CHANNEL_ OUTBOUND_ USERNAME	Offline username created in connector	offlineuser	
274	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password for the Offlineuser user in connector	welcome1	
275	CARD_ USERNAME	Username of Card connector.	orakey	
276	CARD_ PASSWORD	Password of Card connector.	welcome1	
277	RULE_ USERNAME	Username of Rule connector	orakey	
278	RULE_ PASSWORD	Password of Rule connector	welcome1	
279	USER_ TIMEZONE	Time zone entry	+5:30	

Sr. No	Name	Description	Example Value	Value
280	REMOTE_ EXECUTION	Flag for executing installer remotely	Y	
281	IPM_USERNAME	Username of IPM connector	weblogic	
282	IPM_PASSWORD	Password of IPM connector	weblogic1	
283	FTP_IPM_ USERNAME	Username of FTP_IPM connector	ofssobp	
284	FTP_IPM_ PASSWORD	Password of FTP_IPM connector	ofssobp123	
285	FTP_IPM_ BATCH_ USERNAME	Username of FTP_IPM_ BATCH	ofssobp	
286	FTP_IPM_ BATCH_ PASSWORD	Password of FTP_IPM_ BATCH	ofssobp123	
287	HOST_UNIX_ USER	Linux login user id for HOST server	ofssobp	
288	HOST_MW_ HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
289	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
290	SOA_DOMAIN_ NAME	SOA Domain Name	base_domain	
291	SILENT_INSTALL	Flag for installing silent or interactive mode	y	
292	SECURITY_ ENABLED	Flag for security enable	Y	
293	IPM_INSTALLED	Flag for if IPM is installed	Y	

Sr. No	Name	Description	Example Value	Value
294	BIP_INSTALLED	Flag for if BIP is installed	Y	
295	LOCAL_IP	I/P of the local machine which could be a windows machine on which software like XManager is installed for rendering UI of a utility executing on a remote Linux server.	10.180.84.112	
296	LOCAL_ DISPLAY_VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0.0	
297	DOMAIN_NAME	Name of the weblogic domain to be created	Host_domain or ui_domain or base_domain	
298	XD_ COMPONENT_ NAME	XD Component name	obpsoa	
299	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_ NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
300	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
301	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
302	MDS_SCHEMA_ USER	MDS schema user for SOA domain	SOA27_MDS	
303	SOA_ INFRASTRUCTU RE_SCHEMA_ USER	SOA infrastructure schema user for SOA domain	SOA27_SOAINFRA	
304	LOCAL_ DATASOURCE	Local schema user for SOA domain	SOA27_STB	
305	UMS_	UMS schema	SOA27_UMS	

Sr. No	Name	Description	Example Value	Value
	DATASOURCE	user for SOA domain		
306	WLS_RUNTIME_SCHEMA_USER	WLS_RUNTIME schema user for SOA domain	SOA27_WLS_RUNTIME	
307	DB_SCHEMA_PASSWORD	Password for MDS schema user	welcome1	
308	DB_IP	i/p address of MDS db machine	10.180.84.113	
309	DB_PORT	Port of MDS db port	1521	
310	DB_SERVICE_NAME	Service Name of MDS user	P84113A	
311	HOST_SCHEMA_USER	OBDLOCS Host Database username	OBDLOCS27	
312	HOST_SCHEMA_PASSWORD	OBDLOCS Host Database password	welcome1	
313	HOST_DB_IP	OBDLOCS Host Database i/p address	10.180.84.113	
314	HOST_DB_PORT	OBDLOCS Host Database port	1521	
315	HOST_DB_SERVICE_NAME	OBDLOCS Host Database service name	P84113A	
316	ONS_NODE	i/p address of ONS service	10.180.84.113	
317	ONS_PORT	Port of ONS service	6250	
318	OPSS_SOA_SCHEMA_USER	SOA OPSS Schema Name	SOA27_OPSS	
319	OPSS_SOA_AUDIT_DBDS	SOA OPSS AUDIT Schema name	SOA27_IAU_APPEND	
320	OPSS_SOA_AUDIT_VIEWDS	SOA OPSS AUDIT VIEWDS Schema name	SOA27_IAU_VIEWER	

Sr. No	Name	Description	Example Value	Value
321	OPSS_SOA_SCHEMA_PASSWORD	Password of OPSS_SOA_SCHEMA_USER	welcome1	
322	OPSS_SOA_DB_IP	i/p address of SOA OPSS DB.	10.180.84.113	
323	OPSS_SOA_DB_PORT	Port of SOA OPSS DB.	1521	
324	OPSS_SOA_DB_SERVICE_NAME	Service name of SOA OPSS DB.	P84113A	
325	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.112	
326	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
327	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen address	7002	
328	SOA_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
329	SOA_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
330	SOA_SERVER_SSL_LISTEN_PORT	SSL Listen port of SOA server	8002	
331	HUMANTASK_SERVER_LISTEN_ADDRESS	Listen address of humantask server	10.180.84.112	
332	HUMANTASK_SERVER_LISTEN_PORT	Listen port of humantask server	9001	
333	HUMANTASK_SERVER_SSL_LISTEN_PORT	SSL listen port of humantask server	9002	
334	BAM_SERVER_LISTEN_ADDRESS	Listen address of BAM server	10.180.84.112	
335	BAM_SERVER_LISTEN_PORT	Listen port of BAM server	9003	

Sr. No	Name	Description	Example Value	Value
336	BAM_SERVER_SSL_LISTEN_PORT	SSL Listen port of BAM server	9004	
337	HOST_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of HOST admin server	10.180.84.110	
338	HOST_ADMIN_SERVER_LISTEN_PORT	Listen port of HOST admin server	7001	
339	HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of host managed server	10.180.84.110	
340	HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of host managed server	8001	
341	OBEPM_HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of obepm managed server	10.180.4.113	
342	OBEPM_HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of obepm managed server	8003	
343	OBDLOCS_HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of OBDLOCS managed server	10.180.4.98	
344	OBDLOCS_HOST_MANAGED_SERVER_LISTEN_	Listen port of OBDLOCS managed server	8001	
345	OBPM_HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of obpm managed server	10.180.4.98	
346	OBPM_HOST_MANAGED_SERVER_	Listen port of obpm managed server	8003	

Sr. No	Name	Description	Example Value	Value
	LISTEN_PORT			
347	OBCCM_HOST_ MANAGED_ SERVER_ LISTEN_ ADDRESS	Listen address of occm managed server	10.180.4.113	
348	OBCCM_HOST_ MANAGED_ SERVER_ LISTEN_PORT	Listen port of occm managed server	8005	
349	OBEPR_HOST_ MANAGED_ SERVER_ LISTEN_ ADDRESS	Listen address of obepr managed server	10.180.4.113	
350	OBEPR_HOST_ MANAGED_ SERVER_ LISTEN_PORT	Listen port of obepr managed server	8001	
351	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
352	OID_IP	I/P address of the OID server.	10.180.84.113	
353	OID_PORT	Port of the OID process instance.	3060	
354	OID_ADMIN_ USER	Admin user id which can be used to login of the OID as administrator.	cn	
355	OID_ADMIN_ PWD	Refers to the password of admin user of the OID	welcome1	
356	OID_GROUP_ DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
357	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	ou=obp,cn=Users,dc=in,dc=oracle,dc=com	

Sr. No	Name	Description	Example Value	Value
358	NODE_MGR_PORT	Refers to the port number to be used for the weblogic node manager. This port should either be free on the UI Presentation server or an existing weblogic node manager should be installed to listen on this port when the same is started	5556	
359	SOA_IP	i/p address of SOA server	10.180.84.112	
360	SOA_CLUSTER_NAME	Cluster name of SOA server	obpsoa_cluster1	
361	SOA_SERVER_NAME	Server name of SOA server	soa_server1	
362	HUMAN_TASK_CLUSTER_NAME	Cluster name of Humantask server	obphumantask_cluster1	
363	HUMAN_TASK_SERVER_NAME	Server name of Humantask server	obphumantask_server1	
364	SOA_TARGET	Target folder of SOA machine where files will be copied temporarily during installation	/scratch/install/target	
365	SOA_JAVA_HOME	Refers to the home directory of java installation of the SOA machine. The version of java installed should be 1.8.0 or above. This is used to execute the OBDLOCS security policies policy seeding	/scratch/app/product/jdk1.8.0_101	

Sr. No	Name	Description	Example Value	Value
		utility at the end of the installation.		
366	OUI_JAVA_HOME	Refers to the home directory of java installation.	/scratch/app/product/jdk1.8.0_101	
367	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory/	
368	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
369	UI_IP	i/p address of UI server	10.180.84.111	
370	UI_UNIX_USER	Linux login user id for UI server	ofssobp	
371	UI_DOMAIN_ HOME	Full path of UI domain	/scratch/app/ product/fmw/ user_projects/ domains /ui_domain	
372	INSTALL_AS	Linux login user id used to install the OBDLOCS solution.	ofssobp	
373	SOA_ADMIN_ JVM_PARAMS	SOA domain admin JVM startup parameters	-Xms1024m -Xmx2048m	
374	SOA_ HUMANTASKSE RVER_JVM_ PARAMS	SOA domain human task server's JVM startup parameters	-Djbo.ampool. doampooling=false –Xms12g -Xmx12g -XX:NewSize= 512m -XX:MaxNewSize =2048m -XX: +UseParNewGC	

Sr. No	Name	Description	Example Value	Value
			-XX:+ CMSParallel RemarkEnabled -XX:+UseConcMark SweepGC -XX:CMSInitiating OccupancyFraction=75 -Dobp.http. maxRetryCount=1 -Dobp.http .socketBufferSize=81	
375	SOA_MANAGED_ JVM_PARAMS	SOA domain managed soa server's JVM startup parameters	-XX:NewSize =2048m -XX:MaxNewSize =4096m -XX:+UsePa rNewGC -XX: +CMSPar allelRemarkEnabled -XX:+UseCo ncMarkSweepGC -XX:CMSInit iatingOccupancy Fraction=75 -Xms11g -Xmx11g	
376	KEYSTORE_ PASSWORD	Password for generating certificate	welcome1	
377	UI_MANAGED_ SERVER_ LISTEN_ ADDRESS	i/p address of UI Managed server	10.180.84.111	
378	UI_MANAGED_ SERVER_ LISTEN_PORT	Listen port of UI Managed server	8001	
379	UI_MANAGED_ SERVER_SSL_ LISTEN_PORT	SSL Listen port of UI Managed server	8002	
380	UI_ADMIN_ SERVER_ LISTEN_ ADDRESS	i/p address of UI Admin server	10.180.84.111	
381	UI_ADMIN_	Listen port of UI	7001	

Sr. No	Name	Description	Example Value	Value
	SERVER_ LISTEN_PORT	Admin server		
382	DEFAULT_BANK_ CODE	Default bank code will be set while configuring SOA domain	8	
383	DEFAULT_ TRANSACTION_ BRANCH_CODE	Default branch code will be set while configuring SOA domain	89999	
384	DEFAULT_ TARGET_UNIT	Default target unit will be set while configuring SOA domain	OBP_BU	
385	CARD_ USERNAME	Username of Card connector.	orakey	
386	CARD_ PASSWORD	Password of Card connector	welcome1	
387	RULE_ USERNAME	Username of Rule connector	orakey	
388	RULE_ PASSWORD	Password of Rule connector	welcome1	
389	USER_ TIMEZONE	Time zone entry	+5:30	
390	SOA_SSL_ PASSWORD	Password for configuring SSL in SOA domain	welcome1	
391	REMOTE_ EXECUTION	Flag for executing installer remotely	Y	
392	BAM_ INSTALLATION	During SOA installation value Must be 'N' During BAM installation value Must be Y.	N	
393	IPM_USERNAME	Username of IPM connector	ofssobp	
394	IPM_PASSWORD	Password of IPM connector	welcome1	
395	OFFLINE_ CHANNEL_ OUTBOUND_	Username of offline connector	offlineuser	

Sr. No	Name	Description	Example Value	Value
	USERNAME			
396	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password of offline connector	welcome1	
397	FTP_IPM_ USERNAME	Username of FTP_IPM connector	ofssobp	
398	FTP_IPM_ PASSWORD	Password of FTP_IPM connector	ofssobp123	
399	FTP_IPM_ BATCH_ USERNAME	Username of FTP_IPM_ BATCH connector	ofssobp	
400	FTP_IPM_ BATCH_ PASSWORD	Password of FTP_IPM_ BATCH connector	ofssobp123	
401	SOA_ OUTBOUND_ USERNAME	Username of SOA connector	weblogic	
402	SOA_ OUTBOUND_ PASSWORD	Password of SOA connector	weblogic1	
403	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
404	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
405	IPM_MW_HOME	Oracle IPM middleware Home directory on IPM server	/scratch/app/product/fmw	
406	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/wccontent	
407	BIP_SERVER_IP	I/P of the BIP server to host OBDLOCS reports	10.180.84.115	
408	BIP_SERVER_ PORT	Port of the BIP server that hosts OBDLOCS reports	9502	

Sr. No	Name	Description	Example Value	Value
409	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
410	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
411	OAAM_SERVER_IP	oaam sever ip address	oaam-ofss.com	
412	OAAM_SERVER_PORT	oaam server port	14000	
413	OIM_SERVER_IP	oim server ip	oim-ofss.com	
414	OIM_SERVER_PORT	oim server port	16000	
415	OFSAA_SERVER_IP	ofss server ip	ofsaa-ofss.com	
416	OFSAA_SERVER_	ofss server port	17000	
417	DOCUMAKER_SERVER_IP	documaker server ip	documaker-ofss.com	
418	DOCUMAKER_SERVER_PORT	documaker server port	15000	
419	BAM_SERVER_NAME	Bam server name	bam-ofss.com	
420	BAM_SERVER_PORT	Bam server port	9003	
421	ODI_SERVER_NAME	Odi server name	odi-ofss.com	

2.4.3 Database and WebLogic Domain Configuration

The following table lists the other information which should be kept handy to make this installation easy.

Table 2–6 DB and WebLogic Domain Configuration

Sr. No.	Name	Description and Example	Value
UI and Host Linux user login details			
1	UI / Presentation Linux server user id	This is same as INSTALL_AS captured in the checklist above.	
2	UI / Presentation Linux server user password	Password for the user specified against INSTALL_AS.	

Sr. No.	Name	Description and Example	Value
3	Host Linux server user id	This is same as INSTALL_AS captured in the checklist above.	
4	Host Linux server user password	Password for the user specified against INSTALL_AS.	
Database Details			
5	IP address of the OBDLOCS Oracle DB server	10.180.90.30	
6	Port of the OBDLOCS Oracle DB instance	1521	
7	OBDLOCS DB Service Name	OBPDB	
8	OBDLOCS DB sys password	**********	
9	ONS NODE	10.180.90.30, Make sure ons service is started on DB.	
10	ONS Port	6250	
Additional UI Install Checklist			
11	Admin user id and password for the OBDLOCS UI domain.	The default admin user id is WebLogic. Decide on the password to be used and note it.	
12	List of port numbers for the OBDLOCS UI domain for: Admin server HTTP port for managed server HTTPS port for managed server	Default Values Admin Server Port: 7001 Managed Server http port: 15308 Managed Server https port: 15309	
13	Password for the key generated to establish trust between the OBDLOCS UI and Host.	Decide on the password to be used and note it. This is required for the post installation tasks of UI domain.	
14	Password for keystore generated to establish trust.	Decide on the password to be used and note it. This is required for the post installation tasks UI domain.	
Additional Host Install Checklist			
15	Admin user id and password for the OBDLOCS Host domain.	The default admin user id is WebLogic. Decide on the password to be used and note it.	
16	List of port numbers for	Default Values	

Sr. No.	Name	Description and Example	Value
	the OBDLOCS Host domain for: Admin server HTTP port for managed server HTTPS port for managed server	Admin Server Port: 7001 Managed Server http port: 15308 Managed Server https port: 15309	
17	Password for the key generated to establish trust between the OBDLOCS UI and Host.	This is same as password in row 11. This is required for the post installation tasks of host domain.	
18	Password for keystore generated to establish trust.	This is same as password in row 12. This is required for the post installation tasks of host domain.	

2.5 OID Schema Setup – Custom OBDLOCS Schema

This section describes the OID Schema setup which is a pre-installation configuration required for Oracle Banking Deposits and Lines of Credit Servicing setup.

2.5.1 Prerequisite – OID setup

I4.1. It is assumed that OID 12.2.1.3.0 is installed with ODSM and configured.

2.5.2 Verify the OID installation

This section describes the procedure to verify the OID installation.

2.5.2.1 Start and Verify the OID processes

Log in to the Linux console with user id `oracle`, navigate to the 'bin' directory of the OID instance and start the OID processes using the commands as follows:

For example, if the OID installation is in "/scratch/app/product/fmw/user_projects/domains/oid_domain/bin"

cd /scratch/app/product/fmw/user_projects/domains/oid_domain/bin

./startComponent.sh oid1

2.5.2.2 OPSS/OID Performance Tuning

The following changes are required in OID before initiating OBDLOCS installation:

Parameters

Change the parameter values as provided below.

Table 2–7 Parameter Values to be Changed

Parameter Name	Value
orclmaxcc (Number of DB Connections per Server Process)	10

Parameter Name	Value
orclserverprocs (Number of OID LDAP Server Processes)	4
orclgeneratechangelog (Change log Generation)	0
orclldapconntimeout (LDAP Connection Timeout)	60
orclmatchdenabled (Enable MatchDN Processing)	0

Advanced OID tuning

The steps to perform advanced OID tuning are as follows:

1. Create a .ldif file with any name. For example, tune.ldif.
2. Enter the following information in that file and save it:

   dn: cn=dsaconfig,cn=configsets,cn=oracle internet directory
   changetype: modify
   replace: orclecachemaxsize
   orclecachemaxsize: 3g
   -
   replace: orclecachemaxentries
   orclecachemaxentries: 500000

   Sample tune.ldif file
   dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
   changetype: modify
   replace: orclserverprocs
   orclserverprocs: 4

   dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
   changetype: modify
   replace: orclmaxcc
   orclmaxcc: 10

   dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry
   changetype: modify
   replace: orclgeneratechangelog
   orclgeneratechangelog: 0

dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry

changetype: modify

replace: orclldapconntimeout

orclldapconntimeout: 60

dn: cn=oid1,cn=osdldapd,cn=subconfigsubentry

changetype: modify

replace: orclmatchdenabled

orclmatchdenabled: 0

3. See the OID Tuning Guide available at: https://docs.oracle.com/en/middleware/lifecycle/12.2.1.3/asper/oracle-internet-directory-performance-tuning.html#GUID-254611A2-0B71-4FBE-90D1-4D13A41B5F47

OPSS Tuning

The steps to perform advanced OPSS tuning are as follows:

1. **IDM Database recommendations**

   a. The following table presents the suggested values of parameters and alter scripts executed in system for which the user needs to change the parameters.

Table 2–8 Suggested values for Tuning and Alter Command

Sr. No.	DB Property Name	Suggested Value for Tuning	Alter Command
1	Process	1500	ALTER SYSTEM SET processes = 1500 SCOPE = spfile;
2	SGA Target	3G	ALTER SYSTEM SET sga_target = 3221225472 SCOPE = spfile;
3	Audit Trail	None	ALTER SYSTEM SET audit_sys_ operations=FALSE SCOPE =SPFILE; ALTER SYSTEM SET audit_trail = NONE SCOPE = spfile;
4	Open Cursor	500	ALTER SYSTEM SET open_cursors = 500 SCOPE = spfile;
5	PGA_Aggregate_Target	1.5GB	ALTER SYSTEM SET pga_aggregate_ target = 1610612736 SCOPE = spfile;
6	NLS Sort	Binary	ALTER SYSTEM SET nls_sort = BINARY SCOPE = spfile;
7	Filesystemio_Options	SETALL	ALTER SYSTEM SET filesystemio_ options = SETALL SCOPE = spfile;
8	Fast_start_mttr_target	3600	ALTER SYSTEM SET fast_start_mttr_

Sr. No.	DB Property Name	Suggested Value for Tuning	Alter Command
			target = 3600 SCOPE = spfile;
9	db_securefile	ALWAYS	ALTER SYSTEM SET db_securefile = ALWAYS SCOPE = spfile;
10	Session_cached_ cursors	500	ALTER SYSTEM SET session_ cached_cursors = 500 SCOPE = spfile;
11	plsql_code_type	NATIVE	ALTER SYSTEM SET plsql_code_ type = NATIVE SCOPE = spfile;
12	_b_tree_bitmap_plans	false	ALTER SYSTEM SET "_b_tree_ bitmap_plans" = FALSE scope=spfile;
13	Memory_target	0	ALTER SYSTEM SET memory_ target=0 SCOPE = SPFILE;

b. Redo log file.

Allocated Disk Space for Redo Log Files

```
ALTER DATABASE ADD logfile ('<oradata
directory>/ORA4212/redo01.log') SIZE 4G REUSE;

ALTER DATABASE ADD logfile ('<oradata
directory>/ORA4212/redo02.log') SIZE 4G REUSE;

ALTER DATABASE ADD logfile ('<oradata
directory>/ORA4212/redo03.log') SIZE 4G REUSE;
```

c. Undo tablespace.

Increase Disk Space Allocated for UNDO Tablespace

```
ALTER DATABASE DATAFILE '<oradata directory>/ORA4212/undotbs01.dbf'
RESIZE 20G NEXT 1G;
```

2. jps-config.xml (All servers of UI, Host, SOA domains)

a. Remove the following properties from <serviceInstance name="pdp.service" provider="pdp.service.provider"> in jps_config.xml.

```
<property
name="oracle.security.jps.runtime.pd.client.policyDistri
butionMode" value="mixed"/>
<property
name="oracle.security.jps.runtime.instance.name"
value="OracleIDM"/>
<property name="oracle.security.jps.runtime.pd.client.sm_
name" value="OracleIDM"/>
```

```
<property
name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
```

b. Add following properties:

<DOMAIN-HOME>/config/fmwconfig/jps-config.xml

```
<propertySet name="props.db.1">
<property name="authorization_cache_enabled"
value="true"/>
<property name="connection.pool.min.size" value="20"/>
<property name="connection.pool.max.size" value="40"/>
<property name="connection.pool.provider.type"
value="IDM"/>
<property name="connection.pool.timeout" value="300000"/>
<property name="connection.pool.provider.type"
value="5"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.t
ype" value="STATIC"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
trategy" value="NONE"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
ize" value="100"/>
<property
name="oracle.security.jps.policystore.policy.lazy.load.e
nable" value="true"/>
<property
name="oracle.security.jps.policystore.policy.cache.strat
egy" value="NONE"/>
<property
name="oracle.security.jps.policystore.policy.cache.size"
value="1000000"/>
<property
name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
<property
name="oracle.security.jps.policystore.refresh.purge.time
out" value="43200000"/>
<property
name="oracle.security.jps.ldap.policystore.refresh.inter
val" value="6000000"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.w
armup.enable" value="true"/>
```

```
</propertySet>
```

c. All the above properties should also be added in the <pdp.service> service-instance.

```
<serviceInstance name="pdp.service"
provider="pdp.service.provider">
<description>Runtime PDP service instance</description>
<property name="authorization_cache_enabled"
value="true"/>
<property name="connection.pool.min.size" value="20"/>
<property name="connection.pool.max.size" value="40"/>
<property name="connection.pool.provider.type"
value="IDM"/>
<property name="connection.pool.timeout" value="300000"/>
<property name="connection.pool.provider.type"
value="5"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.t
ype" value="STATIC"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
trategy" value="NONE"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
ize" value="100"/>
<property
name="oracle.security.jps.policystore.policy.lazy.load.e
nable" value="true"/>
<property
name="oracle.security.jps.policystore.policy.cache.strat
egy" value="NONE"/>
<property
name="oracle.security.jps.policystore.policy.cache.size"
value="1000000"/>
<property
name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
<property
name="oracle.security.jps.policystore.refresh.purge.time
out" value="43200000"/>
<property
name="oracle.security.jps.ldap.policystore.refresh.inter
val" value="6000000"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.w
armup.enable" value="true"/>
</serviceInstance>
```

3. adf-config.xml (optional)

In adf-config.xml, maintain **authorizationEnforce="true"**

4. setDomainEnv.sh

   In setDomainEnv.sh file, include the following java properties. These are absolutely necessary, if authorizationEnforce = true (previous point).

   Table 2–9 Properties

Property	Description
-Djps.combiner.optimize=true	This system property is used to cache the protection domains for a given subject. Setting –`Djps.combiner.optimize=true` can improve Java authorization performance.
-Djps.combiner.optimize.lazyeval=true	This system property is used to evaluate a subject's protection domain when a checkPermission occurs. Setting –`Djps.combiner.optimize.lazyeval=true` can improve Java authorization performance.
-Djps.policystore.hybrid.mode=false	This 'hybrid mode' property is used to facilitate transition from SUN java.security.Policy to OPSS Java Policy Provider.
-Djps.authz=ACC	Delegates the call to JDK API AccessController.checkPermission which can reduce the performance impact at run time or while debugging.
-DUSE_JAAS=false	
-Djps.auth=ACC	Delegates the call to JDK API AccessController.checkPermission which can reduce the performance impact at run time or while debugging
-Djps.auth.debug=false	Turn off debugging. This is turned on to debug access denied errors.
-Djps.subject.cache.key=5	JPS uses a Subject Resolver to convert a platform subject to JpsSubject which contains user/enterprise-role information, as well as ApplicationRole information. This information is represented as principals in the subject. Value = 5: Instead of using the whole subject as the key, this settings uses a subset of the principal set inside the subject as the key (actually use principals of WLSUSerImpl type). This setting will accelerate the cache retrieval operation if the subject has a large principal set.
-Djps.subject.cache.ttl=600000	Cache's Time To Live (TTL) for case '5' (above). This system property controls how long the cache is valid. When the time expired, the cached value is dumped. The setting can be controlled by the flag of -Djps.subject.cache.ttl=xxxx, where 'xxx' is the duration in milliseconds. Consider setting the duration of this TTL setting to the same value as the value used for the group and user cache TTL in WLS LDAP authenticator.

Example:

```
JAVA_PROPERTIES="-Djps.combiner.optimize=true -
Djps.combiner.optimize.lazyeval=true -Djps.policystore.hybrid.mode=false
-Djps.authz=ACC ${JAVA_PROPERTIES} ${WLP_JAVA_PROPERTIES}"

export JAVA_PROPERTIES
```

2.5.2.3 Import OBDLOCS Specific LDIF files

If Oracle Identity Manager (OIM) is installed as the user provisioning product, use the ldif files from the location <HOST_TARGET>. These ldif files do not contain any predefined users and roles other than some crucial system users that are needed during startup. The privileges of these users are contained. OIM is used for creation of first user in OBDLOCS.

If OIM is not part of the ecosystem and an initial sanity test of the OBDLOCS installation is needed, the sample ldif files present at the location<HOST_TARGET> can be used for creation of Users and Groups. These sample files can be used directly or can be modified as per requirements. In production after initial verification these users have to be removed.

Note

Ensure that 'ldapadd' and 'ldapmodify' are available on the machine.

1. Extract the 'obpus-host.zip' to obtain 'obpinstall-host.zip'. It contains ldif.zip and sampleLdif.zip.
2. Extract ldif.zip. It will create a folder named ldif with ldif files or extract sampleLdif.zip, which will create a folder named ldif, with ldif files as follows:
   - fcPerson.ldif
   - obp_ou.ldif
   - jpsroot.ldif
   - Users.ldif
   - Groups.ldif
   - Weblogic.ldif
   - Administrators.ldif
3. These are to be used and updated in the OID if necessary. The execution commands for uploading these LDIF files are given below. The execution order must be maintained as described.

Table 2–10 Order of Execution

Sr. No.	LDIF File Name	Description
1	fcPerson	Creates fcPerson object class
2	obp_ou	Creates obp user Users

Sr. No.	LDIF File Name	Description
3	Jpsroot	Creates jpsroot and jpscontext
4	Users	Creates OFSSUser
5	Groups	Creates OFSS_Role and offlinerole
6	Weblogic	Creates weblogic user
7	Administrators	Creates Administrators Group

4. DNS should be changed as per the requirement of the bank in the LDIF files for:
   - Users
   - Groups
   - WebLogic
   - Administrators

   Note

   While executing fcPerson.ldif, “value already exist” problem may appear in console.

   For this problem, the objectClasses value is required to be changed.

   It can be found, at the end of the file as:

   “add:objectClasses

   objectClasses:(2.5.6.47”

   To resolve this problem, change the value (default, it is 2.5.6.47) of object classes, then run it again.

5. Before executing the following commands, navigate to the location where the LDIF files reside (that is, inside LDIF folder) in Host machine, where OpenLDAP has been installed as mentioned in prerequisite section.

   ldapadd fcPerson.ldif

   ```
   ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
   fcPerson.ldif
   ```

   ldapadd obp_ou.ldif

   ```
   ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
   obp_ou.ldif
   ```

   ldapadd jpsroot.ldif

   ```
   ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
   jpsroot.ldif
   ```

   ldapadd Users.ldif

```
ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
Users.ldif
```

ldapadd Groups.ldif

```
ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
Groups.ldif
```

ldapadd WebLogic.ldif

```
ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
Weblogic.ldif
```

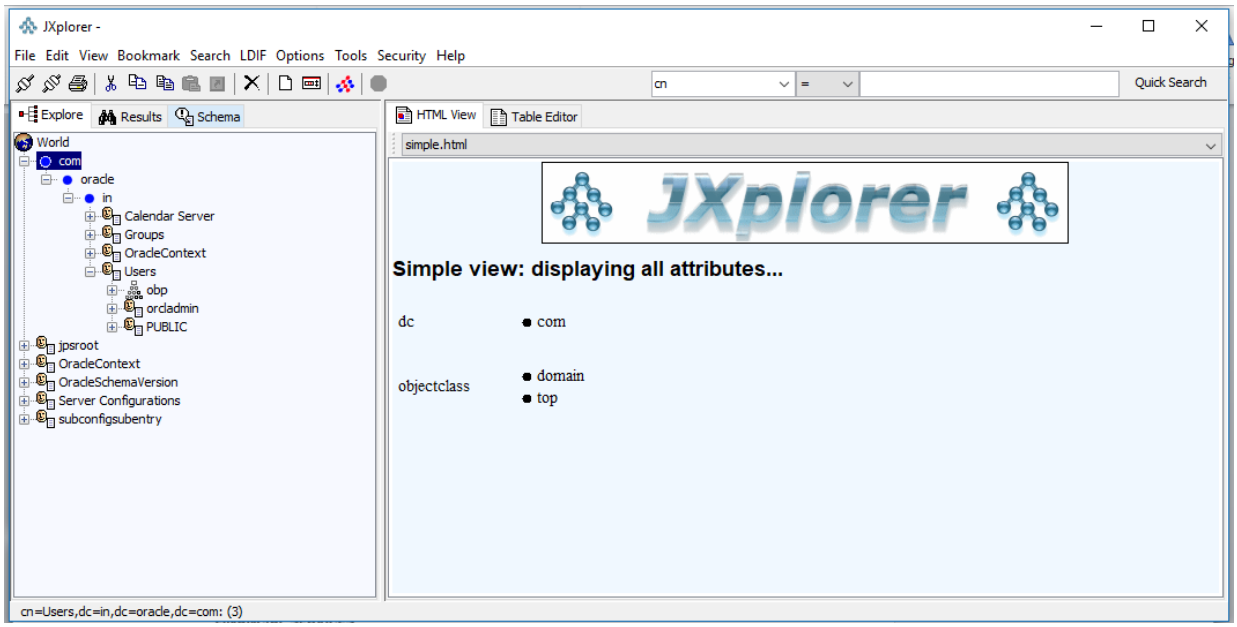
ldapadd Administrators.ldif

```
ldapadd -h $ldapIP -p $ldapPort -D cn=orcladmin -w welcome1 -c -v -f
Administrators.ldif
```

2.5.2.4 Verify the import using ODSM or JXplorer

The import of Oracle Banking Deposits and Lines of Credit Servicing specific LDIF files can be verified using JXplorer.

Figure 2–2 JXplorer



3 OBDLOCS US Localization SOA Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Deposits and Lines of Credit Servicing US Localization SOA Media Pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

3.1 Installation and Configuration Procedure

This section details the installation procedure for the OBDLOCS US Localization SOA Media Pack.

3.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBDLOCS US Localization SOA Media Pack installation.

Step 1 Procuring Installables

Download the appropriate SOA media pack from the following location:

http://edelivery.oracle.com/

Step 2 Extracting the Installables

Copy the 'obpus-soa.zip' to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Three files will be extracted:

- A zip file 'obpinstall-soa.zip'
- The installation script 'installobpsoa.sh'
- The install configuration property file 'installobpsoa.properties'

Step 3 Printing Checklists

Take a printout of the installation checklist mentioned in Section 2.4 Installation Checklist of this guide and note the values applicable for each point in the last column for 'Value' so that the same is handy during the actual installation.

3.1.2 Pre-Installation Steps

This section lists the pre-installation steps required for the OBDLOCS US Localization SOA Media Pack installation.

Step 1 Updating installobpsoa.properties

Navigate to the directory where the files obpinstall-soa.zip, installobpsoa.sh and installobpsoa.properties are placed and update installobpsoa.properties with relevant values from the checklist.

Step 2 Checklist for a new setup

Before initiating installation, check the following:

- Make sure required RCU schemas have been created. For more information, see Section 6.1 Pre-Installation Steps and Section 6.2 OBDLOCS Database Setup – RCU Installation.
- Increase the size of tablespace (at least 6GB and the auto extend mode must be on) for MDS, SOAINFRA and OPSS schema used for SOA domain.
- Node manager must not be running on the target machine.
- Create a dummy folder named target and mention its path against SOA_TARGET property.
- Values given in installobpui.properties must be correct. At run time, no option is given to change the values.
- No processes should be running on the ports given in installobpsoa.properties.
- In case of a re-installation ensure that the directory paths against SOA_TARGET and SOA_MW_HOME specified in installobpsoa.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- Before initiating the installation, ensure that all the values given in installobpsoa.properties are correct. At the time of installation, the values will only be displayed once for verification, and it will not be possible to change the values once the installation begins.

Step 3 OS Level Tuning

OBDLOCS libraries are usually copied on an NFS mount. During startup a lot of time is spent fetching these libraries for classloading and resource loading. The last access time on the files gets imprinted on the file metadata, which actually incurs a WRITE. Since, this is over NFS, this has a performance impact.

The mount points should be mounted using the "noatime" flag to disable updating the access time. This is a recommended parameter as per FMW MAA shared storage WP.

For more information, see the following document:

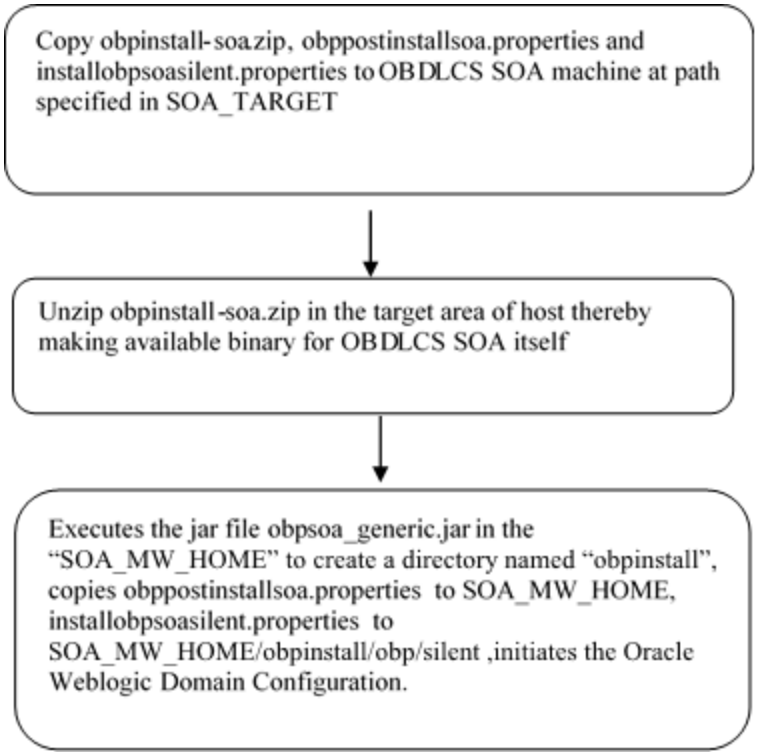
http://www.oracle.com/technetwork/database/availability/maa-fmwsharedstoragebestpractices-402094.pdf

3.1.3 Installation Steps

This section lists the installation steps required for the OBDLOCS US Localization SOA Media Pack installation.

1. Navigate to the directory where the media pack files are placed and execute installobpsoa.sh. The installation script shall echo the values entered in the installobpsoa.properties file and ask for a confirmation to go ahead with the installation.
2. The installation script automatically triggers the following significant steps using secure remote copy ’scp’ command and remote shell commands execution using the ’ssh’ command.

Figure 3–1 Steps in installobpsoa.sh script



A sample output is given here.

./installobpsoa.sh

Figure 3–2 Verification of Properties

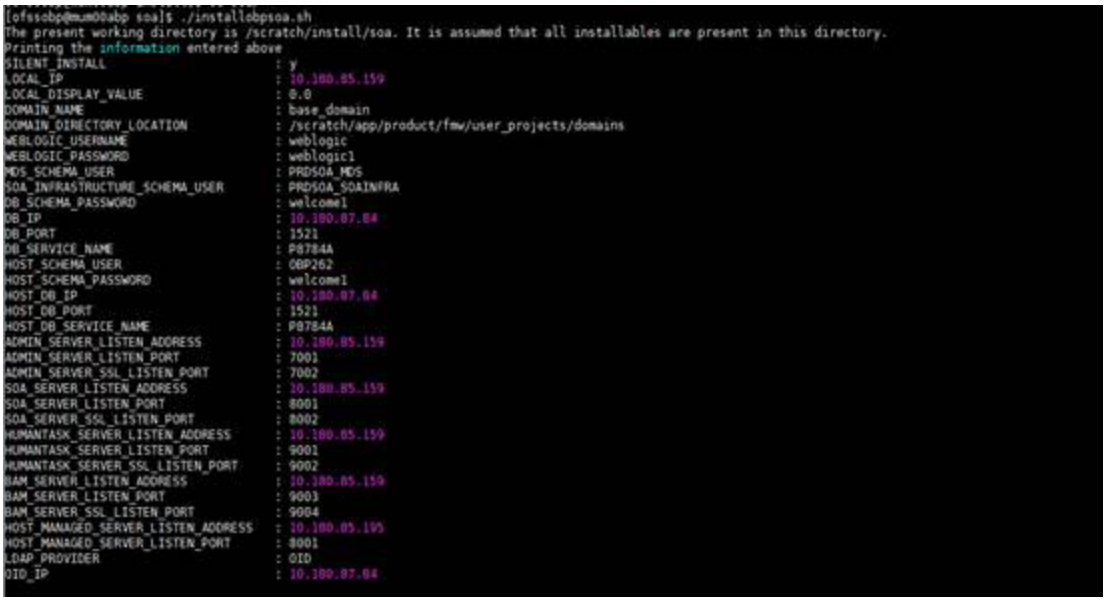


Figure 3–3 Verification of Properties

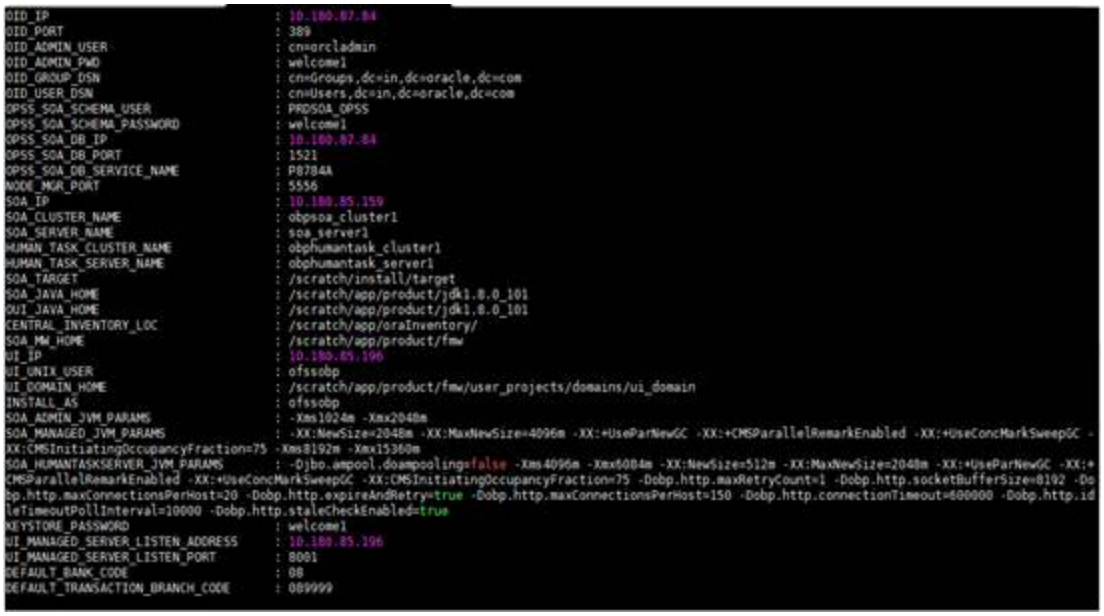
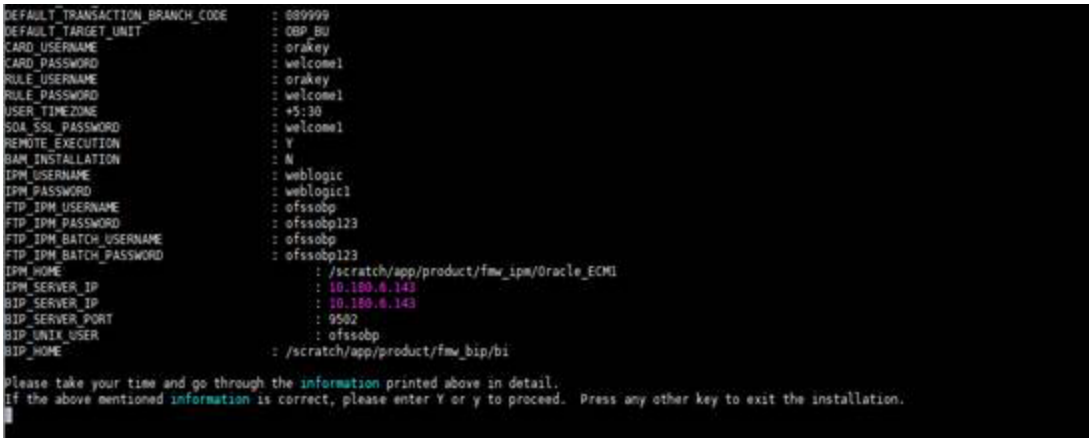


Figure 3–4 Confirmation to Proceed Domain Installation (cont.)



3. Verify the value of each property carefully before proceeding.
4. If all values are correct, then enter 'Y' or 'y' and press Enter to initiate the installation. The installation utility performs the installation and domain is created silently.

Figure 3–5 Copying and Extraction of obpinstall-soa.zip

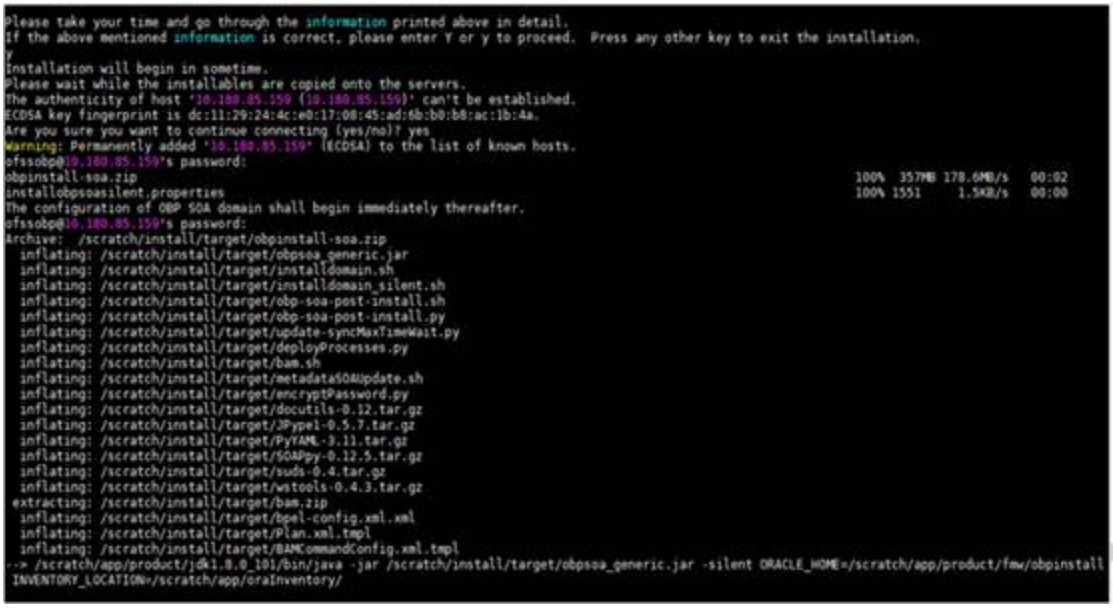


Figure 3–6 Copying and Extraction of obpinstall-soa.zip

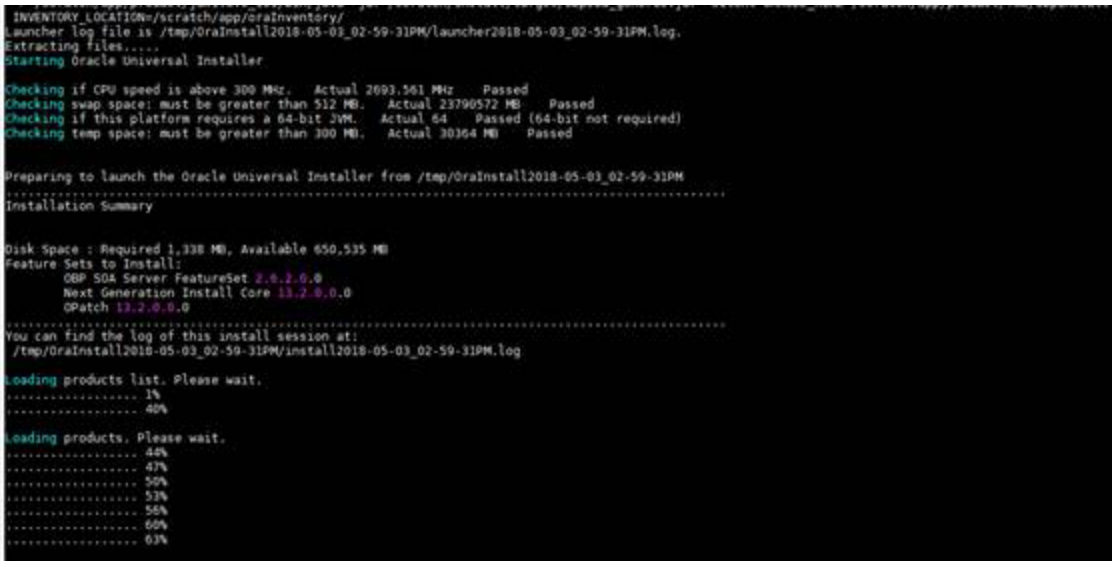


Figure 3–7 Copying and Extraction of obpinstall-soa.zip

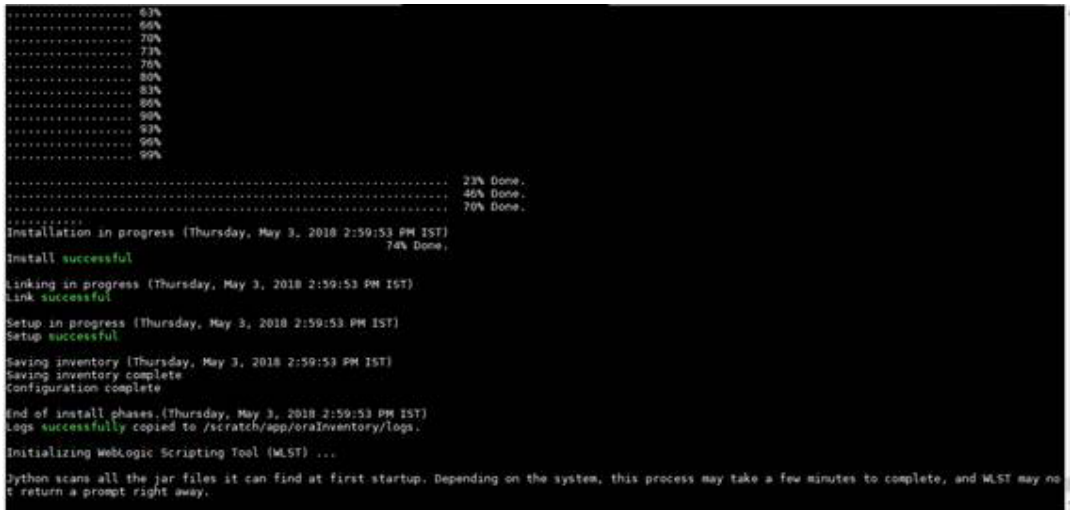


Figure 3–8 Domain Creation Confirmation

3.2 Post Installation Configuration

This section describes the post installation configuration procedure for OBDLOCS US Localization SOA Media Pack.

Checklist for Post Installation Procedure

Before proceeding with the post installation procedure for SOA, ensure the following:

- Replace /scratch/app/product/fmw path with your middleware home path in setDomainEnv.sh and setDomainEnvSOA if not replaced.
- Node manager is not running on the SOA machine.
- All values in obppostinstallsoa.properties are correct
- OID_DOMAIN_NAME given in obppostinstallsoa.properties must not exist.
- Node manager port should be free. You can verify using the following command, where 5556 is the Node Manager Port.

```
$netstat -na | grep 5556
```

Post Installation Configuration

1. Start the OBDLOCS SOA domain admin WebLogic server by executing the startWebLogic.sh script in the domain directory.

```
cd <middleware home>
cd user_projects/domains/obpsoadomain/bin
./startWebLogic.sh
```

2. Enter the username and password when prompted.
3. Start the managed server – soa_server1.

```
cd <middleware home>
cd user_projects/domains/obpsoadomain/bin
./startManagedWebLogic.sh soa_server1 t3://localhost:<admin_
server_port>
```

Note

Do not run the post-install as soon as SOA server comes up.

Wait until it loads all the processes and displays the message *SOA platform is running and accepting requests.*

Initiate post-install after getting this message in the console.

4. Once the SOA admin and managed servers are running, execute the post install script 'obp-soa-post-install.sh' created under middleware directory just like other domains.
5. Navigate to the middleware location and give executable permission to the post install script:

```
$cd <soa middleware home>
```

Then execute following script:

```
$./obp-soa-post-install.sh
```

A sample output is given here:

Figure 3–9 Starting Post Installation

```
[ofssobp@mum00abp fmw]$ ./obp-soa-post-install.sh
DOMAIN_NAME                         : base_domain
DOMAIN_DIRECTORY_LOCATION           : /scratch/app/product/fmw/user_projects/domains
WEBLOGIC_USERNAME                   : weblogic
WEBLOGIC_PASSWORD                   : weblogic1
ADMIN_SERVER_LISTEN_ADDRESS         : 10.180.85.159
ADMIN_SERVER_LISTEN_PORT            : 7001
SOA_SERVER_LISTEN_ADDRESS           : 10.180.85.159
SOA_SERVER_LISTEN_PORT              : 8001
BAM_SERVER_LISTEN_ADDRESS           : 10.180.85.159
BAM_SERVER_LISTEN_PORT              : 9003
HOST_MANAGED_SERVER_LISTEN_ADDRESS  : 10.180.85.195
HOST_MANAGED_SERVER_LISTEN_PORT     : 8001
LDAP_PROVIDER                       : OID
OID_IP                              : 10.180.87.84
OID_PORT                            : 389
OID_ADMIN_USER                      : cn=orcladmin
OID_ADMIN_PWD                       : welcome1
OID_GROUP_DSN                       : cn=Groups,dc=in,dc=oracle,dc=com
OID_USER_DSN                        : cn=Users,dc=in,dc=oracle,dc=com
NODE_MGR_PORT                       : 5556
SOA_IP                              : 10.180.85.159
SOA_CLUSTER_NAME                    : obpsoa_cluster1
SOA_SERVER_NAME                     : soa_server1
HUMAN_TASK_CLUSTER_NAME             : obphumantask_cluster1
HUMAN_TASK_SERVER_NAME              : obphumantask_server1
SOA_TARGET                          : /scratch/install/target
SOA_JAVA_HOME                       : /scratch/app/product/jdk1.8.0_101
SOA_MW_HOME                         : /scratch/app/product/fmw
UI_IP                               : 10.180.85.196
UI_UNIX_USER                        : ofssobp
UI_DOMAIN_HOME                      : /scratch/app/product/fmw/user_projects/domains/ui_domain
INSTALL_AS                          : ofssobp
SOA_ADMIN_JVM_PARAMS                : -Xms1024m -Xmx2048m
SOA_MANAGED_JVM_PARAMS              : -XX:NewSize=2048m -XX:MaxNewSize=4096m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -
XX:CMSInitiatingOccupancyFraction=75 -Xms8192m -Xmx15360m
SOA_HUMANTASKSERVER_JVM_PARAMS      : -Djbo.ampool.doampooling=false -Xms4096m -Xmx6084m -XX:NewSize=512m -XX:MaxNewSize=2048m -XX:+UseParNewGC -XX:+
CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -Dobp.http.maxRetryCount=1 -Dobp.http.socketBufferSize=8192 -Do
```

Figure 3–10 Starting Post Installation (contd)

```
SOA_HUMANTASKSERVER_JVM_PARAMS      : -Djbo.ampool.doampooling=false -Xms4096m -Xmx6084m -XX:NewSize=512m -XX:MaxNewSize=2048m -XX:+UseParNewGC -XX:+
CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -Dobp.http.maxRetryCount=1 -Dobp.http.socketBufferSize=8192 -Do
bp.http.maxConnectionsPerHost=20 -Dobp.http.expireAndRetry=true -Dobp.http.maxConnectionsPerHost=150 -Dobp.http.connectionTimeout=600000 -Dobp.http.id
leTimeoutPollInterval=10000 -Dobp.http.staleCheckEnabled=true
KEYSTORE_PASSWORD                   : welcome1
UI_MANAGED_SERVER_LISTEN_ADDRESS    : 10.180.85.196
UI_MANAGED_SERVER_LISTEN_PORT       : 8001
DEFAULT_BANK_CODE                   : 08
DEFAULT_TRANSACTION_BRANCH_CODE     : 089999
DEFAULT_TARGET_UNIT                 : OBP_BU
CARD_USERNAME                       : orakey
CARD_PASSWORD                       : welcome1
RULE_USERNAME                       : orakey
RULE_PASSWORD                       : welcome1
USER_TIMEZONE                       : +5:30
REMOTE_EXECUTION                    : Y
BAM_INSTALLATION                    : N
DB_SCHEMA_PASSWORD                  : welcome1
DB_IP                               : 10.180.87.84
DB_PORT                             : 1521
DB_SERVICE_NAME                     : P8784A
IPM_USERNAME                        : weblogic
IPM_PASSWORD                        : weblogic1
FTP_IPM_USERNAME                    : ofssobp
FTP_IPM_PASSWORD                    : ofssobp123
FTP_IPM_BATCH_USERNAME              : ofssobp
FTP_IPM_BATCH_PASSWORD              : ofssobp123
Please take your time and go through the information printed above in detail.
If the above mentioned information is correct, please enter Y or y to proceed.  Press any other key to exit the installation.
```

Figure 3–11 Starting Post Installation (contd)

```
Please take your time and go through the information printed above in detail.
If the above mentioned information is correct, please enter Y or y to proceed.  Press any other key to exit the installation.
y
Post-installation will begin in sometime...
The authenticity of host '10.180.6.143 (10.180.6.143)' can't be established.
RSA key fingerprint is 36:d8:2d:c8:3f:d1:c3:4e:cd:38:f7:19:48:be:33:8c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.180.6.143' (RSA) to the list of known hosts.
ofssobp@10.180.6.143's password:
i18nAPI_v3.jar                                                                                100%  904KB 904.4KB/s   00:00
i18nAPI_v3.jar copied from BIP machine
ofssobp@10.180.6.143's password:
xdocore.jar                                                                                   100% 9060KB   8.9MB/s   00:00
xdocore.jar copied from BIP machine
ofssobp@10.180.6.143's password:
versioninfo.jar                                                                               100% 6204KB   6.1MB/s   00:00
versioninfo.jar copied from BIP machine
ofssobp@10.180.6.143's password:
imaging-client.jar                                                                            100%  863KB 863.3KB/s   00:00
imaging-client.jar copied from IPM machine
ofssobp@10.180.6.143's password:
oracle.ucm.ridc-11.1.1.jar                                                                    100%  619KB 618.9KB/s   00:00
oracle.ucm.ridc-11.1.1.jar copied from IPM machine
base_domain
*******************************************************
** Setting up SOA specific environment...
*******************************************************
EXTRA_JAVA_PROPERTIES= -da:org.apache.xmlbeans...
.
LD_LIBRARY_PATH=::/scratch/app/product/fmw/wlserver/server/native/linux/x86_64:/scratch/app/product/fmw/wlserver/server/native/linux/x86_64/oci920_8
.
.
*******************************************************
** End SOA specific environment setup
*******************************************************
Logging WLS stderr to /scratch/app/product/fmw/user_projects/domains/base_domain/servers/AdminServer/stderr.log
Verifying OBP_ORACLE_HOME /scratch/app/product/fmw/obpinstall/obp
Buildfile: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/replace.xml
```

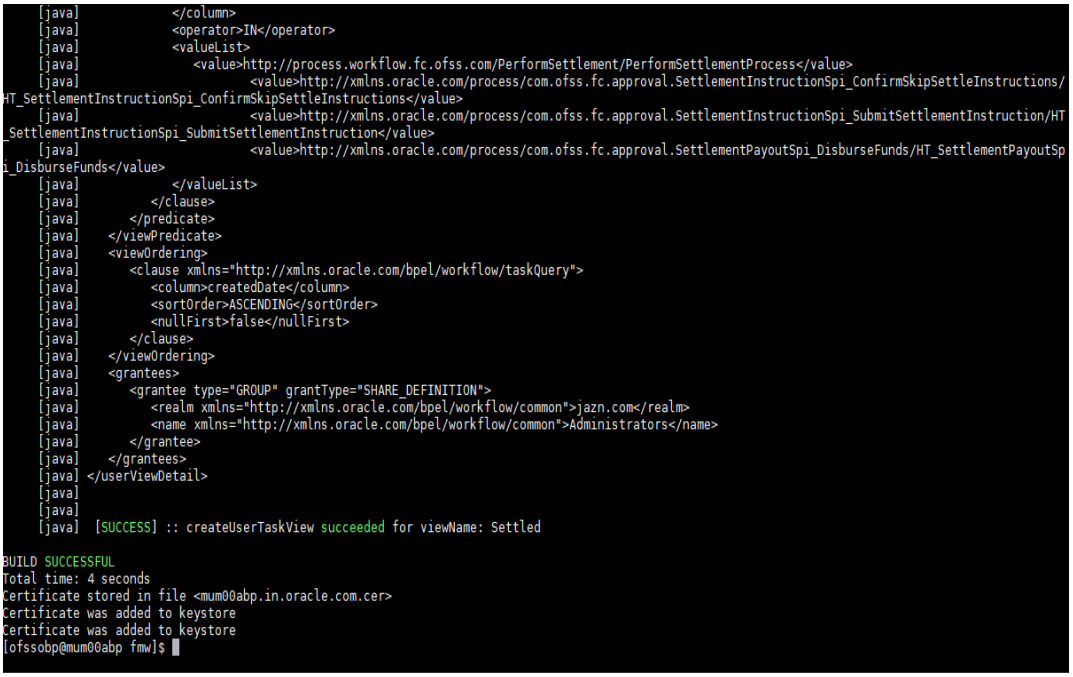
Figure 3–12 Starting Post Installation (contd)

```
Buildfile: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/replace.xml

replace:
    [unzip] Expanding: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/Metadata_soa.zip into /scratch/app/product/fmw/obpinstall/obp/o
b.soa.process/metadata/metadata
    [unjar] Expanding: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/metadata/sharedResources.jar into /scratch/app/product/fmw/obpi
nstall/obp/ob.soa.process/metadata/metadata/sharedResources
   [delete] Deleting: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/metadata/sharedResources.jar
      [jar] Building jar: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/metadata/sharedResources.jar
      [zip] Building zip: /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/Metadata_updated.zip
   [delete] Deleting directory /scratch/app/product/fmw/obpinstall/obp/ob.soa.process/metadata/metadata

BUILD SUCCESSFUL
Total time: 10 seconds
Archive:  BPELRecoveryConfig.zip
  inflating: recoveryconfig.sh
  inflating: BPELRecoveryConfig.jar
50
Updating RecurringScheduleConfig.maxMessageRaiseSize from 50 to 0
Updating StartupScheduleConfig.maxMessageRaiseSize from 50 to 0
javax.management.openmbean.CompositeDataSupport(compositeType=javax.management.openmbean.CompositeType(name=RecurringScheduleConfig,items=((itemName=m
axMessageRaiseSize,itemType=javax.management.openmbean.SimpleType(name=java.lang.Integer)),(itemName=startWindowTime,itemType=javax.management.openmbe
an.SimpleType(name=java.lang.String)),(itemName=stopWindowTime,itemType=javax.management.openmbean.SimpleType(name=java.lang.String)),(itemName=subseq
uentTriggerDelay,itemType=javax.management.openmbean.SimpleType(name=java.lang.Long)),(itemName=threshHoldTimeInMinutes,itemType=javax.management.open
mbean.SimpleType(name=java.lang.Integer)))),contents={maxMessageRaiseSize=0, startWindowTime=00:00, stopWindowTime=23:59, subsequentTriggerDelay=300,
threshHoldTimeInMinutes=10})
null
null
javax.management.openmbean.CompositeDataSupport(compositeType=javax.management.openmbean.CompositeType(name=RecoveryConfig,items=((itemName=ClusterCon
fig,itemType=javax.management.openmbean.CompositeType(name=ClusterConfig,items=((itemName=clusterDbTimeRefresh,itemType=javax.management.openmbean.Sim
pleType(name=java.lang.Long)),(itemName=heartBeatInterval,itemType=javax.management.openmbean.SimpleType(name=java.lang.Long)),(itemName=masteAliveThr
eshold,itemType=javax.management.openmbean.SimpleType(name=java.lang.Long)),(itemName=nodeReapInterval,itemType=javax.management.openmbean.SimpleType(
name=java.lang.Long)),(itemName=nodeReapThreshold,itemType=javax.management.openmbean.SimpleType(name=java.lang.Long))))),(itemName=RecurringScheduleC
onfig,itemType=javax.management.openmbean.CompositeType(name=RecurringScheduleConfig,items=((itemName=maxMessageRaiseSize,itemType=javax.management.op
enmbean.SimpleType(name=java.lang.Integer)),(itemName=startWindowTime,itemType=javax.management.openmbean.SimpleType(name=java.lang.String)),(itemName
=stopWindowTime,itemType=javax.management.openmbean.SimpleType(name=java.lang.String)),(itemName=subsequentTriggerDelay,itemType=javax.management.open
mbean.SimpleType(name=java.lang.Long)),(itemName=threshHoldTimeInMinutes,itemType=javax.management.openmbean.SimpleType(name=java.lang.Integer))))),(i
temName=StartupScheduleConfig,itemType=javax.management.openmbean.CompositeType(name=StartupScheduleConfig,items=((itemName=maxMessageRaiseSize,itemTy
```

Figure 3–13 SOA Post Installation Completion



6. For monitoring the script run, check the following log files created under the SOA domain directory:

   deploy-composite-SOA-WLST.log

   post-obp-SOA-WLST.log

   post-soa-GrantAndPolicySet-log.log

   post-soa-taskflow-grants.log

   update-syncMaxTimeWait.log

   obp-soa-install-log.txt

7. Deselect the following flag for all the OBDLOCS data sources:

   a. Log in to weblogic console
   b. Navigate to Data Sources > datasource name (eg. OBP_SYS_CONFIG) > Connection Pool > Advanced.
   c. Deselect the **Remove Infected Connections Enabled** check box.
   d. Add below parameter in obphumantask server memory parameters in setStartupEnv.sh

      -Dweblogic.servlet.DIDisabled=true.

   e. Restart SOA admin and SOA managed server and obphumantask server.

4 OBDLOCS US Localization Host Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Deposits and Lines of Credit Servicing US Localization Host Media Pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

4.1 Installation and Configuration Procedure

This section details the installation procedure for the OBDLOCS US Localization Host Media Pack.

4.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBDLOCS US Localization Host Media Pack installation.

Step 1 Procuring Installables

Download the appropriate host media pack from the following location:

http://edelivery.oracle.com/

Step 2 Extracting the Installables

Copy the 'obpus-host.zip' to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Below files will be extracted:

- The zip file:
  - 'obpinstall-host.zip'
  - 'Table_Partitioning.zip'
- The installation script:
  - 'installobphost.sh'
  - 'ossh.sh'
  - 'ossh.sh'
  - 'load-artifacts.sh'
- The install configuration property file 'installobphost.properties'
- dbScripts_us.tar.gz

Step 3 Printing Checklists

Take a printout of the installation checklist mentioned in Section 2.4 Installation Checklist of this guide and note the values applicable for each point in the last column for “Value” so that the same is handy during the actual installation.

4.1.2 Pre-Installation Steps

This section lists the pre-installation steps required for the OBDLOCS US Localization Host Media Pack installation. The procedure can be started after SOA pre-installation steps are executed.

Following are the domains for XD components of middleware. Domain for batchhost must be created first and then others (no sequence for others).

The following table lists the XD components.

Table 4–1 XD Components

Sr. No.	Name	Value	Description
1	XD_COMPONENT_NAME	batchhost	Value for batch host sever, Policy seeding and BIP reports upload will be done with this batch host server installation.
2	XD_COMPONENT_NAME	obepmhost	Value for OBEPM server (Product Manufacturing)
3	XD_COMPONENT_NAME	obcsdshost	Value for OBCSDS server (Deposits)
4	XD_COMPONENT_NAME	obpmhost	Value for OBPM server (Party)
5	XD_COMPONENT_NAME	obeprhost	Value for OBPR server (Pricing)
6	XD_COMPONENT_NAME	obeohost	Value for obccm server (LCM)

The following table shows examples of fmw dir name, domain name, server name, and memory parameters. Multiple domains can be created on a single VM according to memory parameters.

Table 4–2 Examples of FMW Dir Name, Domain Name, Server Name and Memory Parameters

XD Component Name	MW_HOME	Domain Name	Server Name or Cluster Name
batchhost	/scratch/app/product/fmw	host_ domain	obphost_ server1/obphost_ cluster1
obepmhost	/scratch/app/product/fmw_pm	obepm_ domain	obepm_ server1/obepm_ cluster1
obcsdshost	/scratch/app/product/fmw_deposits	deposits_ domain	deposits_ server1/deposits_ cluster1
obpmhost	/scratch/app/product/fmw_party	obparty_ domain	obparty_ server1/obparty_ cluster1
obeprhost	/scratch/app/product/fmw_pr	obpr_ domain	obpr_server1/obpr_ cluster1
obccmhost	/scratch/app/product/fmw_occm	occm_ domain	occm_server1/occm_ cluster1

Memory Parameters

1. **Batchhost:**
   - Admin Server: USER_MEM_ARGS="-Xms2g -Xmx4g"
   - Managed Server: USER_MEM_ARGS="-Xms8g -Xmx8g -XX:NewSize=2048m -XX:MaxNewSize=4096m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75"
2. **Other XD HOST:**
   - Admin Server: USER_MEM_ARGS="-Xms512m -Xmx512m"
   - Managed Server: USER_MEM_ARGS="-Xms1g -Xmx3g -XX:+UseG1GC -XX:ParallelGCThreads=8 -XX:ConcGCThreads=2 -XX:+UseStringDeduplication"

Batchhost Installation Steps

Following are the pre-installation steps for batchhost XD component.

Step 1 Updating installobphost.properties

Navigate to the directory where the files obpinstall-host.zip, installobphost.sh and installobphost.properties are placed and update installobphost.properties with relevant values from the checklist.

Value for below properties should be 'Y' in installobphost.properties for batchhost installation. For other XD host, value should be 'N'.

- OID_FARM_AND_POLICY_SEEDING_FLAG
- BIP_REPORTS_UPLOADING_FLAG

Step 2 Checklist for a new setup

Before initiating installation on a completely new setup, check the following:

- Please make sure required RCU schemas have been created. For more information, see Section 6.1 Pre-Installation Steps and Section 6.2 OBDLOCS Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against HOST_TARGET property.
- In case of re-installation ensure that the directory paths against DOMAIN_DIRECTORY_LOCATION, HOST_TARGET and HOST_MW_HOME specified in installobphost.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- No processes should be running on the port in HOST machine given in installobphost.properties.
- Values in installobphost.properties must be correct. At run time no option is given to change them.
- No other schema should exist in db with the same prefix as HOST_DB_SCHEMA_PREFIX specified in installobphost.properties. OBP_HOST_DB_USER should be given on the basis of HOST_DB_SCHEMA_PREFIX.

  For example, if HOST_DB_SCHEMA_PREFIX is DEV, then OBP_HOST_DB_USER should be DEV_OBP.
- OID_DOMAIN_NAME in installobphost.properties should match with the OID_DOMAIN_NAME given in installobpui.properties. Any other domain with the same name must not exist in OID. The domain in OID will be created in host pre-install.

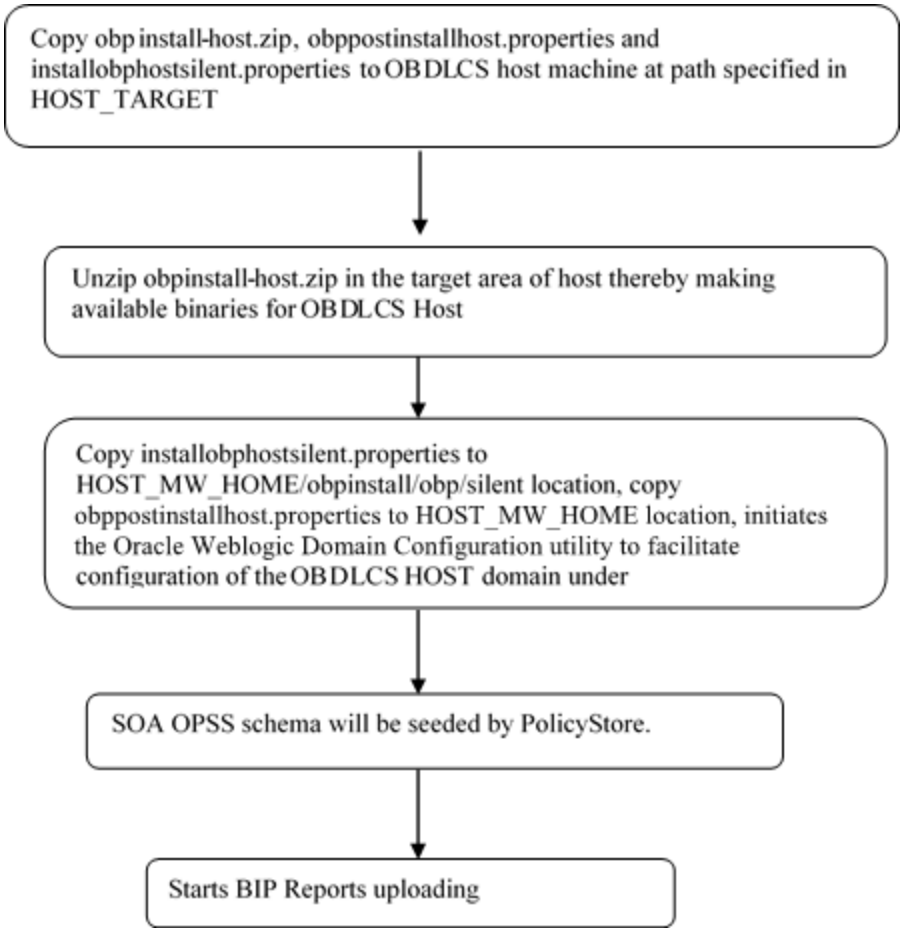
- OBP_HOST_DB_USER and BIP_DATASOURCE_NAME must be same in installobphost.properties.
- The following schemas are manually created prior to installation and are available for updation in the checklist:
  - OBP_HOST_DB_USER (by RCU)
- MDS_HOST_DB_USER as updated in installobphost.properties and MDS_SCHEMA_USER as updated in installobpui.properties should point to the same MDS db schema.

4.1.3 Installation Steps

This section lists the installation steps required for the OBDLOCS US Localization Host Media Pack installation.

1. Navigate to the directory where the media pack files are placed and execute installobphost.sh. The installation script shall echo the values entered in the installobphost.properties file and ask for confirmation to go ahead with the installation.
2. The installation script automatically triggers the following significant steps using secure remote copy 'scp' command and remote shell commands execution using the 'ssh' command.

Figure 4–1 Steps in installobphost.sh script



A sample output is given here.

Figure 4–2 Verification of Properties

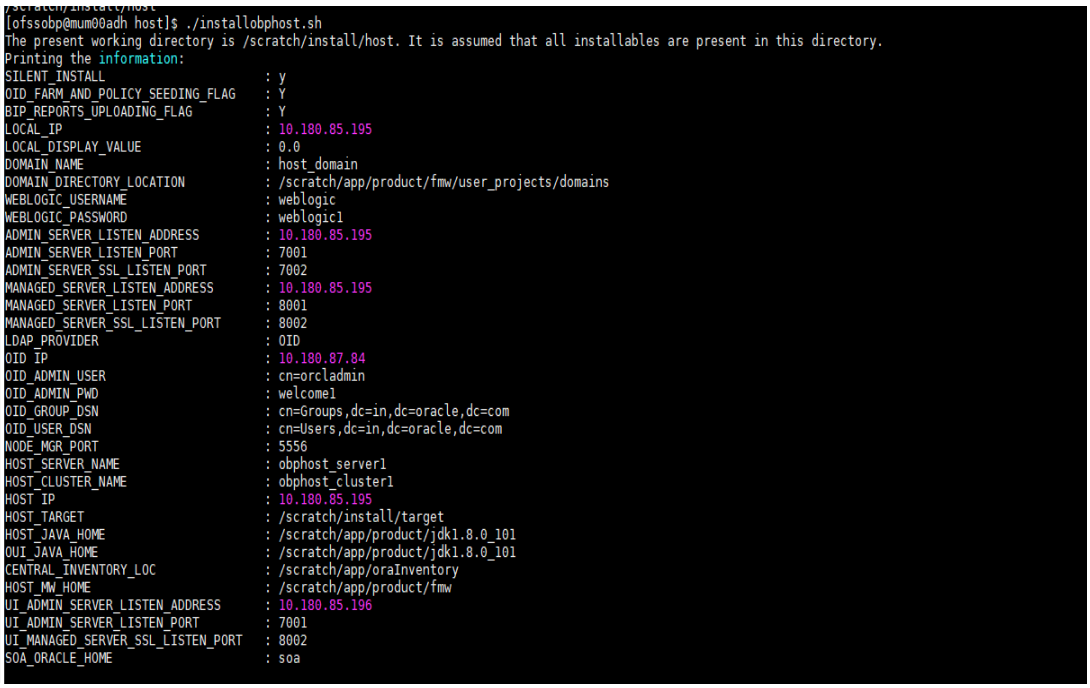


Figure 4–3 Verification of Properties (contd)

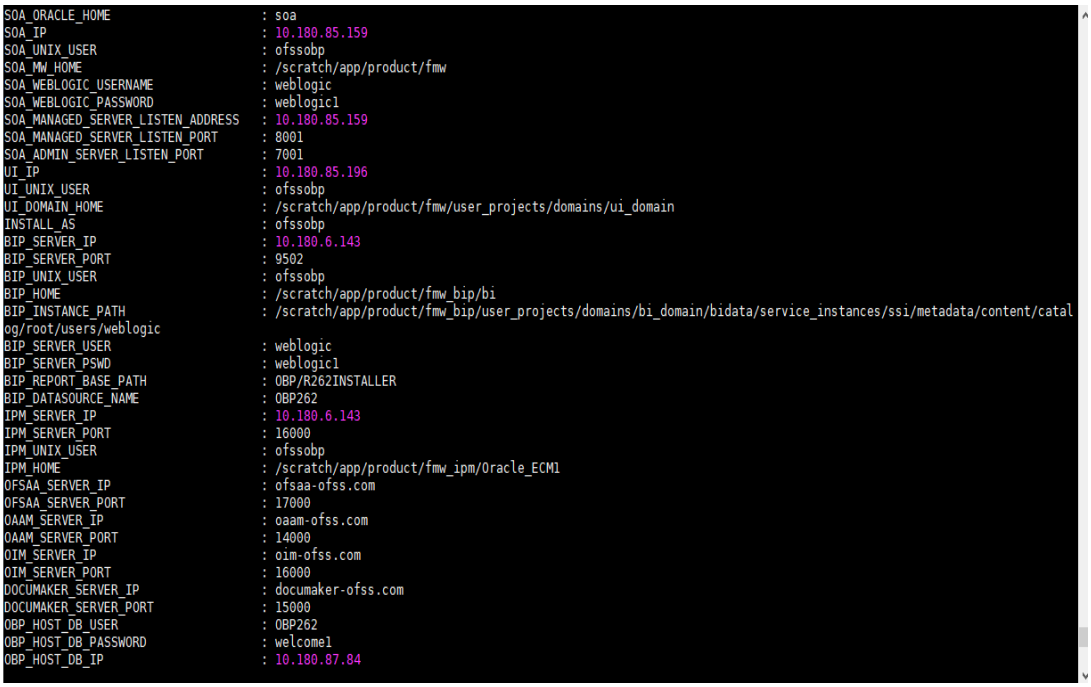


Figure 4–4 Verification of Properties (contd)

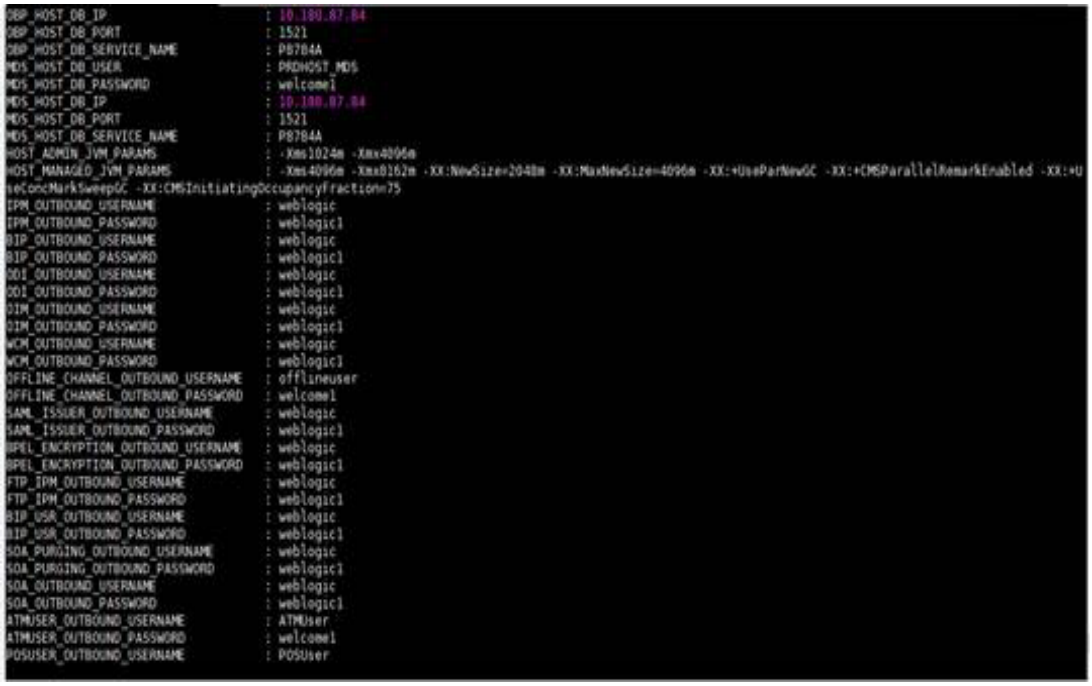
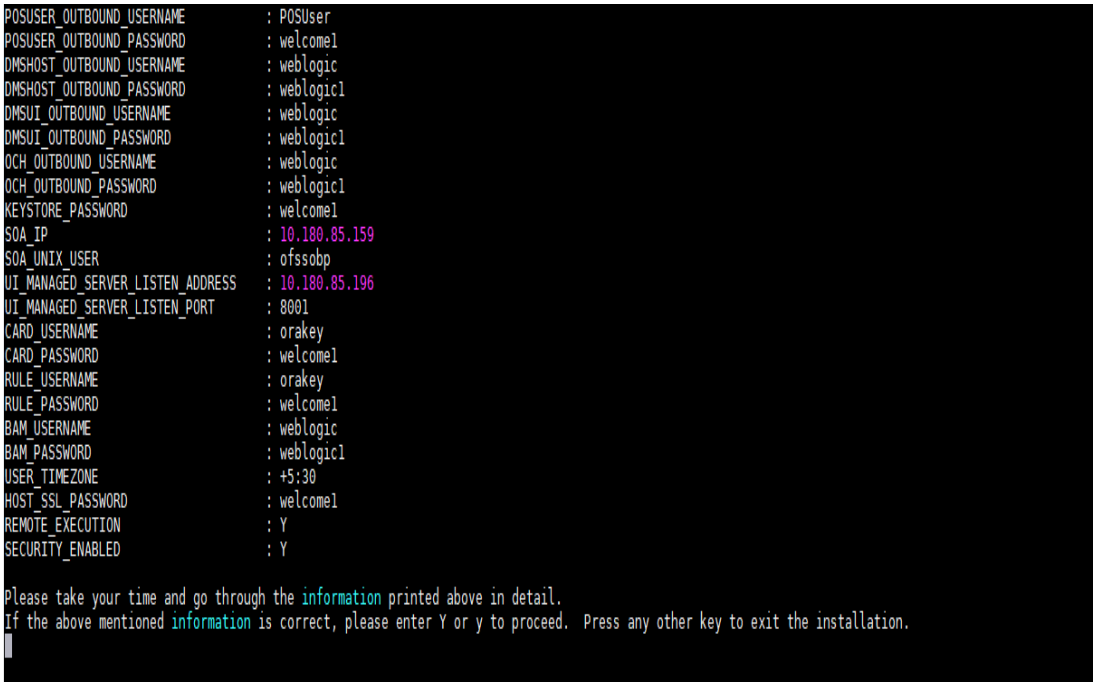


Figure 4–5 Verification of Properties (contd)



3. Verify the value of each property carefully before proceeding.
4. If all values are correct, then enter 'Y' or 'y' and press Enter to initiate the installation. The installation

utility performs the installation and domain is created silently.

Figure 4–6 Confirmation and Copying of Installables to Target Machine

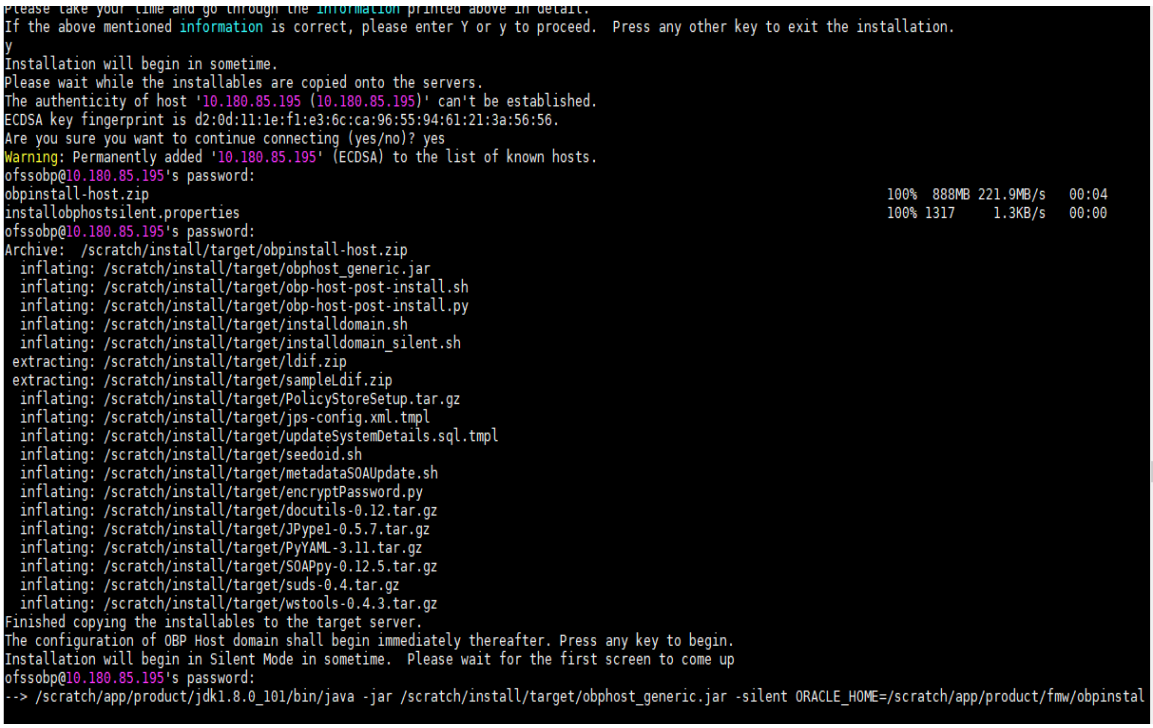


Figure 4–7 Confirmation and Copying of Installables to Target Machine (contd)

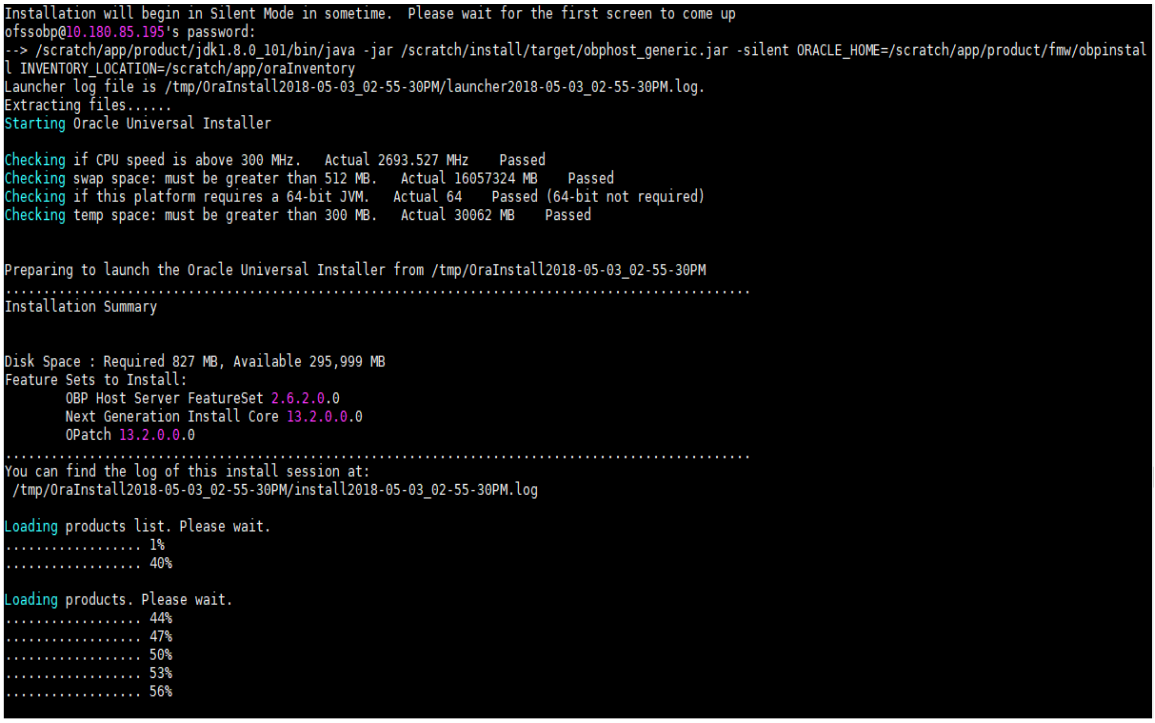
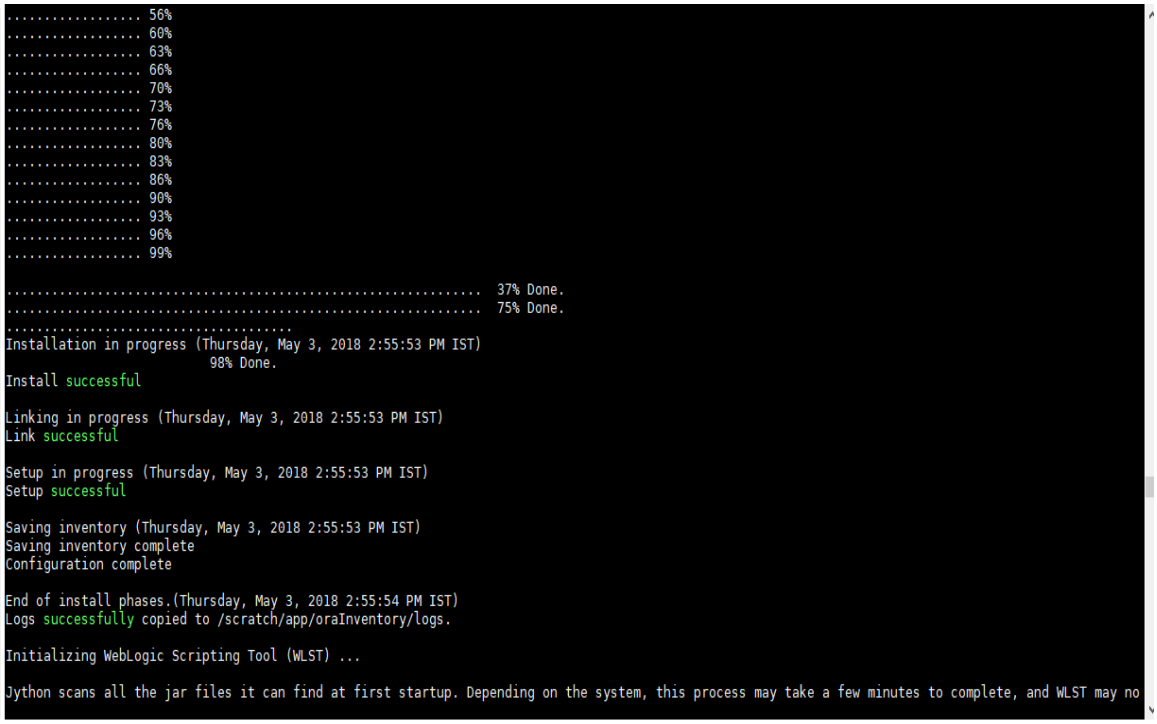
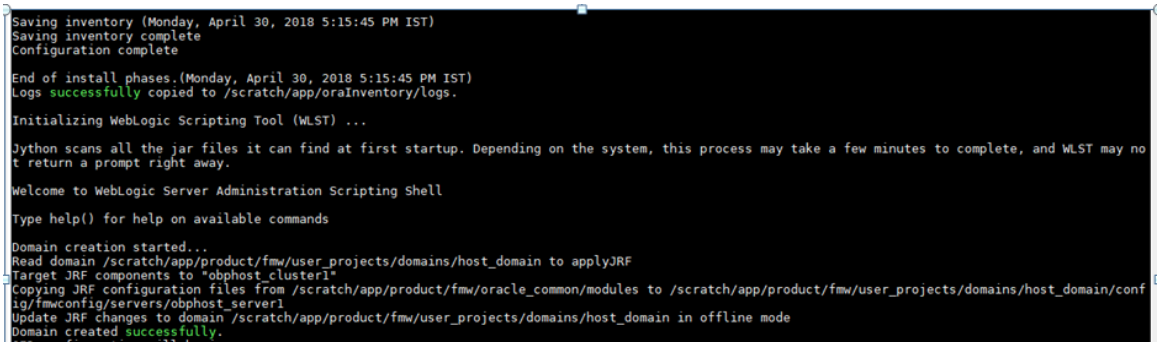


Figure 4–8 Confirmation and Copying of Installables to Target Machine (contd)



5. After copying, there is host DB schema creation and seeding. After extracting the installables, the domain gets installed and a confirmation message is shown.

Figure 4–9 Domain Installation Confirmation



6. After completion of domain installation, it will proceed to seeding.

Figure 4–10 Untar the policyStoreSetup and Copy on destination location

Figure 4–11 Untar the policyStoreSetup and Copy on destination location (contd)

```
adf-controller-security.jar                                   100% 2255     2.2KB/s   00:00
jps-ee.jar                                                    100%   79KB  78.5KB/s   00:00
ojdl.jar                                                      100%  332KB 332.4KB/s   00:00
org.openliberty.openaz.azapi_1.1.jar                          100%   52KB  52.2KB/s   00:00
identitystore.jar                                             100%  471KB 471.3KB/s   00:00
identitydirectory.jar                                         100%  270KB 270.0KB/s   00:00
javax.security.jacc.jar                                       100%   51KB  51.0KB/s   00:00
jps-audit.jar                                                 100%  892KB 891.6KB/s   00:00
adf-share-security.jar                                        100%   22KB  22.0KB/s   00:00
jps-sidm-api.jar                                              100% 4326     4.2KB/s   00:00
jps-common.jar                                                100% 1519KB   1.5MB/s   00:00
dms.jar                                                       100% 2253KB   2.2MB/s   00:00
jps-internal.jar                                              100% 6636KB   6.5MB/s   00:00
osdt_saml2.jar                                                100%  281KB 280.9KB/s   00:00
identityutils.jar                                             100%  211KB 210.8KB/s   00:00
javax.faces.jsf-api.jar                                       100%  355KB 355.3KB/s   00:00
eclipselink.jar                                               100% 8865KB   8.7MB/s   00:00
jps-az-common.jar                                             100%  407KB 407.0KB/s   00:00
fmw_audit.jar                                                 100% 1148     1.1KB/s   00:00
osdt_wss.jar                                                  100%  186KB 186.4KB/s   00:00
osdt_ws_sx.jar                                                100%  241KB 240.8KB/s   00:00
jps-az-management.jar                                         100%  314KB 314.4KB/s   00:00
oraclepki.jar                                                 100%  295KB 295.4KB/s   00:00
ojdbc6dms.jar                                                 100% 4325KB   4.2MB/s   00:00
UIComponentsDiagnosticHelper.sh                               100%  167     0.2KB/s   00:00
README_UPGRADE.txt                                            100% 5060     4.9KB/s   00:00
jps-config.xml(db)                                            100% 4324     4.2KB/s   00:00
jps-config.xml                                                100% 4331     4.2KB/s   00:00
refreshMatrixAuthPolicies.sh                                  100%   39     0.0KB/s   00:00
PolicyMigrator.sh                                             100%  170     0.2KB/s   00:00
Connection to 10.180.85.195 closed.
ofssobp@10.180.85.195's password:
ofssobp@10.180.85.195's password:
seedOIDDomain.sh                                              100% 1427     1.4KB/s   00:00
ofss-oid-silent-seedOIDDomain.py                              100% 5013     4.9KB/s   00:00
createDummyDomainAndStartSeedingOID.sh                        100%  828     0.8KB/s   00:00
oid-configure-silent.properties                               100%  352     0.3KB/s   00:00
ofss-oid-silent-createOIDDomain.py                            100% 2533     2.5KB/s   00:00
```

Figure 4–12 Untar the policyStoreSetup and Copy on destination location (contd)

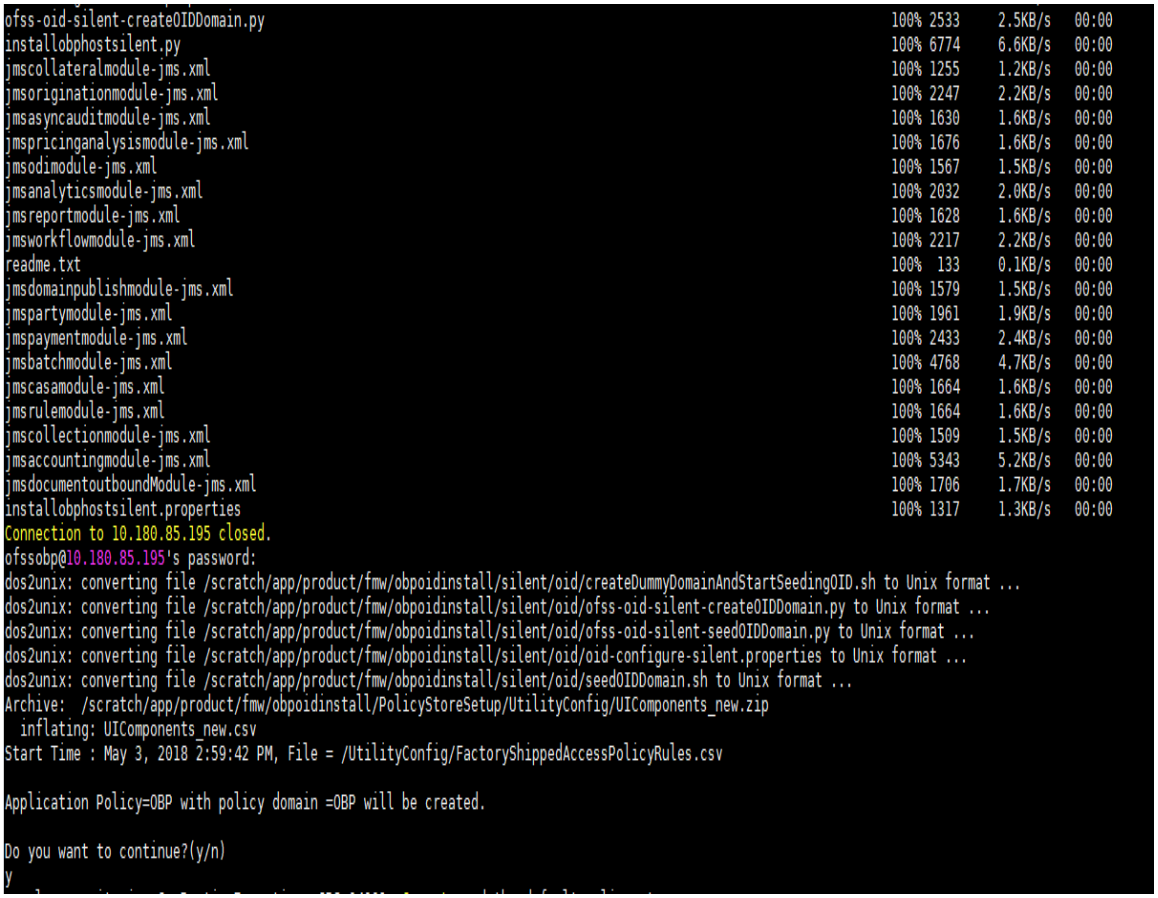


Figure 4–13 Policy Seeding

Figure 4–14 Policy Seeding (contd)

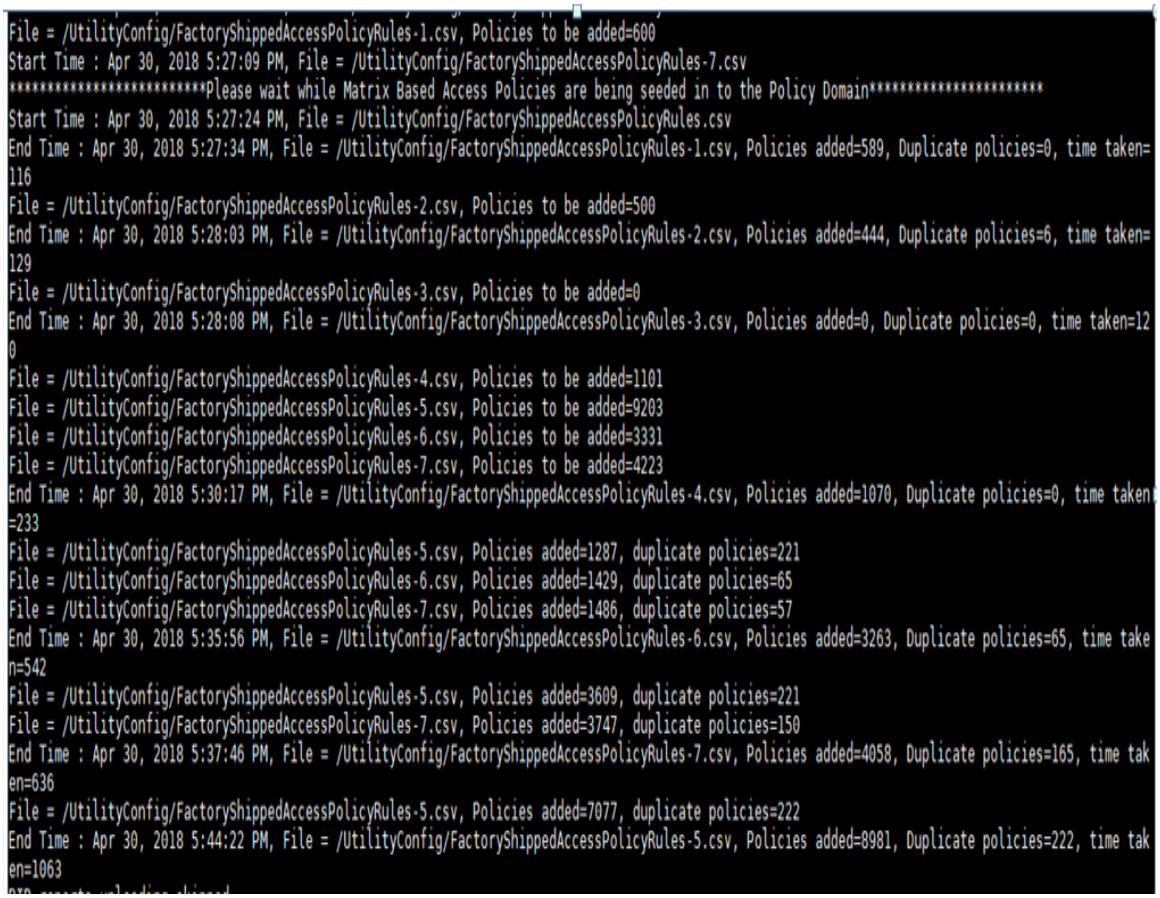


Figure 4–15 BIP Reports Upload

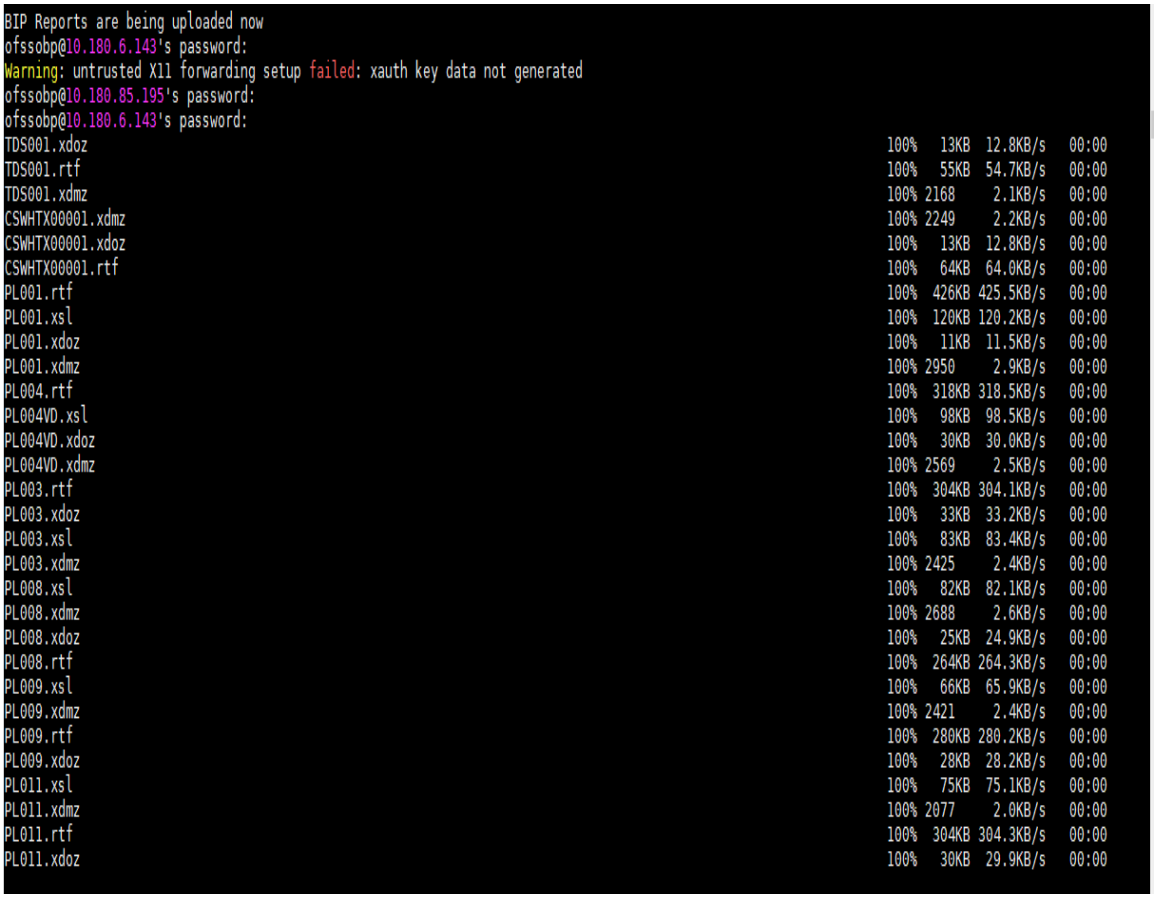
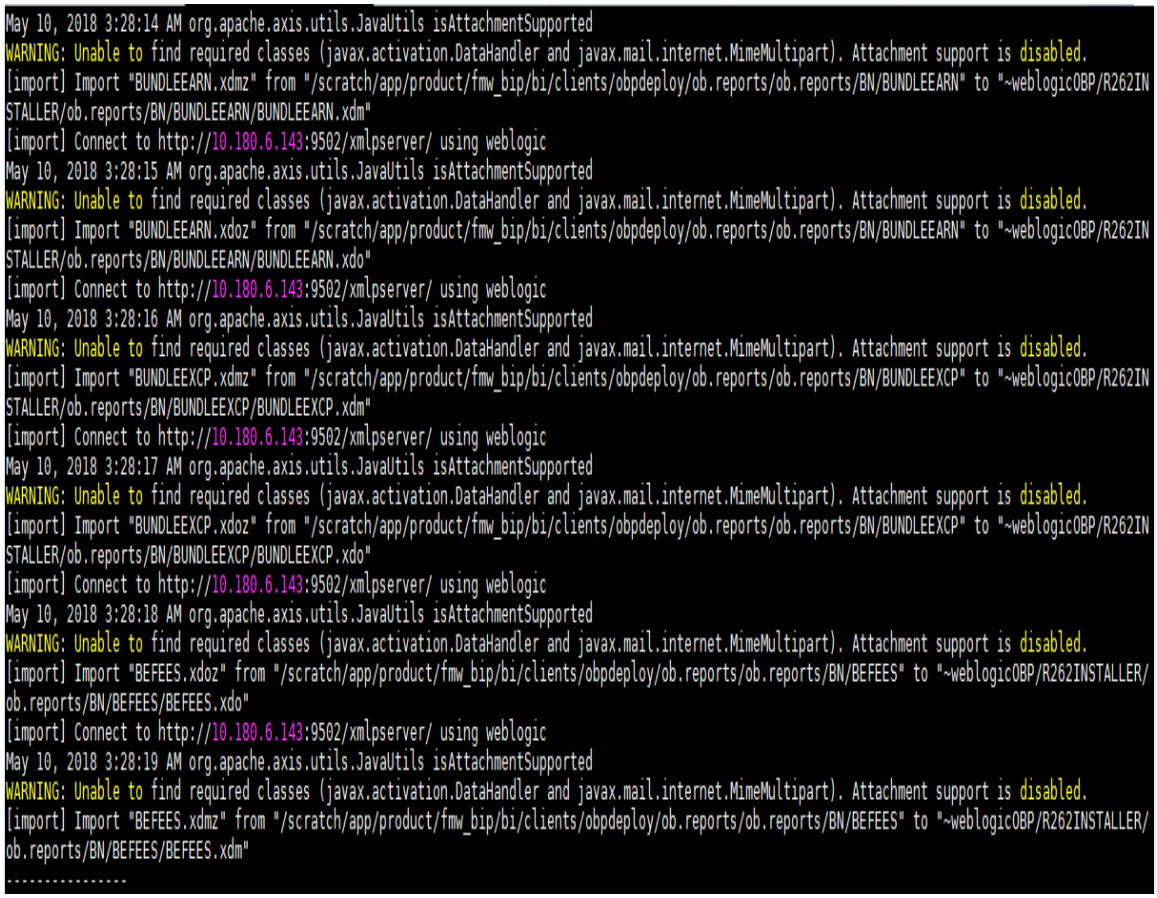


Figure 4–16 BIP Reports Upload (contd)

```
ofssobp@10.180.6.143's password:
Warning: untrusted X11 forwarding setup failed: xauth key data not generated
Archive:  /scratch/app/product/fmw_bip/bi/clients/bipublisher/reportscripts.zip
  inflating: /scratch/app/product/fmw_bip/bi/clients/bipublisher/ngpUploadReports.sh
  inflating: /scratch/app/product/fmw_bip/bi/clients/bipublisher/ngpUpdateUrlAndDataSource.sh
mkdir: cannot create directory `fc_lib': File exists
[import] Connect to http://10.180.6.143:9502/xmlpserver/ using weblogic
May 10, 2018 3:20:14 AM org.apache.axis.utils.JavaUtils isAttachmentSupported
WARNING: Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart). Attachment support is disabled.
[import] Import "BR106.xdmz" from "/scratch/app/product/fmw_bip/bi/clients/obpdeploy/ob.reports/ob.reports/TP/BR106" to "~weblogicOBP/R262INSTALLER/ob
.reports/TP/BR106/BR106.xdm"
[import] Connect to http://10.180.6.143:9502/xmlpserver/ using weblogic
May 10, 2018 3:20:15 AM org.apache.axis.utils.JavaUtils isAttachmentSupported
WARNING: Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart). Attachment support is disabled.
[import] Import "BR106.xdoz" from "/scratch/app/product/fmw_bip/bi/clients/obpdeploy/ob.reports/ob.reports/TP/BR106" to "~weblogicOBP/R262INSTALLER/ob
.reports/TP/BR106/BR106.xdo"
[import] Connect to http://10.180.6.143:9502/xmlpserver/ using weblogic
May 10, 2018 3:20:16 AM org.apache.axis.utils.JavaUtils isAttachmentSupported
WARNING: Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart). Attachment support is disabled.
[import] Import "BR105.xdoz" from "/scratch/app/product/fmw_bip/bi/clients/obpdeploy/ob.reports/ob.reports/TP/BR105" to "~weblogicOBP/R262INSTALLER/ob
.reports/TP/BR105/BR105.xdo"
[import] Connect to http://10.180.6.143:9502/xmlpserver/ using weblogic
May 10, 2018 3:20:17 AM org.apache.axis.utils.JavaUtils isAttachmentSupported
WARNING: Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart). Attachment support is disabled.
[import] Import "BR105.xdmz" from "/scratch/app/product/fmw_bip/bi/clients/obpdeploy/ob.reports/ob.reports/TP/BR105" to "~weblogicOBP/R262INSTALLER/ob
.reports/TP/BR105/BR105.xdm"
```

Figure 4–17 BIP Reports Upload (contd)



Similar to above, perform pre-installation for other XD components.

If you are creating multiple domains on same VM, then change fmw path, domain path, ports, node manager port and so on.

OID POLICY SEEDING and BIP Reports upload will be done only once during batchhost installation.

4.1.4 Front End Processing Interface (FEPI) Installation Steps

Following are the basic steps for FEPI installation procedure:

Step 1 Installation

The installer will create a directory structure for FEPI as /scratch/app/product/fmw/obpinstall/obp/fepi

1. Change the paths in FEPI start scripts based on the environment.
2. Modify Start_fepi_atm.sh and Start_fepi_pos.sh located at /scratch/app/product/fmw/obpinstall/obp/fepi/scripts.
3. Change the property values in channels_atm.properties and channels_pos.properties based on the environment as follows:

Table 4–3 Properties

Property	Description	Example
BANK_CODE	Indicates the bank code	BANK_CODE=335
LISTENER_PORT	The port number on which FEPI server accepts incoming ISO message requests	LISTENER_PORT=9999
COMMAND_PORT	The port number on which FEPI server accepts command message Note: Need to specify an available valid port number, so that FEPI starts; it is a feature of native code and currently no messages are sent.	COMMAND_PORT=9998
ISO_TRACE_FILE_AREA	The location for ATM Trace logs	ISO_TRACE_FILE_ AREA=/scratch/app/product/fmw/obpinstall /obp/fepi/logs/ATMTRACE
FNDI.FJ.java.naming.provider.url	The IP address and port number on which WebLogic accepts requests	FNDI.FJ.java.naming.provider.url =t3://10.180.9.108:7001

4. Start ATM and POS FEPI.
5. On prompt enter WebLogic login credentials. For example, $ sh start_fepi_atm.sh.

Step 2 ATM and POS Trace logs

The Trace logs are available in the logs folder. For example, the trace logs can be located at /oracle/deployables/iut2/fepi/logs.

Additionally, fepi-console and fepi-ofss logs are also stored at the above location for ATM and POS FEPI server.

Step 3 module.channel or cz.module.channel enabling of logs

This is not related to FEPI, and these logs (host logs) are controlled by logging.xml of the WebLogic server.

Step 4 Multiple Instances

Currently, there are two instances of FEPI which are ATM and POS. Each instance has the following set of individual files along with the common shared files. For example, for the ATM FEPI server, the files are as follows:

Table 4–4 Examples of files

File Name	Description
channels_atm.properties	Configuration file
fepi_atm.logging.xml	Logging configuration file
start_fepi_atm.sh	Start script
stop_fepi_atm.sh	Stop script

4.2 Post Installation Configuration

This section describes the post installation configuration procedure for OBDLOCS US Localization Host Media Pack. The procedure can be started after SOA pre- installation and standalone database setup steps are executed.

Checklist for Post Installation Procedure

Before proceeding with the post installation procedure for the host, ensure the following:

- Node manager is not running and no other process is running on NODE_MGR_PORT.
- Host db schema creating and seeding has been done.

  For more information , see Section 6.3.3 HOST DB Schema Seeding and Section 6.3.4 System Configuration DB Update Script Execution.
- The node manager port should be free. You can verify this using the following command, where 5556 is the Node Manager Port.

  ```
  $netstat -na | grep 5556
  ```

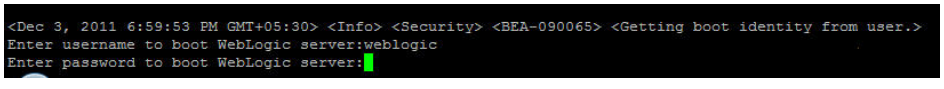
Post Installation Configuration

1. Start the domain admin WebLogic server by executing the startWebLogic.sh script in the host domain directory.

   ```
   cd <middleware home>
   cd user_projects/domains/obphostdomain/bin
   ./startWebLogic.sh
   ```

2. Enter the username and password to ensure that the WebLogic server starts.

   Figure 4–18 Host Domain Admin Server Credentials

3. Once the server status changes to RUNNING, proceed to execute the post installation script for Host

domain located under middleware. This script performs a multitude of configurations such as:

- Making changes in OBDLOCS config properties to point to the appropriate integration server (Example: Setting the BIP server URL)
- Setting the security realm properties of WebLogic domain and reassociating the same to the OID
- Trust configuration setup using the trust keys copied from the SOA domain

> **Note**
>
> Ensure that Oracle IPM application is running as during post install of OBDLOCS host. There is a call to the same for creating OBDLOCS content applications.

4. Navigate to the middleware home and list the files in the directory. A post installation and configuration script named obp-host-post-install.sh will be listed along with other files and directories.
5. Execute the script using the following command:

   ```
   ./obp-host-post-install.sh
   ```

6. For monitoring the script run, check the following log files created under the UI domain directory:
   - obp-host-install-log.txt
   - obp-host-install-log-py.txt

> **Note**
>
> The output shown here is a sample output and may vary slightly from the original output.

Figure 4–19 Host Domain Post Installation Script Execution

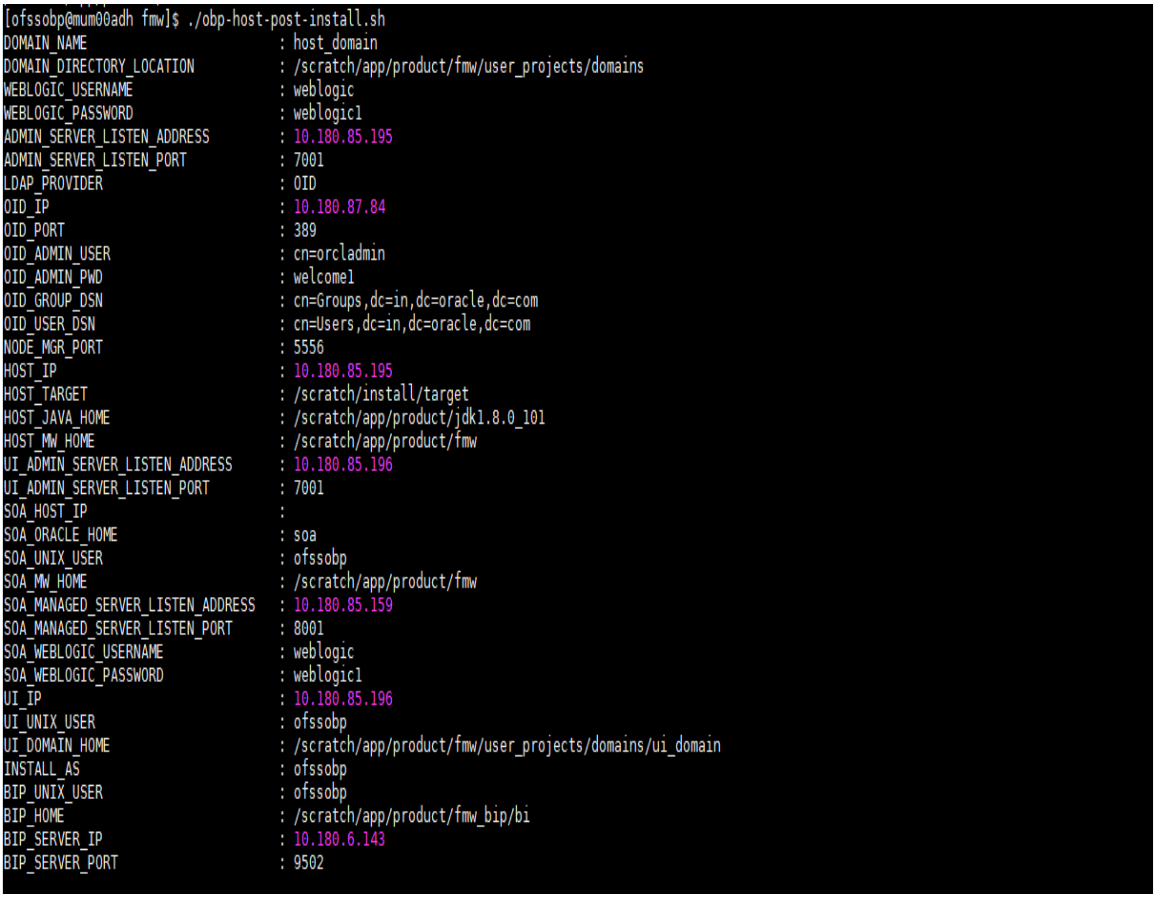


Figure 4–20 Host Domain Post Installation Script Execution (contd)

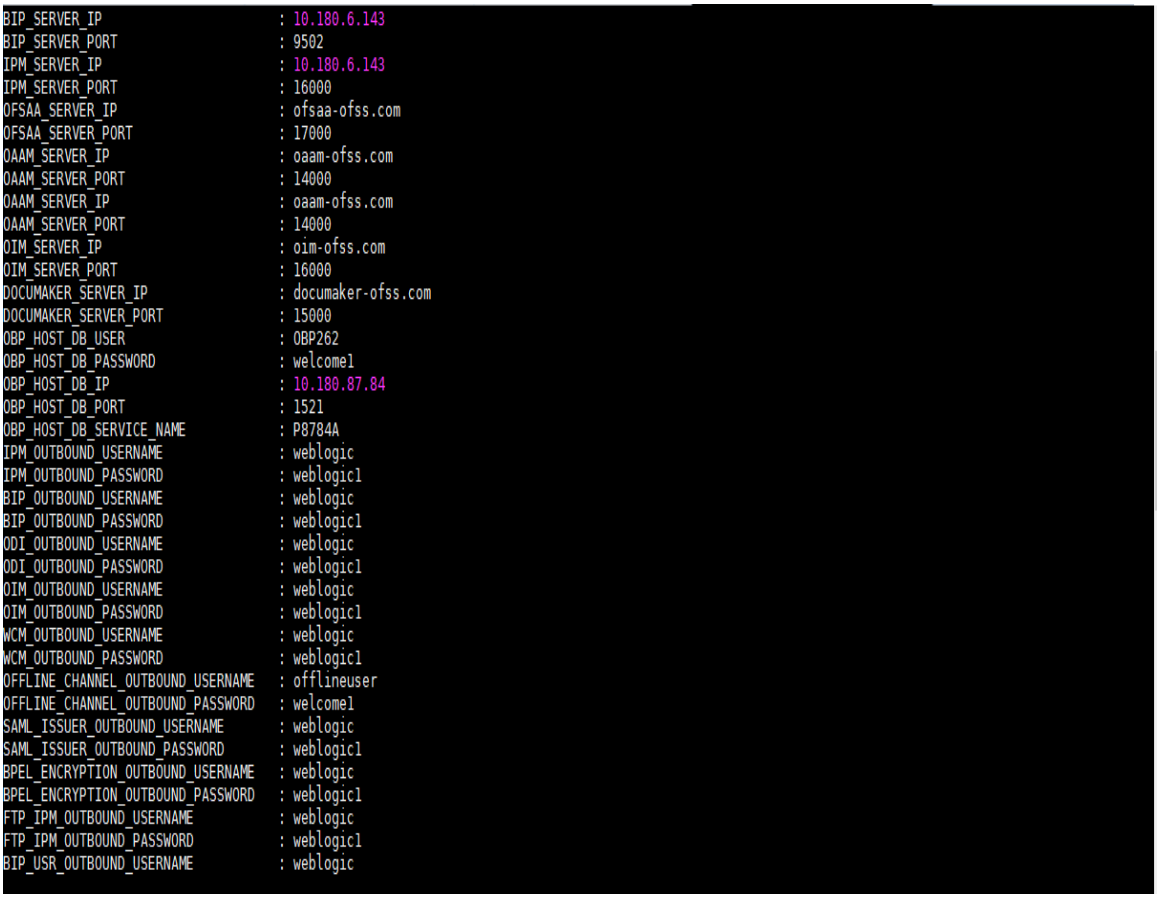


Figure 4–21 Host Domain Post Installation Script Execution (contd)

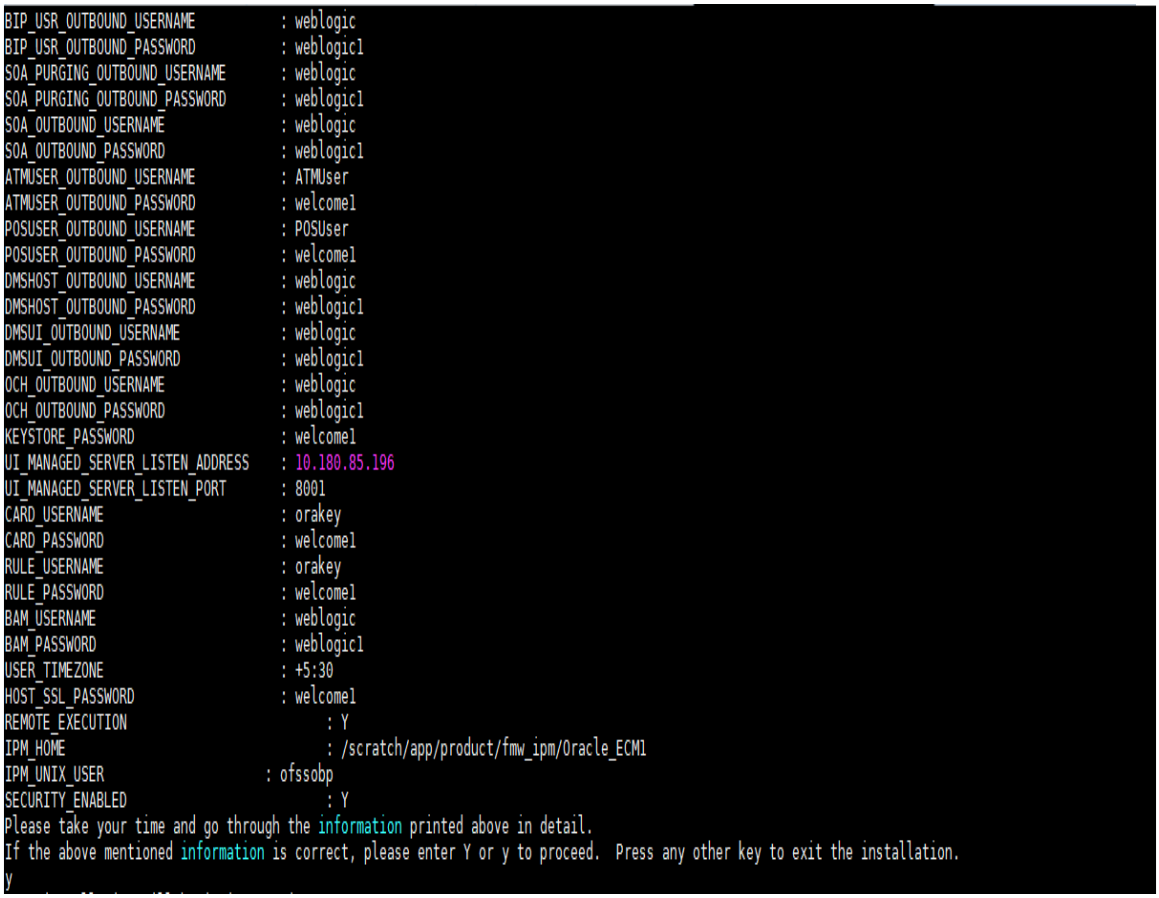


Figure 4–22 Host Domain Post Installation Script Execution (contd)

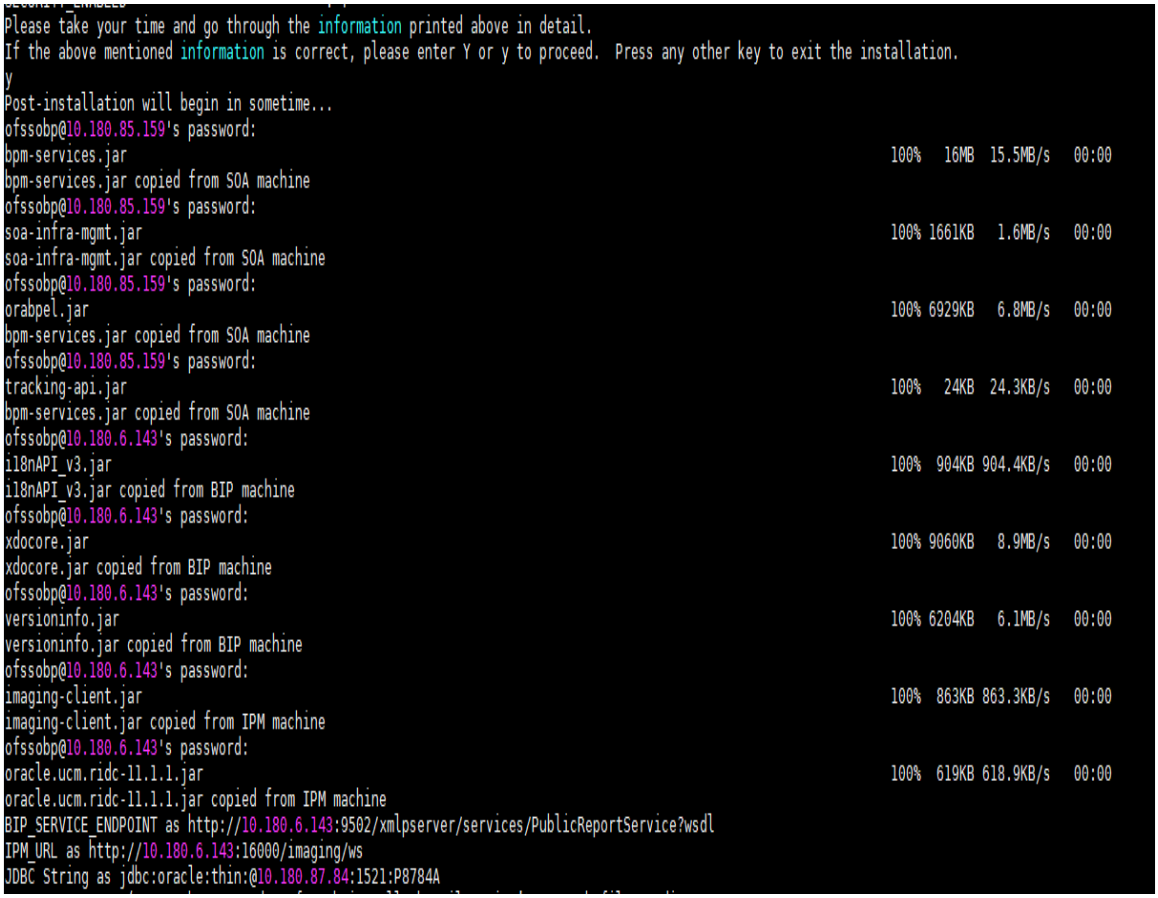
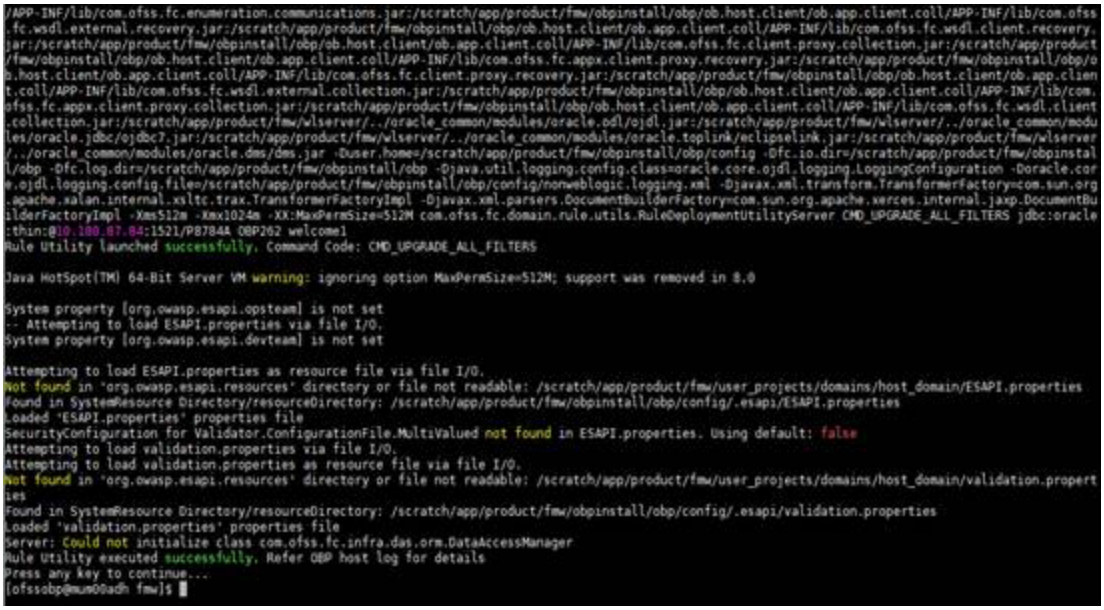


Figure 4–23 Host Domain Post Installation Script Execution Summary



7. After completion of the host post installation, it will return to the command prompt.
8. Finally inside logging.xml file for managed servers,

   for example: /scratch/app/product/fmw/user_projects/domains/host_ domain/config/fmwconfig/servers/obphost_server1/logging.xml

   within the following xml tag:

   <logging_configuration> <log_handlers> </log_handlers></logging_configuration>

   add:

   ```
   <log_handler name='el-handler' level='TRACE:32'
   class='oracle.core.ojdl.logging.ODLHandlerFactory'>
   <property name='path' value='${fc.log.dir}/logs/eclipselink.log' />
   <property name='maxFileSize' value='10485760' />
   <property name='maxLogSize' value='104857600' />
   <property name='encoding' value='UTF-8' />
   <property name='useThreadName' value='true' />
   <property name='supplementalAttributes'
   value='J2EE_APP.name,J2EE_MODULE.name,WEBSERVICE.name,WEBSERVICE_
   PORT.name,composite_instance_id,component_instance_id,composite_
   name,component_name' />
   </log_handler>
   ```

9. Within the following xml tag:

<logging_configuration><loggers></loggers></logging_configuration>

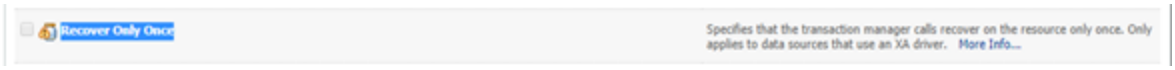
add:

```
<logger name='org.eclipse.persistence' level='TRACE:32'
useParentHandlers='false'>
<handler name='el-handler' />
</logger>
<logger name='javax.persistence' level='TRACE:32'
useParentHandlers='false'>
<handler name='el-handler' />
</logger>
```

10. Deselect the following flag for all the OBDLOCS data sources:

    a. Log in to weblogic console.
    b. Navigate to Data Sources > datasource name (eg. OBP_SYS_CONFIG) > Connection Pool > Advanced.
    c. Deselect the **Remove Infected Connections Enabled** check box.

11. Select the **Recover Only Once** for ONLY XA datasource (OBP_HOST_DS_XA) for all middleware servers.



    a. Log in to weblogic console.
    b. Navigate to Data Sources > datasource name (OBP_HOST_DS_XA) > Transaction.
    c. Select the **Recover Only Once** check box.

12. Then start the admin and managed servers to check the domain configuration status as described in verification part in Section 11.2 Host Domain Verification.

Similar to the above batchhost post installation, perform post installation for other XD components.

5 OBDLOCS US Localization Presentation Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation (UI) Media Pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

5.1 Installation and Configuration Procedure

This section details the installation procedure for the Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation Media Pack.

5.1.1 Preparatory Steps

This section lists the preparatory steps required for the Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation Media Pack installation.

Step 1 Procuring Installables

Download the appropriate presentation media pack from the following location:

http://edelivery.oracle.com/

Step 2 Extracting the Installables

Copy the 'obpus-ui.zip' to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Three files will be extracted:

- A zip file 'obpinstall-ui.zip'
- The installation script 'installobpui.sh'
- The install configuration property file 'installobpui.properties'

Step 3 Printing Checklists

Take a printout of the installation checklist mentioned in Section 2.4 Installation Checklist of this guide and note the values applicable for each point in the last column for 'Value' so that the same is handy during the actual installation.

5.1.2 Pre-Installation Steps

This section lists the pre-installation steps required for the Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation Media Pack installation. The procedure can be started after SOA pre-installation steps are executed.

Step 1 Updating installobpui.properties

Navigate to the directory where the files obpinstall-ui.zip, installobpui.sh and installobpui.properties are placed and update installobpui.properties with relevant values from the checklist.

Step 2 Checklist for a new setup

Before initiating installation on a completely new setup, check the following:

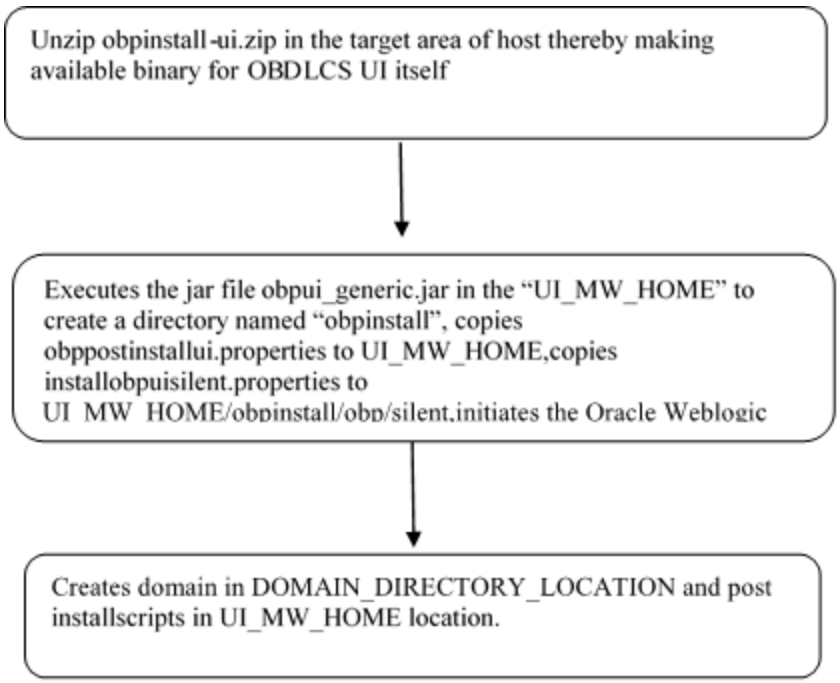
- Make sure required RCU schemas have been created. For more information, see Section 6.1 Pre-Installation Steps and Section 6.2 OBDLOCS Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against UI_TARGET property.
- In case of a re-installation ensure that the directory paths against DOMAIN_DIRECTORY_ LOCATION, HOST_TARGET and HOST_MW_HOME specified in installobpui.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- No processes should be running on the port in HOST machine given in installobpui.properties.
- MDS_SCHEMA_USER schema given in the installobpui.properties exists. This should point to the same schema as MDS_HOST_DB_USER of installobphost.properties.
- Values given in installobpui.properties must be correct. At run time, no option will be given to change the values.

5.1.3 Installation Steps

This section lists the installation steps required for the Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation Media Pack installation.

1. Navigate to the directory where the media pack files are placed and execute installobpui.sh. The installation script shall echo the values entered in the installobpui.properties file and ask for a confirmation to go ahead with the installation.
2. The installation script automatically triggers the following significant steps using secure remote copy ’scp’ command and remote shell commands execution using the ’ssh’ command.

Figure 5–1 Steps in installobpui.sh script



A sample output is given here.

Figure 5–2 Confirmation to Proceed Domain Installation

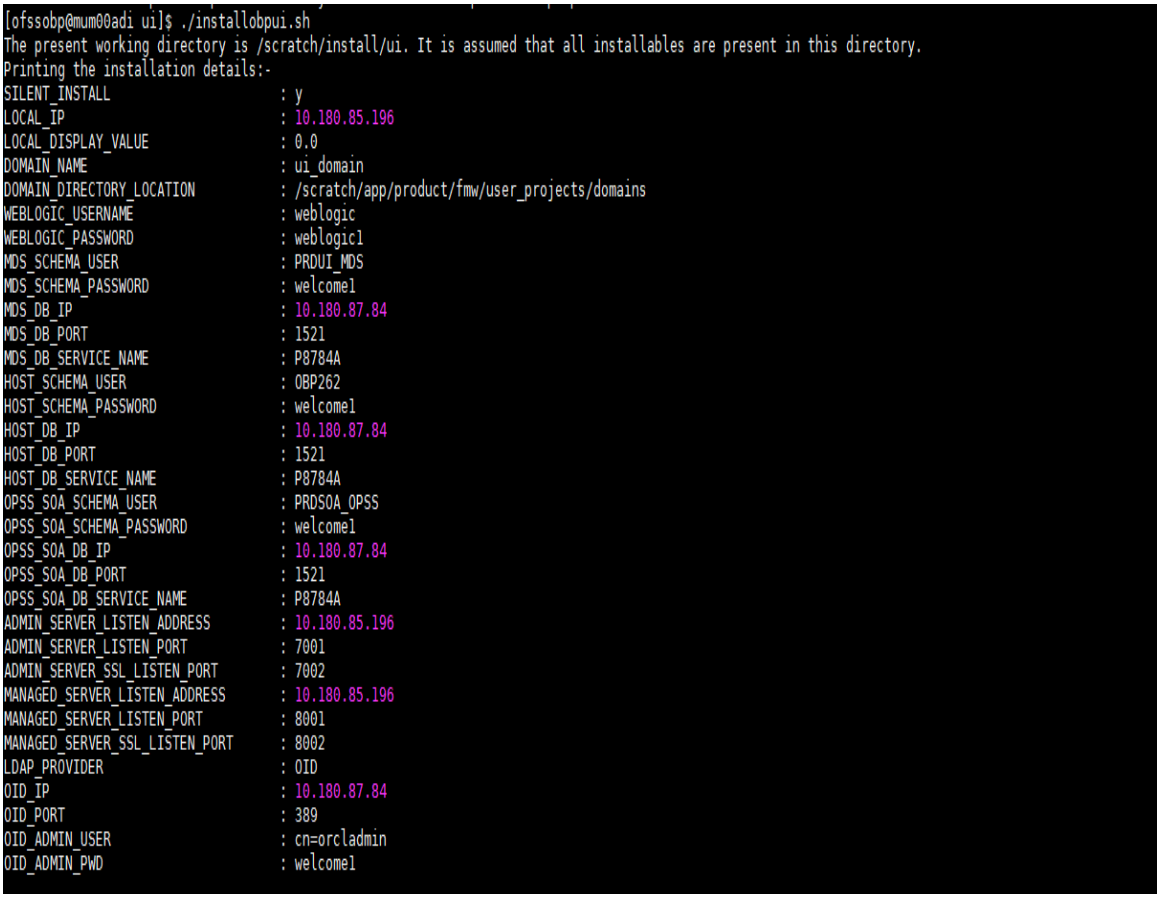


Figure 5–3 Confirmation to Proceed Domain Installation (contd)

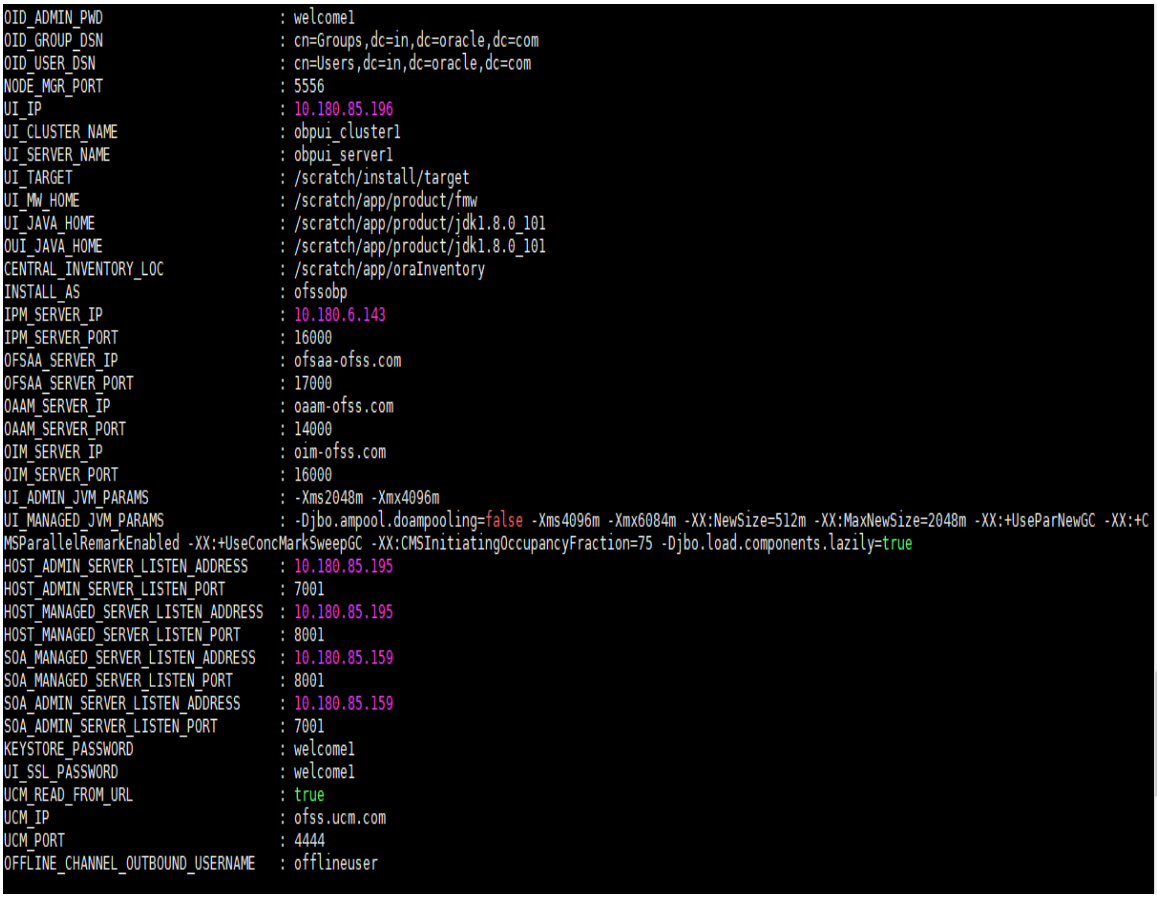


Figure 5–4 Confirmation to Proceed Domain Installation (contd)

3. Verify the value of each property carefully before proceeding.
4. If all values are correct, then enter 'Y' or 'y' and press Enter to initiate the installation. The installation utility performs the installation and domain is created silently.

Figure 5–5 Copying and Extraction of obpinstall-ui.zip

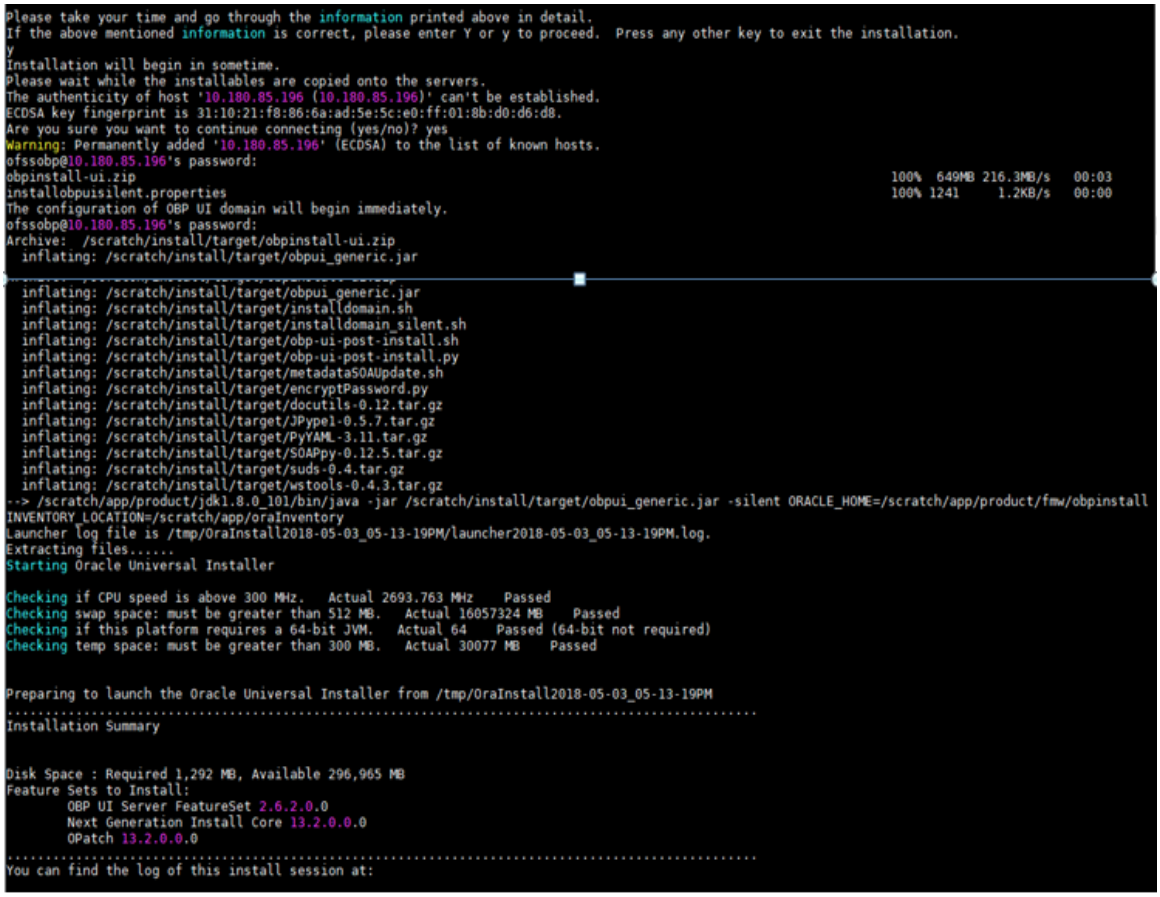


Figure 5–6 Copying and Extraction of obpinstall-ui.zip (contd)

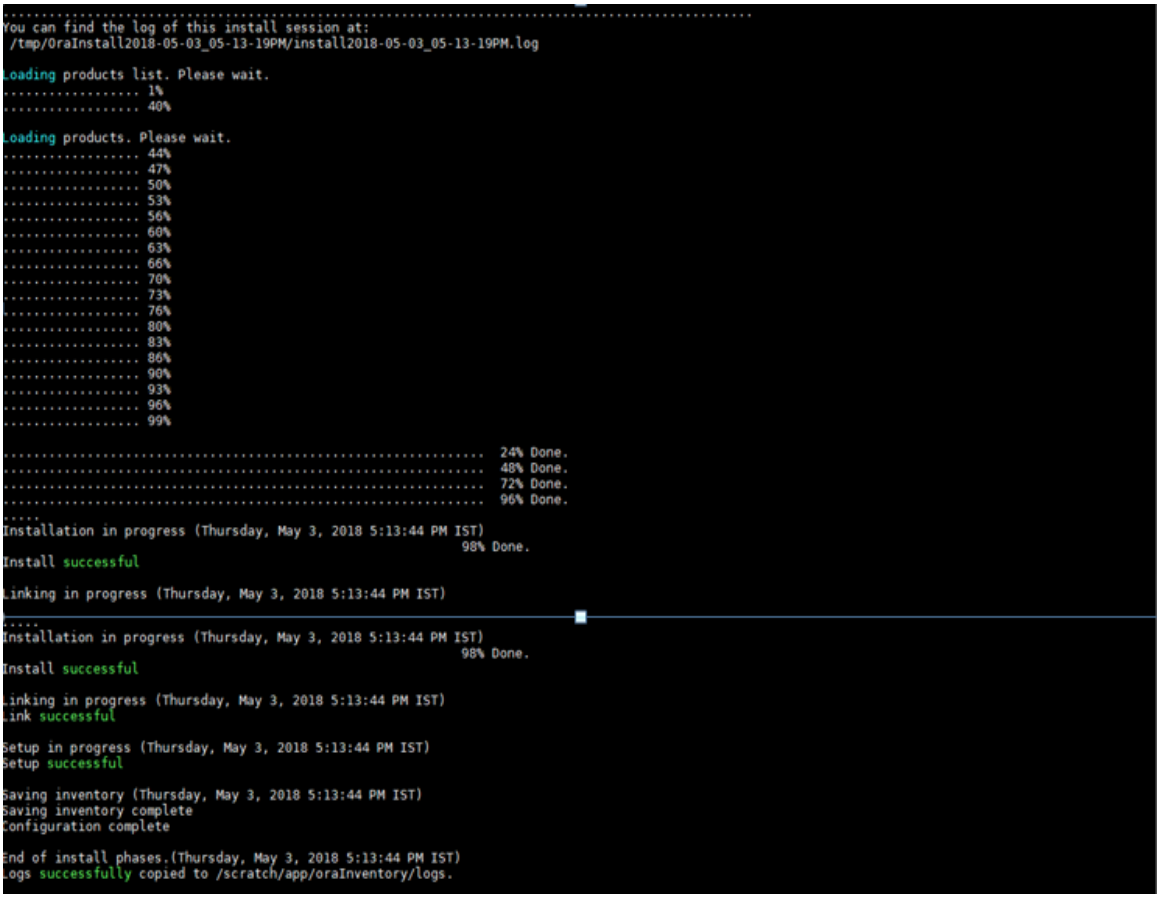
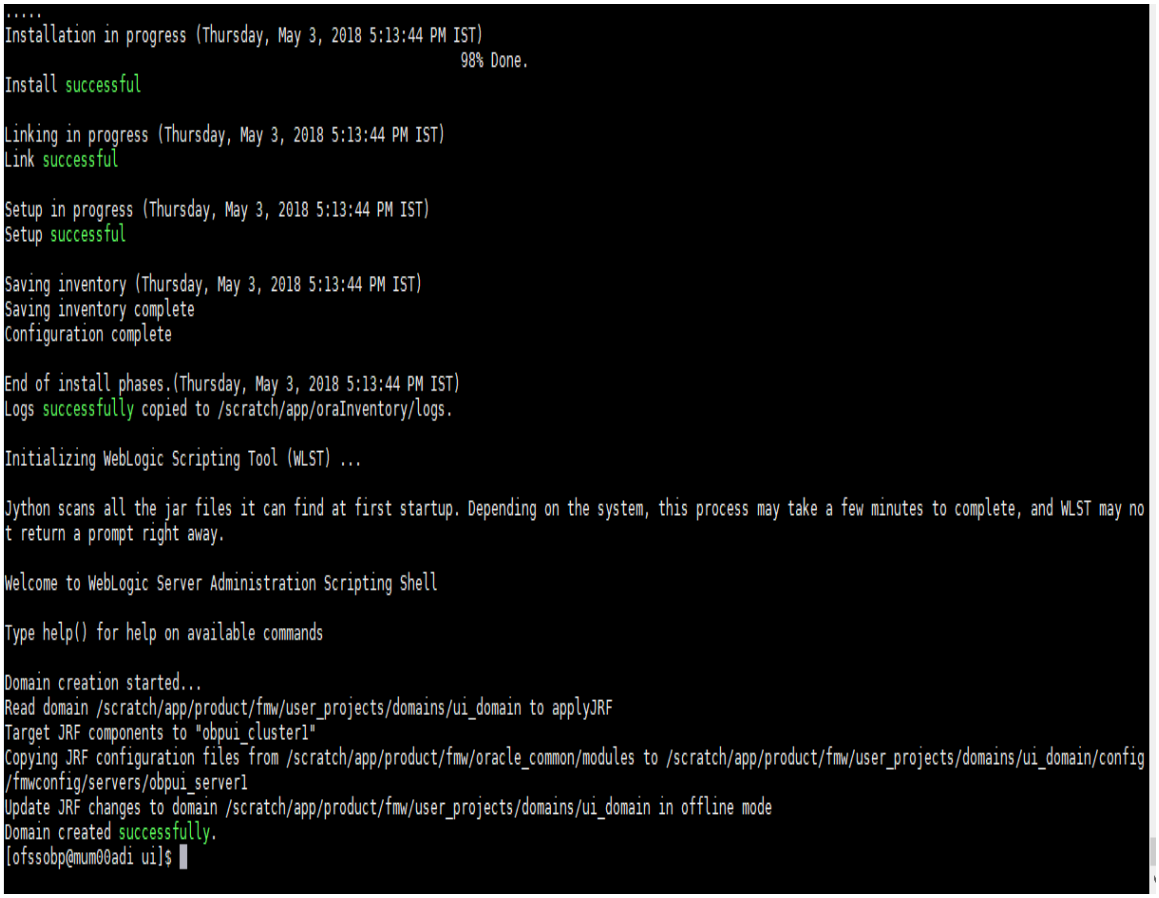


Figure 5–7 Domain Creation Confirmation



The above domain configuration process also creates files named obp-ui-post-install.sh and obp-ui-post-install.py in UI_MW_HOME location which are to be used to perform post installation configuration as elaborated in Section 5.2 Post Installation Configuration.

5.2 Post Installation Configuration

This section describes the post installation configuration procedure for Oracle Banking Deposits and Lines of Credit Servicing US Localization Presentation Media Pack.

Checklist for Post Installation Procedure

Before proceeding with the post installation procedure for UI, ensure the following:

- Node manager is not running on the UI machine.
- OID domain given in obppostinstallui.properties must exist in OID. (The OID domain is created at the time of host pre-install).
- Node manager port should be free. You can verify this using the following command, where 5556 is the Node Manager Port.

```
$netstat -na | grep 5556
```

Post Installation Configuration

1. Start the domain admin WebLogic server by executing the startWebLogic.sh script in the domain directory.

```
cd <middleware home>
cd user_projects/domains/obpuidomain/bin
./startWebLogic.sh
```

2. Enter the username and the password to ensure that the WebLogic server starts up.

Figure 5–8 UI Admin Server Credentials

Figure 5–9 UI Admin Server Running

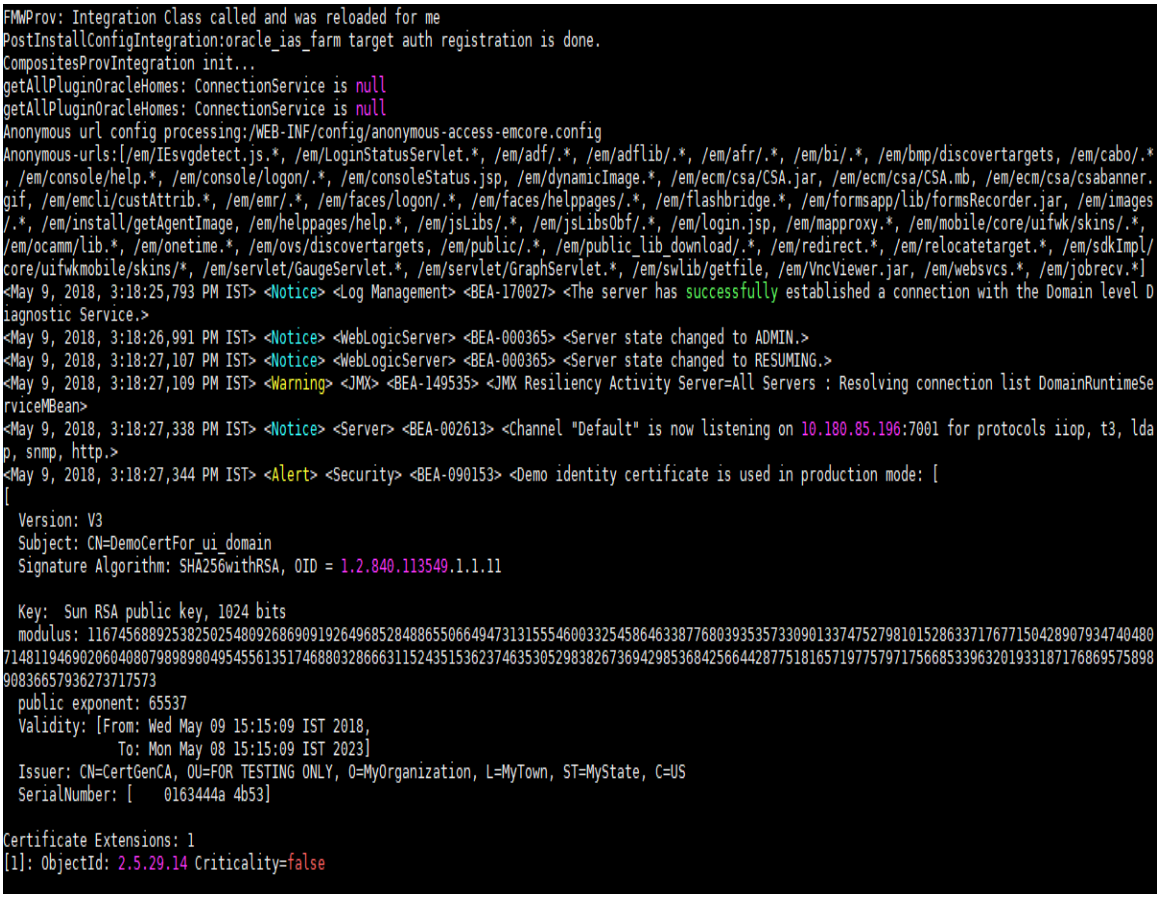


Figure 5–10 UI Admin Server Running (contd)

3. Once the server status changes to RUNNING proceed to execute the post installation script.
4. Navigate to the middleware home and list the files in the directory. A post installation and configuration script named obp-ui-post-install.sh will be listed along with other files and directories.
5. Navigate to the UI middleware location and give executable permission to the post install script:

```
$cd <ui middleware home>
```

6. Execute the script using the following commands:

```
$./obp-ui-post-install.sh
```

Figure 5–11 Starting Post Installation

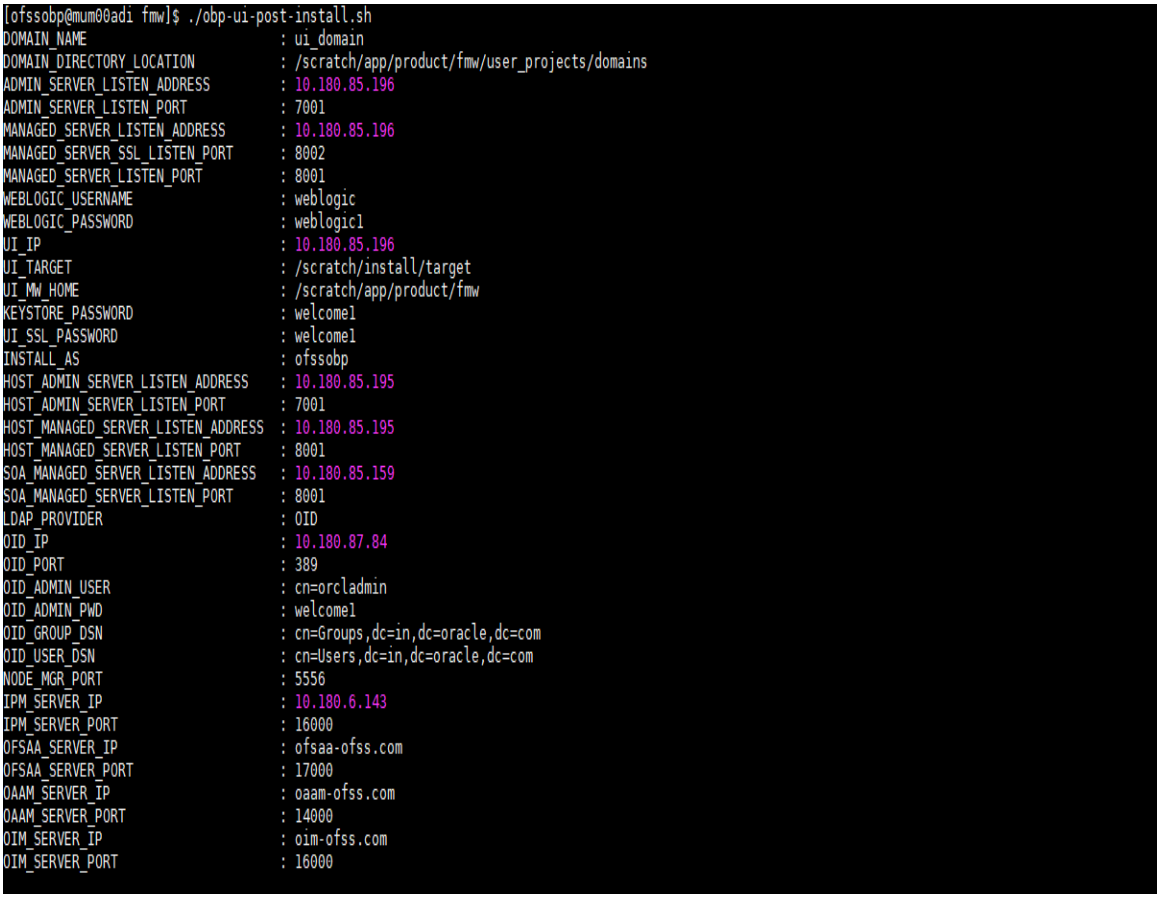


Figure 5–12 Starting Post Installation (contd)

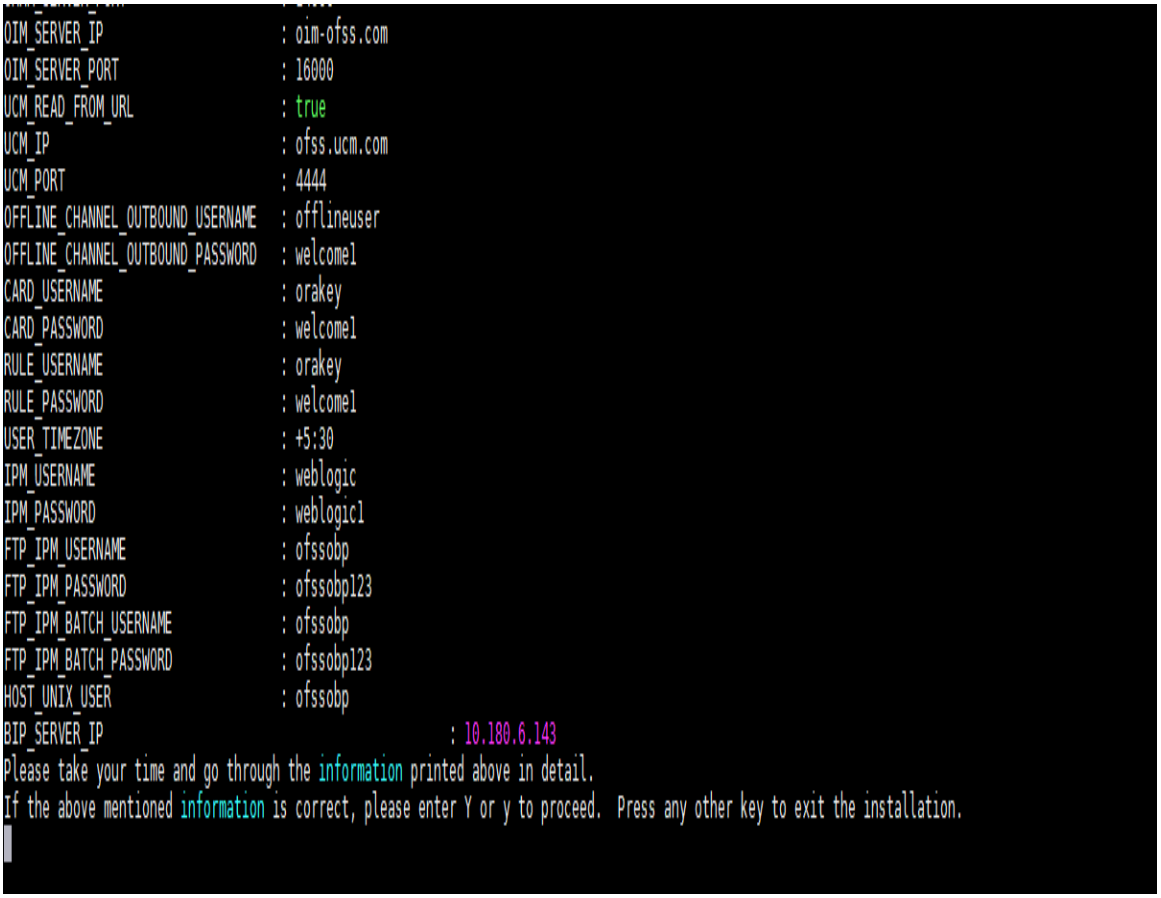


Figure 5–13 Continuation of Post-Installation

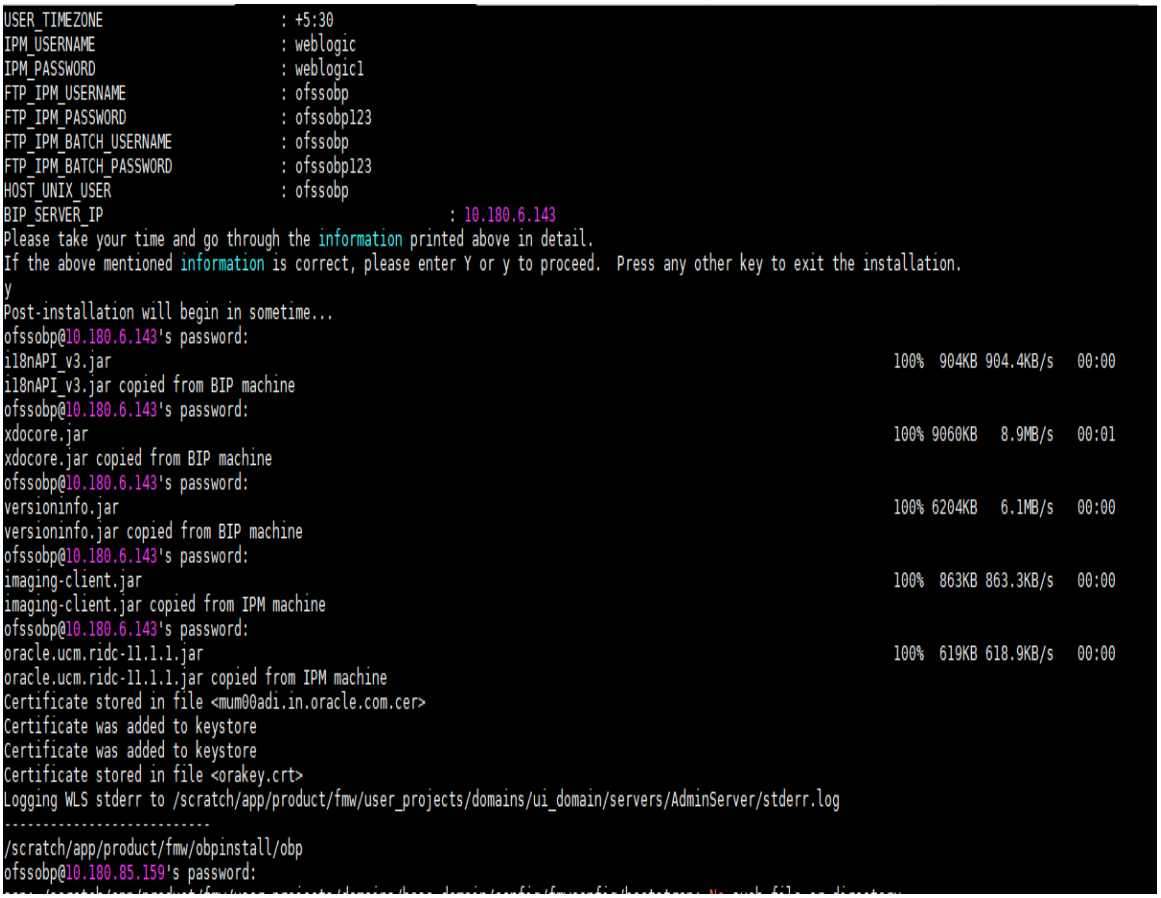
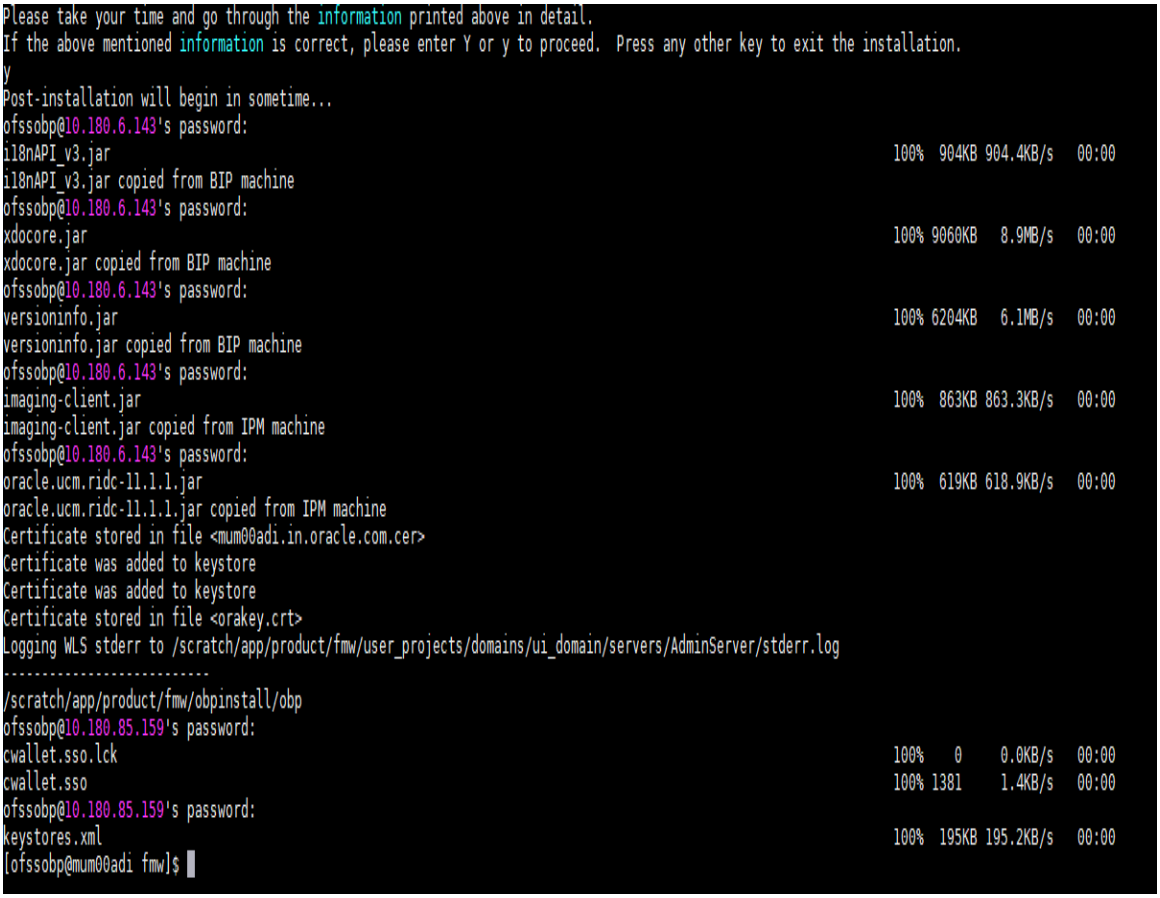


Figure 5–14 Continuation of Post-Installation (contd)



7. For monitoring the script run check the following log files created under the ui domain directory:
   - obp-ui-install-log.txt
   - obp-ui-install-log-py.txt
8. Deselect the following flag for all the OBDLOCS data sources:

   a. Log in to weblogic console
   b. Navigate to Data Sources > datasource name (eg. OBP_SYS_CONFIG) > Connection Pool > Advanced.
   c. Deselect the **Remove Infected Connections Enabled** check box.
   d. Add below parameter in UI server memory parameters in setDomainEnv.sh

      -Dweblogic.servlet.DIDisabled=true.
   e. Restart UI admin and UI managed server.

6 Standalone Database Setup

This chapter details the steps involved in setting up Oracle Banking Deposits and Lines of Credit Servicing database.

6.1 Pre-Installation Steps

The following steps should be completed prior to the process of executing the installation steps for the Oracle Banking Deposits and Lines of Credit Servicing DB mentioned in Section 6.2 OBDLOCS Database Setup – RCU Installation:

1. Oracle Database Enterprise Edition 12.2.0.1.0 is installed on the database server.
2. Obtain the tar file dbScripts_us.tar.gz (present in host.zip) from OBDLOCS Host localization media pack and copy it onto the database server.
3. Ensure that the ONS service is started after DB installation where the OBDLOCS Application schema needs to be created.

6.2 OBDLOCS Database Setup – RCU Installation

The steps that should be performed to create the OBDLOCS Host DB schema are provided in Section 6.3.1 Host DB Schema Creation and Verification

For other RCU schemas, while installing software on HOST, UI, and SOA, specific RCU should execute to create schemas for SOA, UI, and HOST.

RCU utility is present under <MW_HOME/oracle_common/bin> for respective components.

Following is the list of schemas to be created for SOA, UI, and HOST, respectively (note that SOA, UI and HOST are the prefix in below schemas which is given during schema creation).

- SOA_SOAINFRA
- SOA_MDS
- SOA_STB
- SOA_UMS
- SOA_OPSS
- SOA_IAU_APPEND
- SOA_IAU_VIEWER
- SOA_WLS_RUNTIME

- UI_STB
- UI_OPSS
- UI_MDS

- UI_IAU_APPEND
- UI_IAU_VIEWER
- UI_WLS_RUNTIME

- HOST_STB
- HOST_OPSS
- HOST_IAU_APPEND
- HOST_IAU_VIEWER
- HOST_MDS
- HOST_WLS_RUNTIME

UI_MDS and UI_STB schemas are used by UI component.

HOST_MDS and HOST_STB schemas are used by HOST component.

SOA_SOAINFRA, SOA_STB, SOA_MDS and SOA_UMS schemas are used by SOA component.

UI_OPSS and HOST_OPSS schemas are used for silent domain creation in pre installation by UI and HOST respectively.

SOA_OPSS, SOA_IAU_APPEND and SOA_IAU_VIEWER schemas are shared by HOST and UI also pointed during post installation of HOST and UI.

Increase the size of tablespace (at least 6GB and should be in auto extend mode on) for SOA_MDS, SOAINFRA and OPSS schema used for SOA domain creation.

6.3 OBDLOCS Database Installation

This section includes steps for application schema creation along with execution of its ddl and seed. Also it includes system configuration database update and table partitioning.

6.3.1 Host DB Schema Creation and Verification

For the host db schema creation, copy the dbScripts_us.tar.gz file (present in host.zip) from OBDLOCS Host media pack location to any machine where sqlplus is available.

Untar the file which contains createobp.sql, ddl and seed file and folders. (TNS entry of the host db may be required in that machine to enable connectivity from the machine to the host db server.)

In createobp.sql, Replace &&1,&&2 and &&3 with schema, password, and tablespace name.

Before executing createobp.sql, make sure tablespace is created in the database.

The createobp.sql will create application schema with required database grants.

createobp.sql execution

```
PROMPT> sqlplus sys/password@TNSEntryOfDB as sysdba @createobp.sql
```

6.3.2 HOST DB schema ddl execution

Now open command prompt and navigate inside “ddl” folder in the machine where it has been copied. Then run the following using the actual details of host db schema while was created.

Connect to application schema (which is created using createobp.sql) using sqlplus

```
PROMPT> sqlplus schemauser/password@TNSEntryOfDB @ddl/SCHEMA_
DDL.sql
```

The example assumes that the seed is being executed from “D:\ORACLE” folder of a Windows machine having sqlplus console available for execution of sql commands and scripts.

```
C:> D:
C:> cd D:\ORACLE
D:\ > sqlplus DEV_OBP/welcome1@OBPDB
D:\ >@ddl/SCHEMA_DDL.sql
```

The following verification steps can be executed to check that the Database setup is complete:

1. Verify that the new tablespace is created.
2. Log on to the database with user id created.
3. Execute the query “select * from tab;” on the sql prompt to verify that the OBP tables are present.

6.3.3 HOST DB Schema Seeding

This section provides information on the Host Database Schema Seeding. The procedure is as follows:

Now open command prompt and navigate inside the ’seed’ folder in the machine where it has been copied. Run the following commands using the actual details of host db schema which was created.

```
PROMPT> sqlplus schemauser/password@TNSEntryOfDB @seed.sql
```

For example, assume that the seed is being executed from ’D:\seed’ folder of a Windows machine having sqlplus console available for execution of sql commands and scripts.

```
C:> D:
C:> cd D:\seed
D:\seed > sqlplus DEV_OBP/welcome1@OBPDB
D:\seed >@seed.sql
```

It will take some time to completely execute all the seed scripts. It will ask for some inputs at the time of seeding, just press Enter to continue. When OBDLOCS DB seeding is completed, the control will return to the sql prompt.

Note

If you are going to install localization on top of product, DO NOT execute ddl and seed of product, execute ddl and seed which are present under localization host mediapack in form of dbscripts_au.tar.gz and dbScripts_us.tar.gz.

6.3.4 System Configuration DB Update Script Execution

After the host db schema has been created successfully, copy the ’updateSystemDetails.sql’ file from ’SOA_MW_HOME’ location to any machine where 'sqlplus' is available. (TNS entry of the host db may be required in that machine to enable connectivity from the machine to the host db server).

Now, open command prompt and navigate 'updateSystemDetails.sql' file in the local machine where it has been copied. Then run the following using the actual details of host db schema which was created.

```
PROMPT> sqlplus schemauser/password@TNSEntryOfDB @
updateSystemDetails.sql
```

For example, assume that the seed is being executed from 'D:\script' folder of a Windows machine having sqlplus console available for execution of sql commands and scripts.

```
C:> D:
C:> cd D:\script
D:\seed > sqlplus DEV_OBP@welcome1@OBPDBB
D:\seed >@updateSystemDetails.sql
```

6.3.5 Removing Preference Refresh Level

OBDLOCS Preferences are held in the weblogic servers in the form of a cache which is refreshed at a configurable interval. As part of installation, the preferences are declared in a file called Preferences.xml in the "config" folder. These preference values are mostly technical in nature and are seldom changed in production.

Hence, majority of OBDLOCS customers have configured to disable preference refresh. This is done by setting "syncTimeInterval" to -1 on the target preference. Customers should deliberate and take a decision on the preferences for which they wish to disable the refresh.

For example:

<Preference name="MiddlewareTaskMetadataDTOFieldConfig"

PreferencesProvider="com.ofss.fc.infra.config.impl.DBBasedPropertyProvider"

parent="jdbcpreference"

propertyFileName="SELECT SERVICE_ID || ':' || DTO_CLASS || ':' ||

COD_ATTR_ID valuekey, FIELD_NAME AS valuestring FROM flx_fw_mw_tasks_dto_map"

syncTimeInterval="-1" />

6.3.6 Database Table Partitioning

For Database Table Partitioning, execute the scripts present in Table_Partitioning.zip present in host.zip. Execute the script in sequence and follow the guidelines mentioned in the script.

1. OBP_PARTITION_TABLE.sql
2. OBP_PARTITION_TABLE_SEED.sql
3. APPLY_PARTITION.sql

7 OBDLOCS and IPM Integration

This chapter details the steps involved in the integration of Oracle Banking Deposits and Lines of Credit Servicing and Oracle Imaging and Process Management (IPM).

OBDLOCS integrates natively with Oracle IPM as the content management solution. Configuration information relevant from an OBDLOCS point of view is provided in the following sections:

- Section 7.1 IPM Application Setup for OBDLOCS Content Management
- Section 7.2 IPM Configuration for Bulk Upload Process Setup
- Section 7.3 IPM Report Upload Setup

The steps listed therein should be followed to configure IPM to facilitate it to integrate with OBDLOCS. However, you can see the administration guide for Oracle IPM for details on how to manage connections, inputs and applications in IPM.

7.1 IPM Application Setup for OBDLOCS Content Management

This is a mandatory configuration required on IPM to enable integration of OBDLOCS with IPM for content management.

The following properties from the checklist should be used for creating connection profiles in the Manage Connections section. These connection profiles will be used while creating the applications on the next section on Manage Applications.

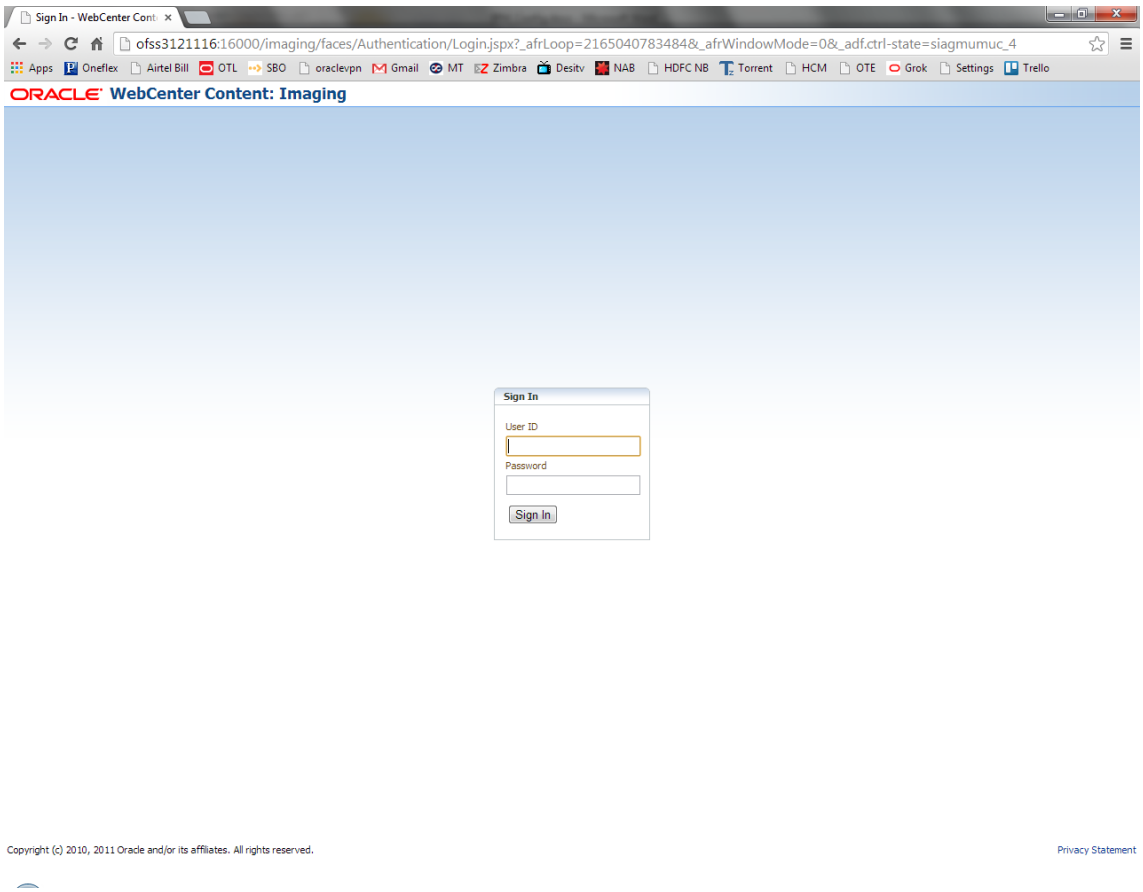
7.1.1 UCM Connection

The UCM connection is used to point to the underlying UCM Server where the documents are stored.

1. Log in to IPM imaging console through a URL such as follows:

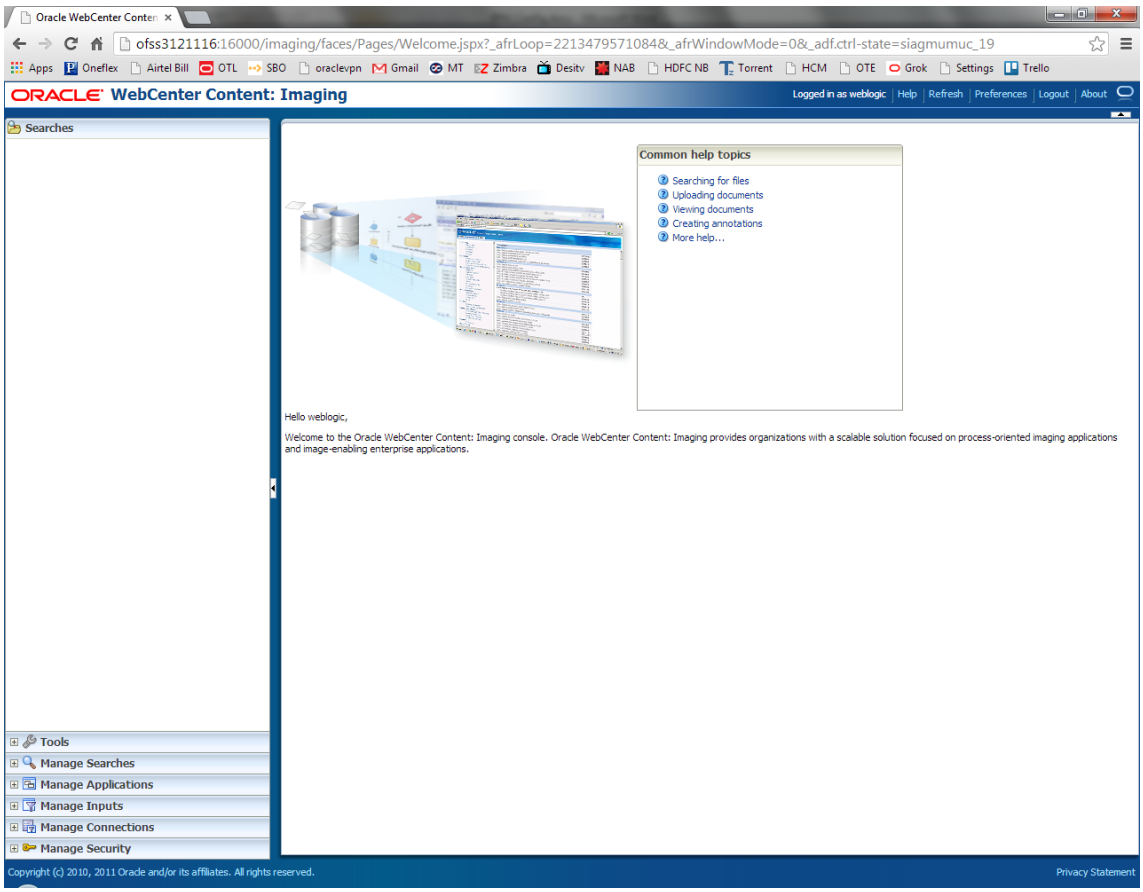
   http:// hostname:16000/imaging

Figure 7–1 IPM Imaging Console - Login page



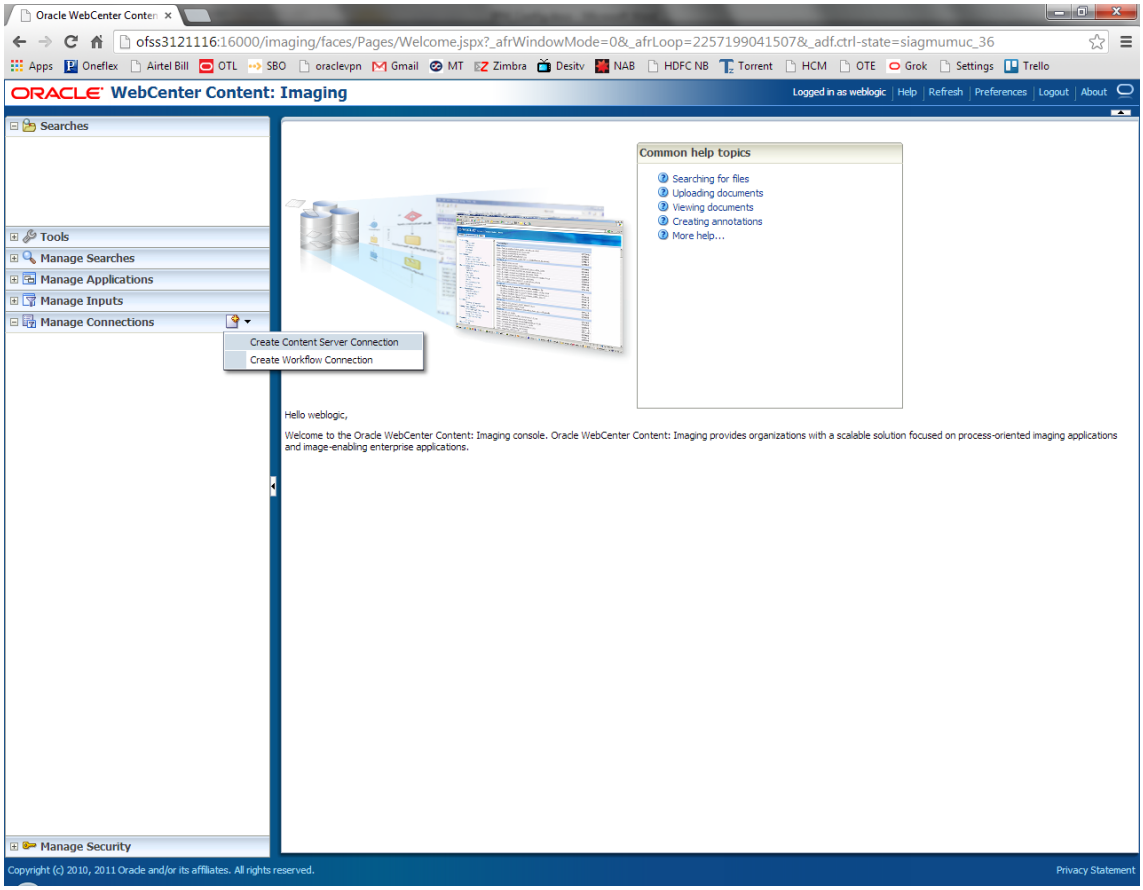
2. Enter the user ID and password set during IPM installation.

Figure 7–2 IPM - Welcome page



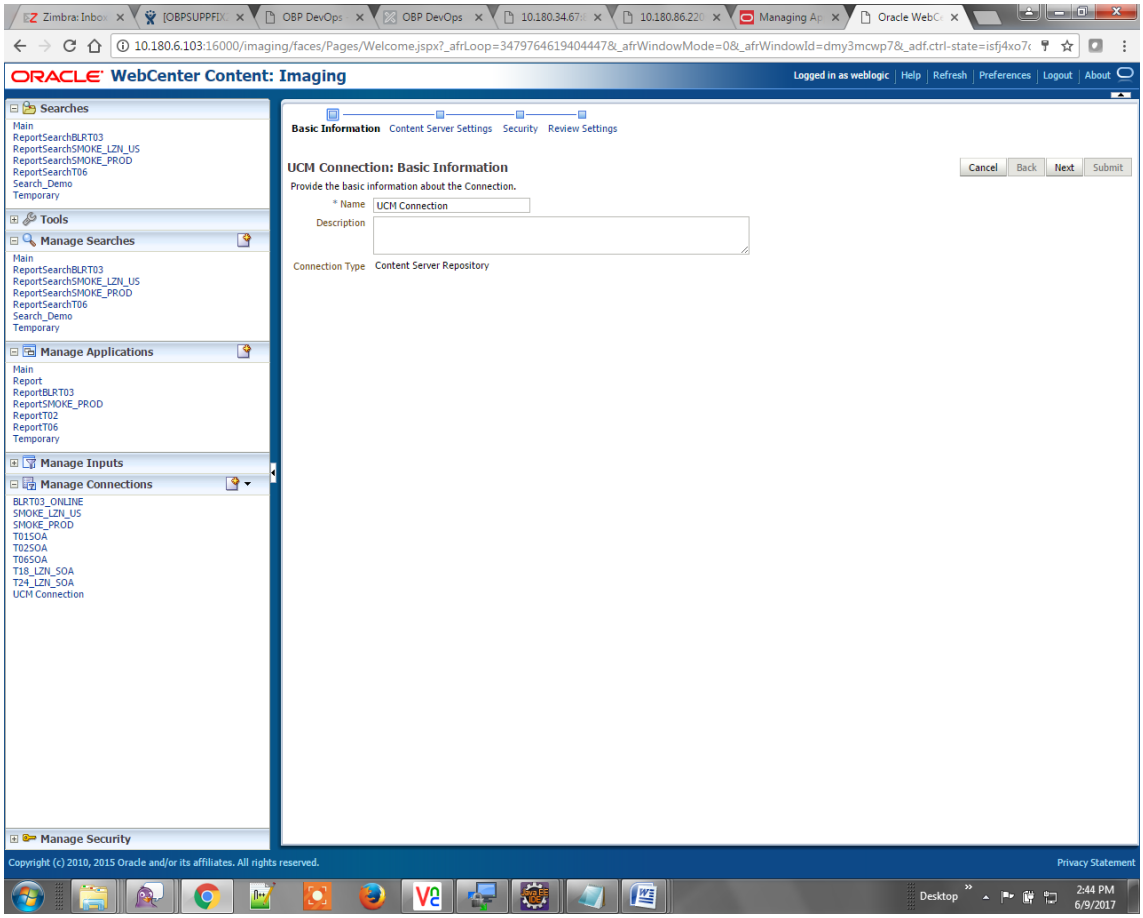
3. Navigate to Manage Connection and select Create Content Server Connection.

Figure 7–3 Create Content Server Connection



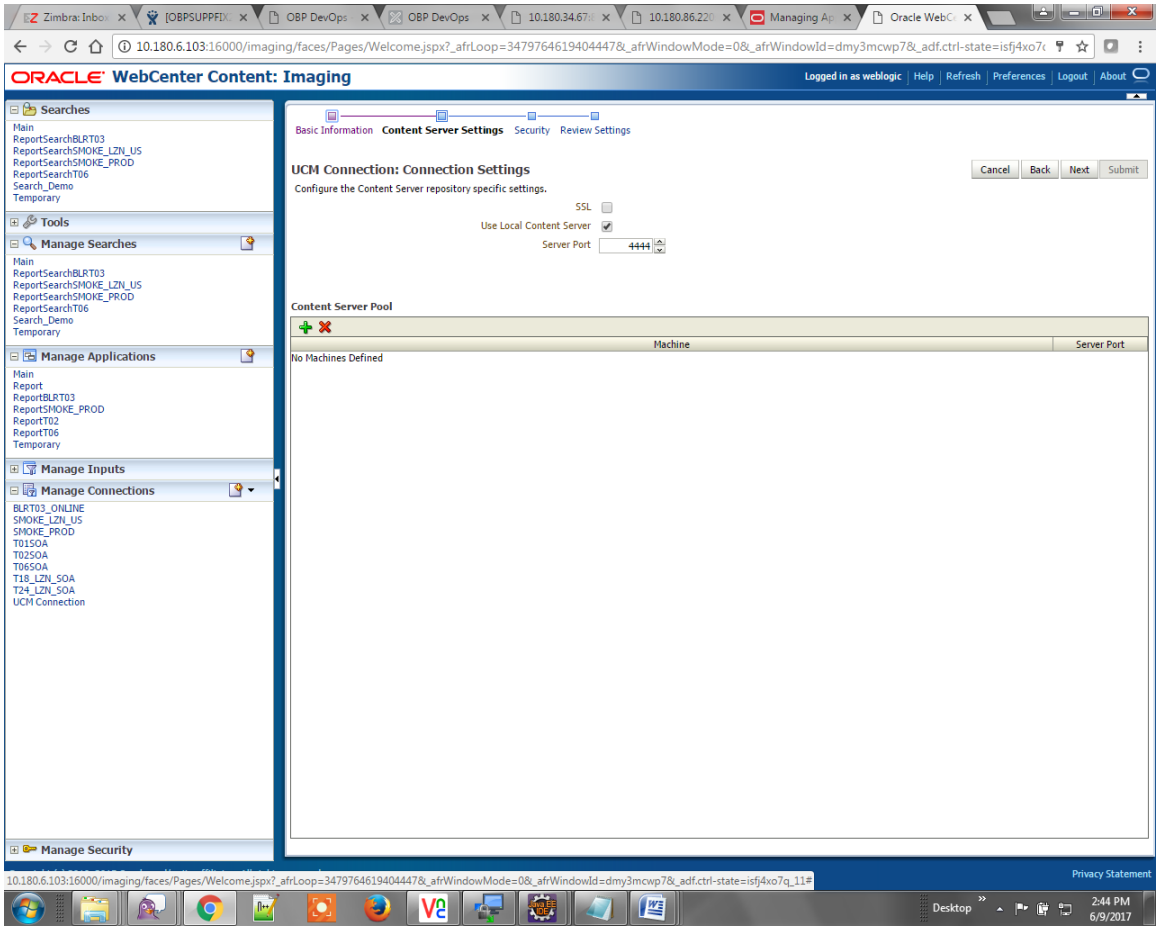
4. In the Basic Information stage, enter the name and description for Content Server Connection as UCM Connection and click Next.

Figure 7–4 UCM: Basic information



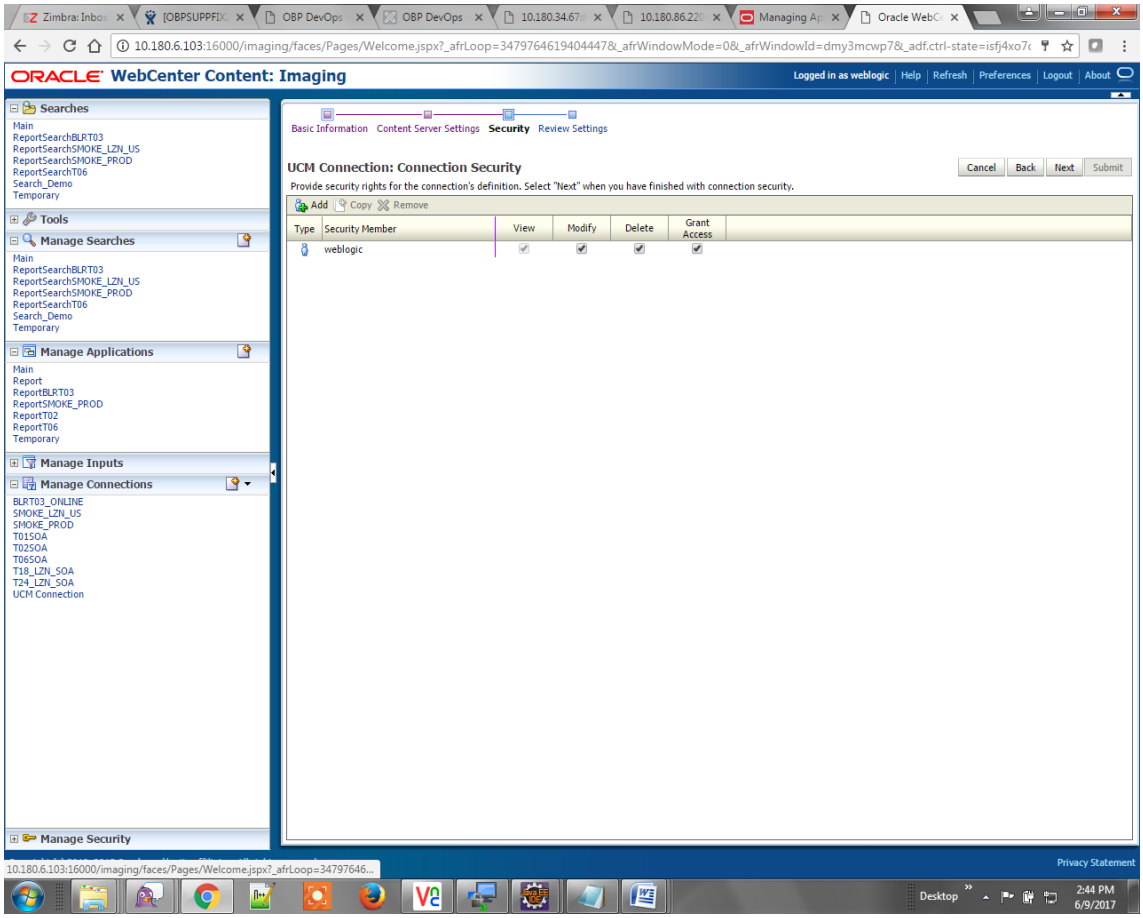
5. In the Content Server Settings page, select the Use Local Content Server check box and select the Server Port as 4444. Click Next.

Figure 7–5 UCM: Connection Settings



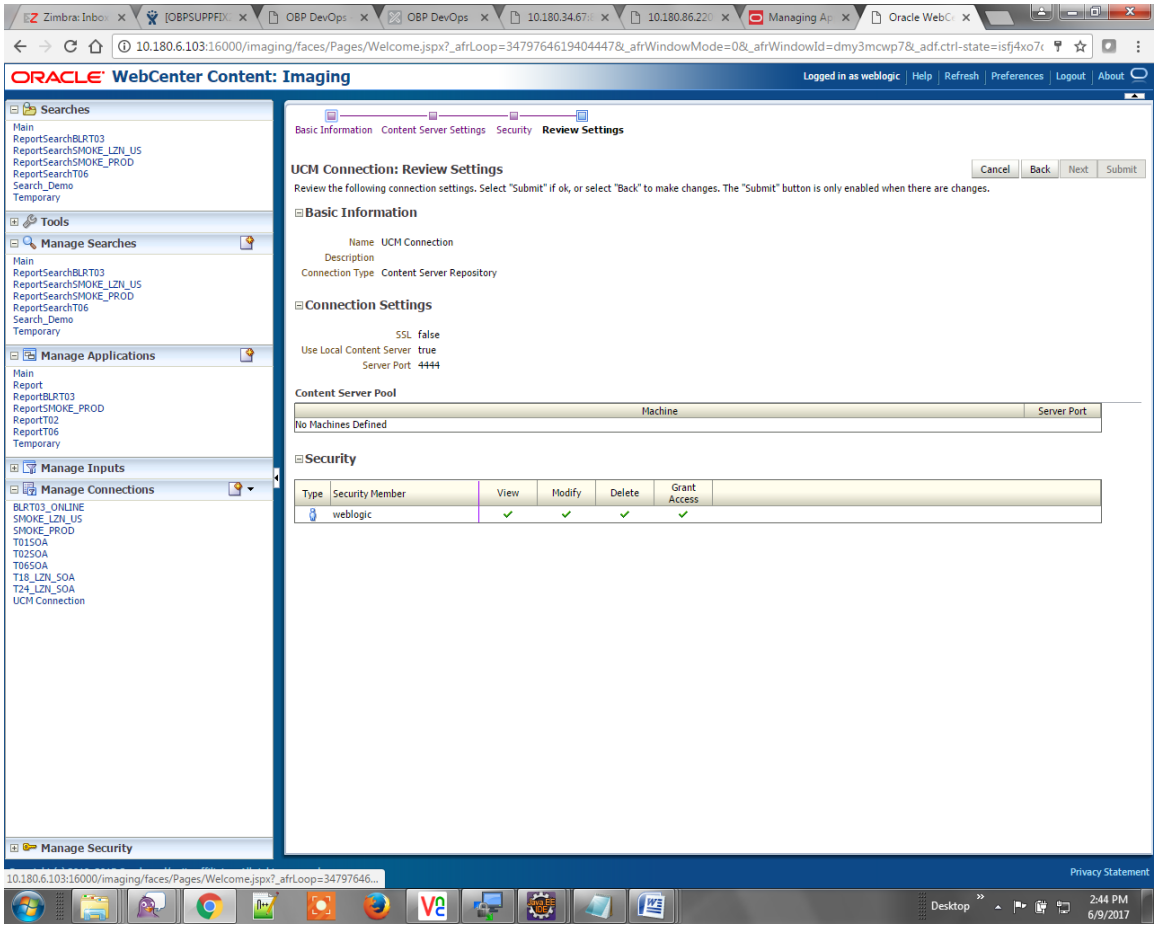
6. In the Security stage, select security rights for connection definition as shown below and click Next. If weblogic security member is not present, create it by clicking Add.

Figure 7–6 UCM: Connection Security



7. In the Review Settings stage, review the settings and click **Submit.**

Figure 7–7 UCM: Review Settings



7.1.2 Main Application Configuration

The documentation for Oracle IPM should be referred to for details on how to create applications in IPM. For more information, see https://docs.oracle.com/middleware/12213/wcc/admin-image/GUID-4A1A138D-FFEC-4FBB-A6D3-7F4FA4BDE06A.htm#IPMGA162.

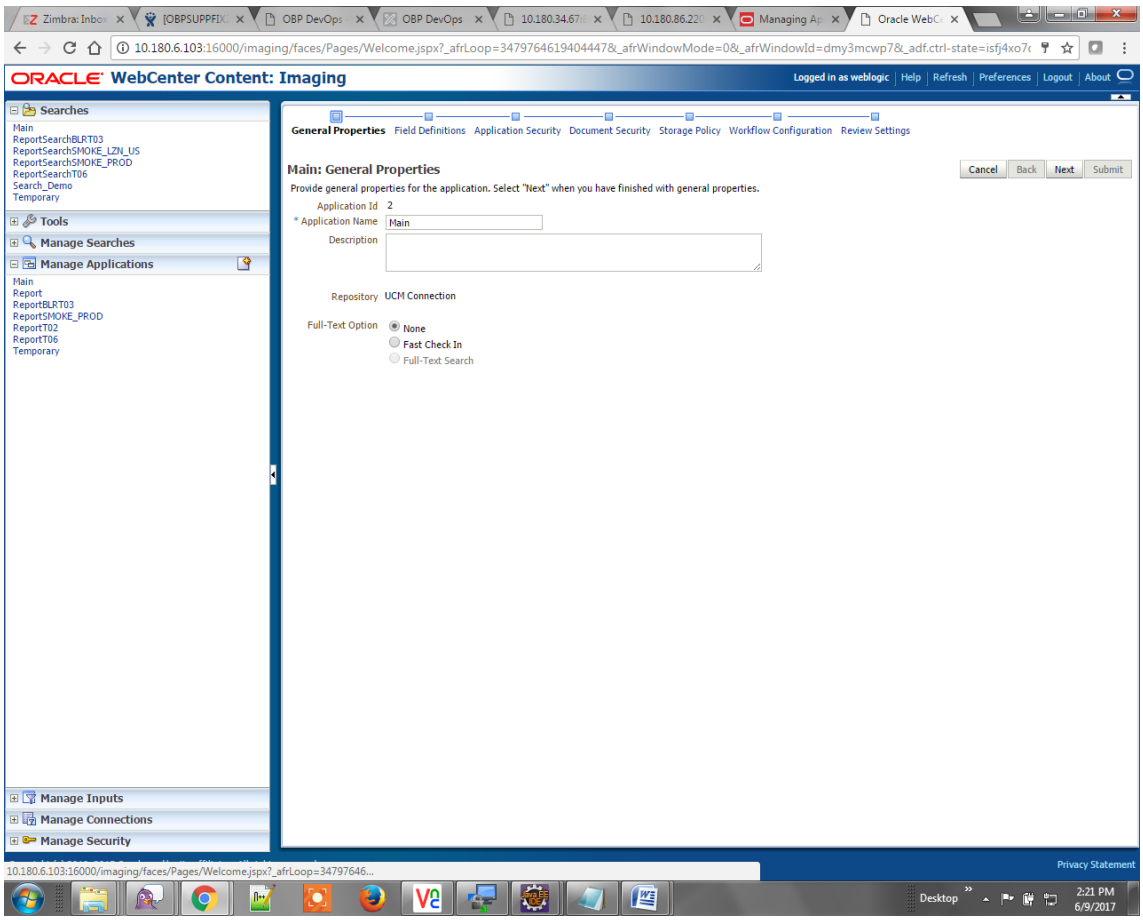
Create a main application and a temporary application in IPM.

7.1.2.1 Manage Application Configuration

To manage application configuration:

1. Select Create New Application option.
2. Enter the general properties and click **Next.**

Figure 7–8 Main: General Properties



3. Enter the field definition details and click **Next.**

Figure 7–9 Main: Field Definitions

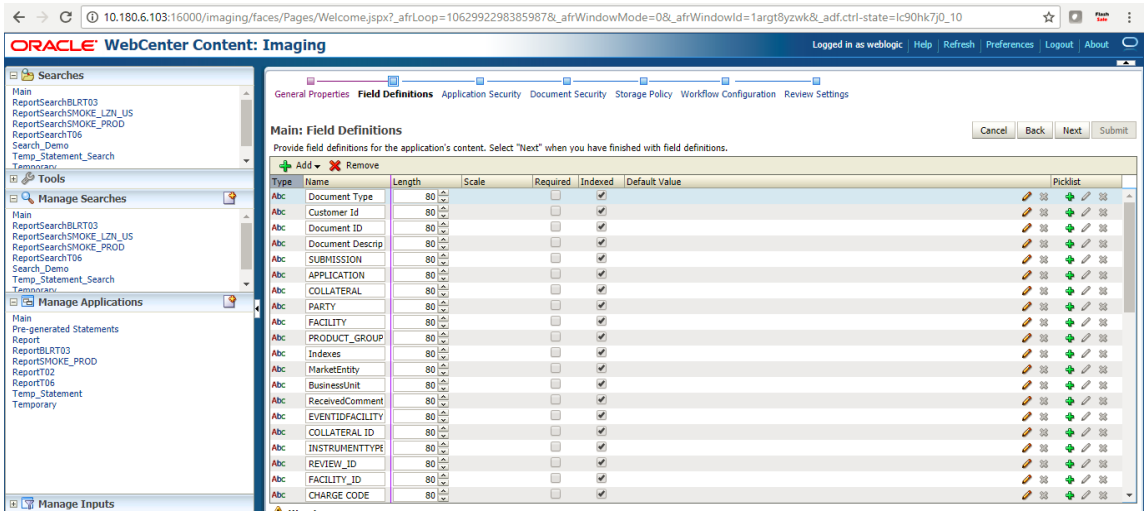
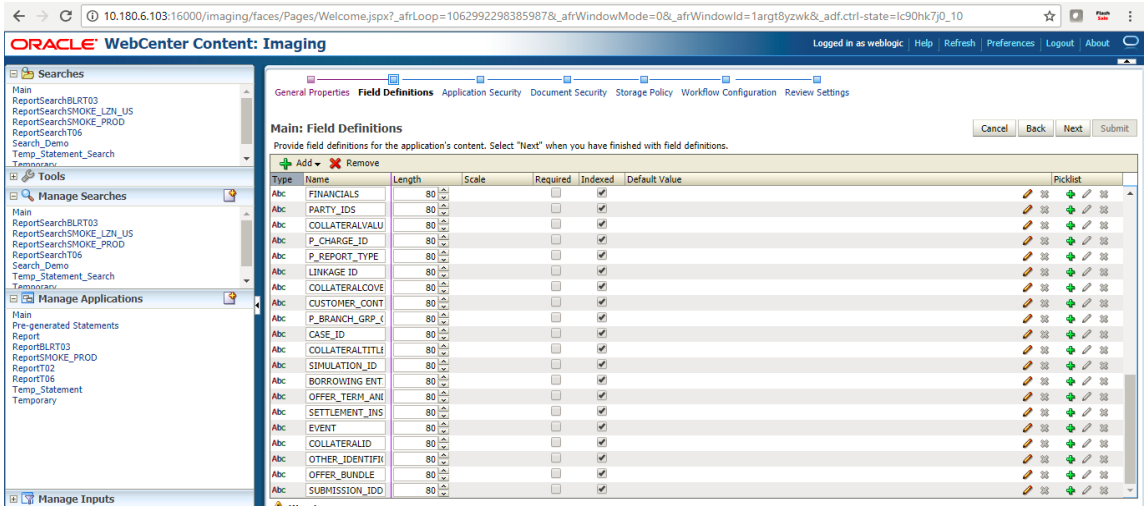


Figure 7–10 Field Definitions (cont.)



4. In Application Security and Document Security pages, select the access rights for users and click **Next.**

Figure 7–11 Main: Application Security

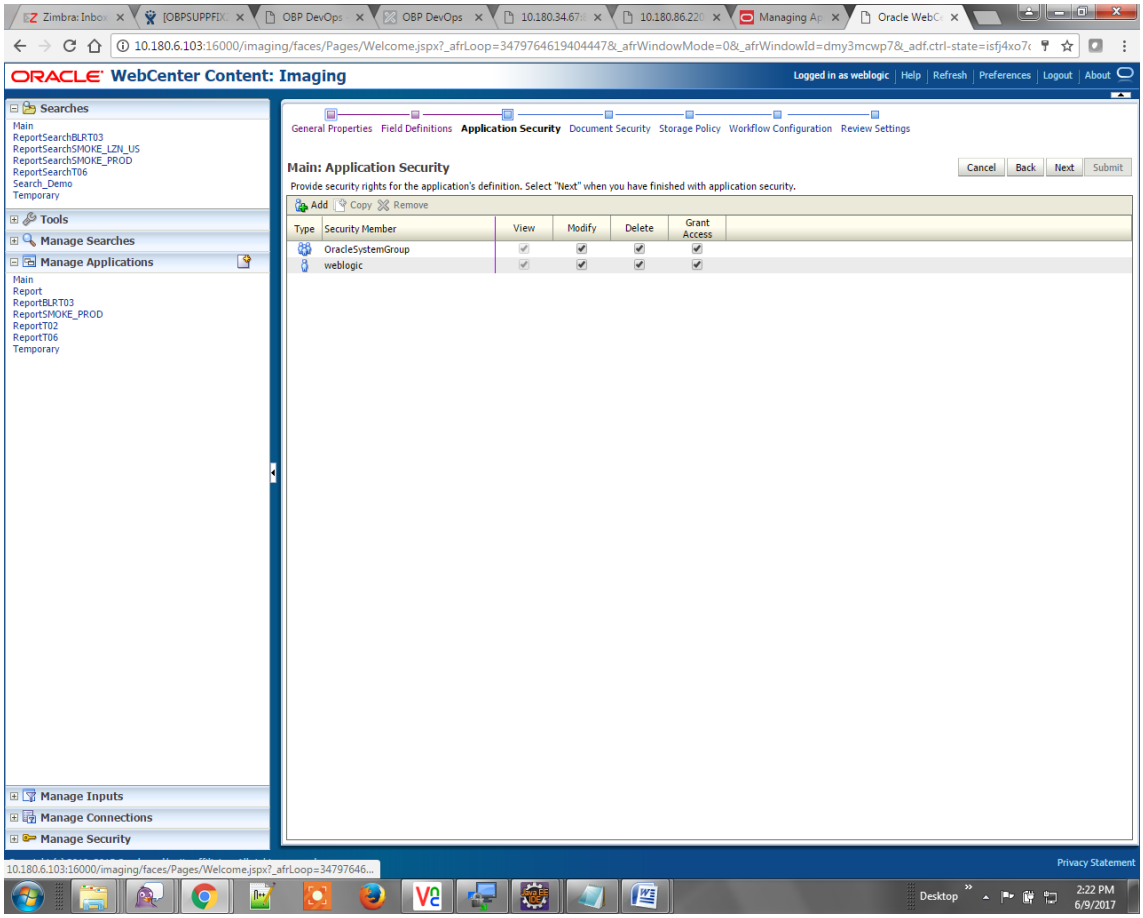
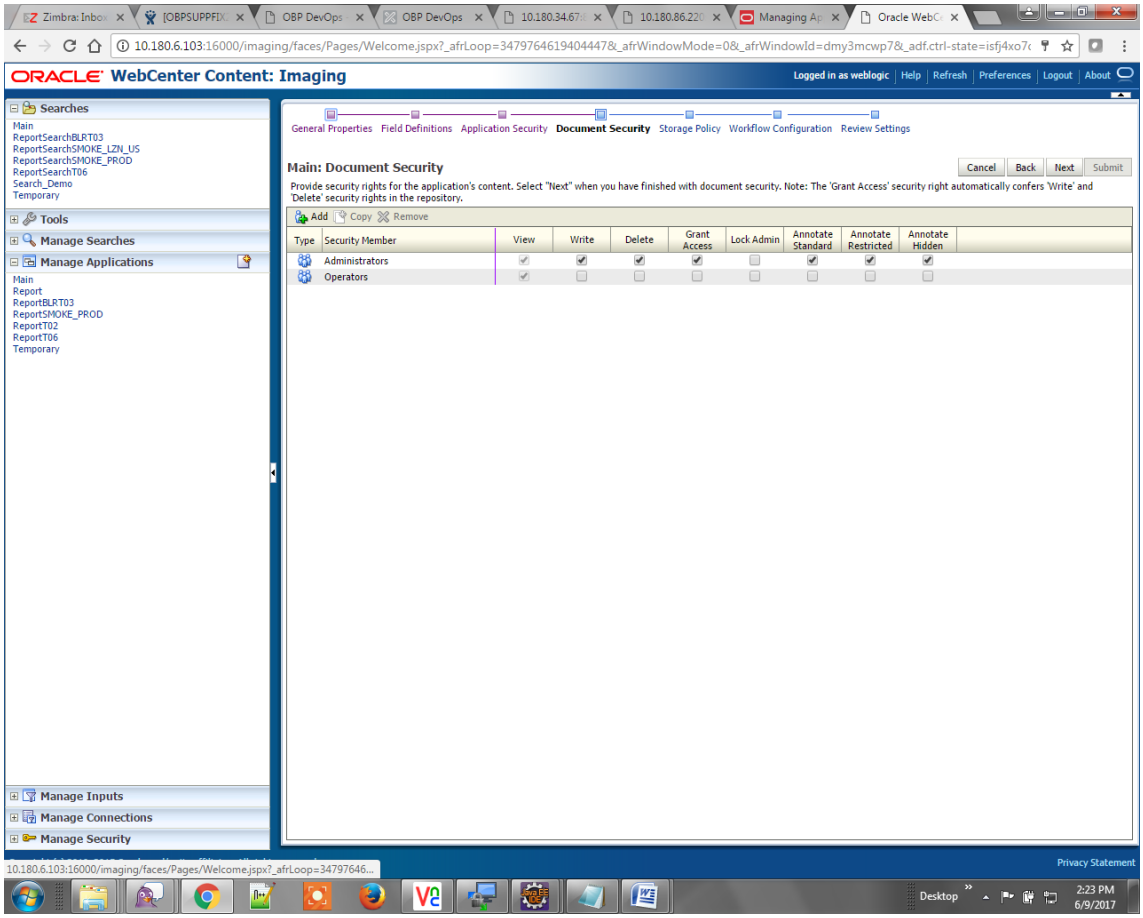
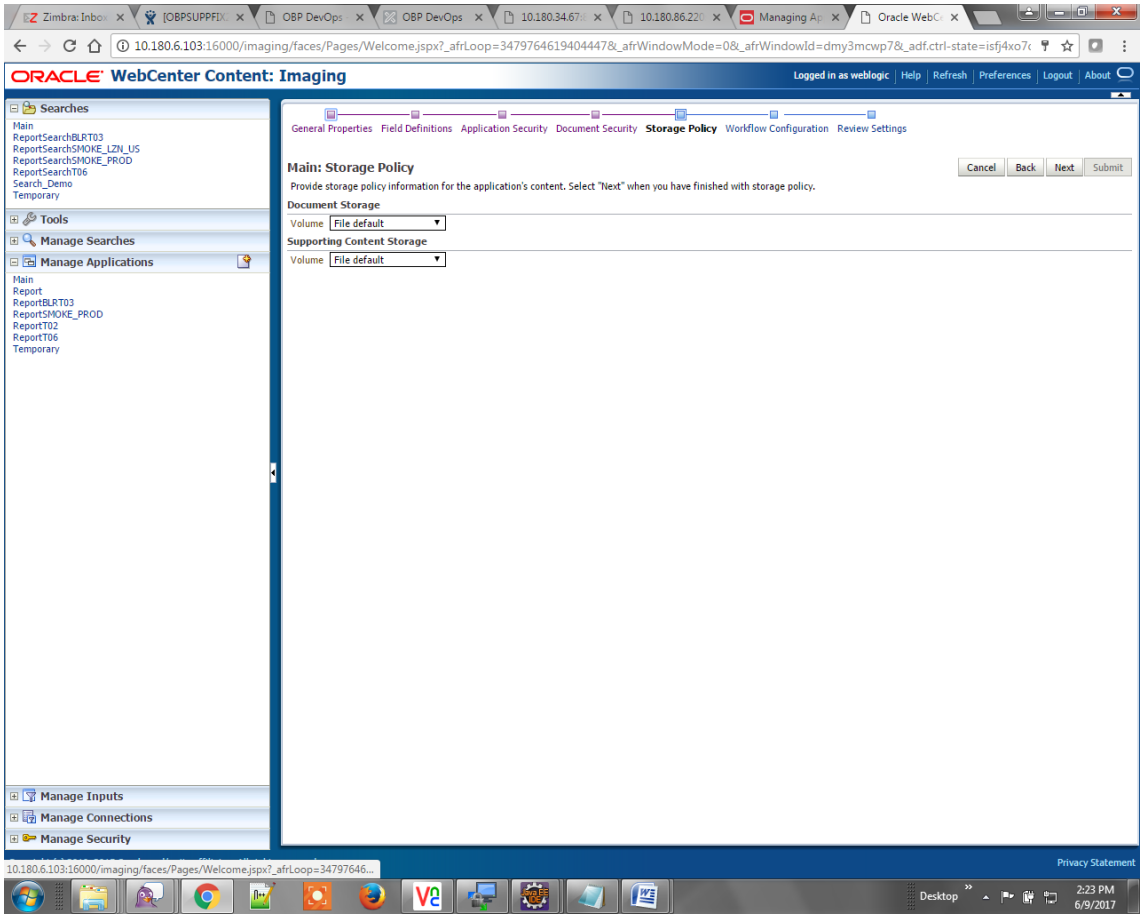


Figure 7–12 Main: Document Security



5. In the Storage Policy page, select the file default option as shown below.

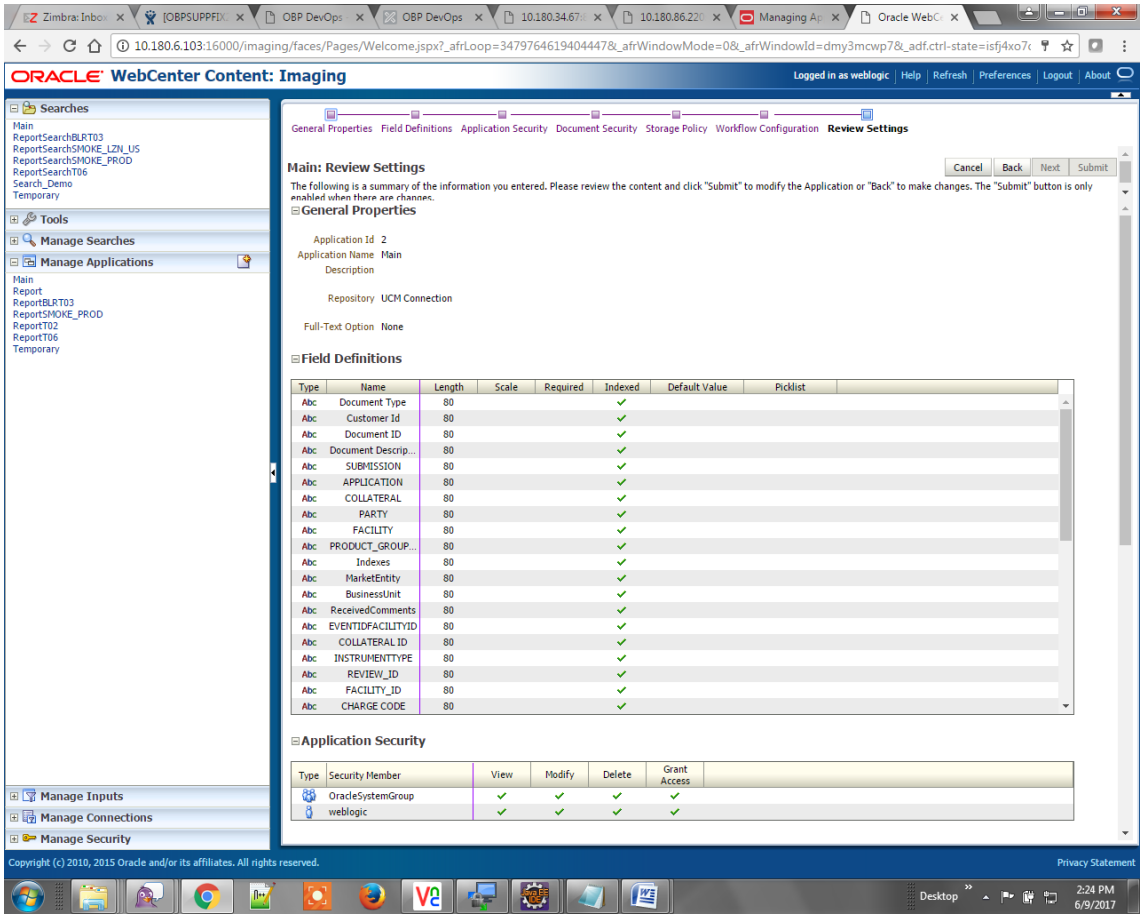
Figure 7–13 Main: Storage Policy



6. Click **Next.** Skip the Workflow Configuration page.
7. Click **Next.**

8. Review the summary and click **Submit.**

Figure 7–14 Main: Review Settings

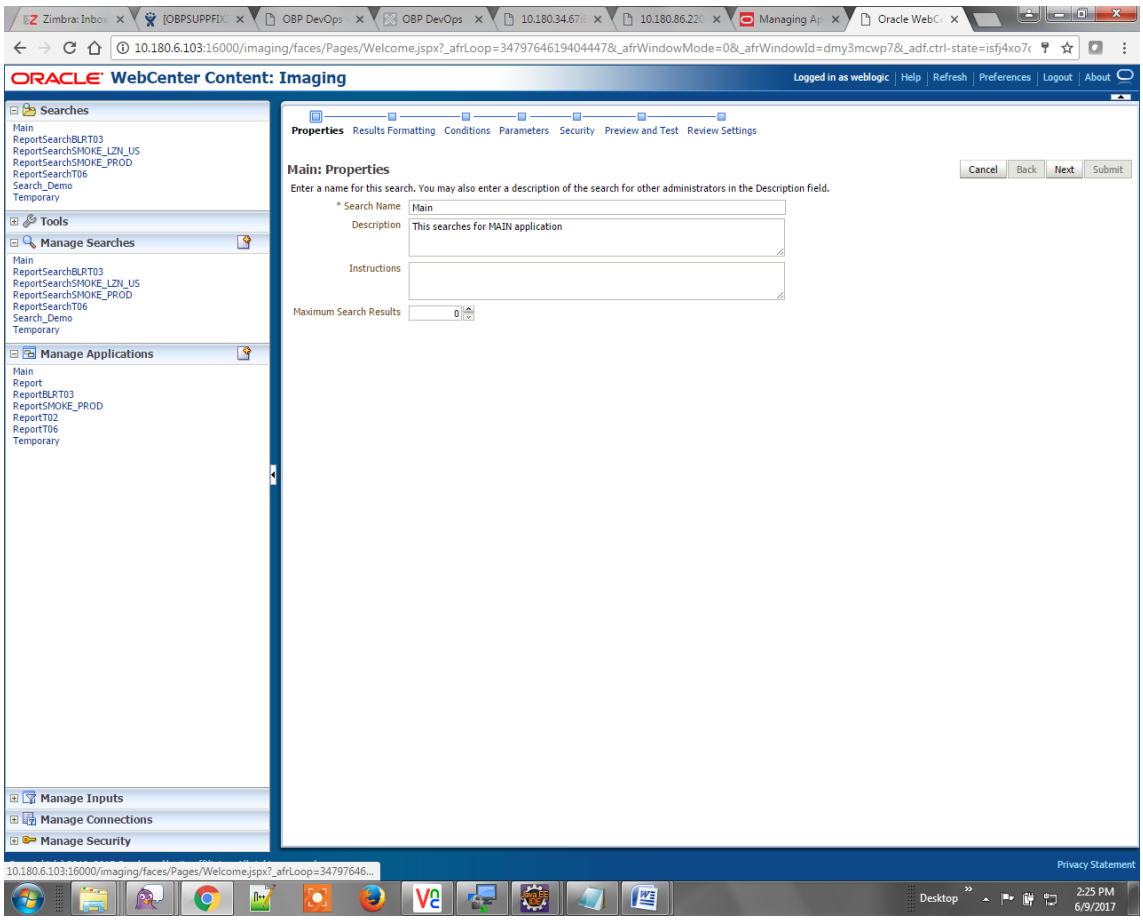


7.1.2.2 Manage Searches

To manage searches:

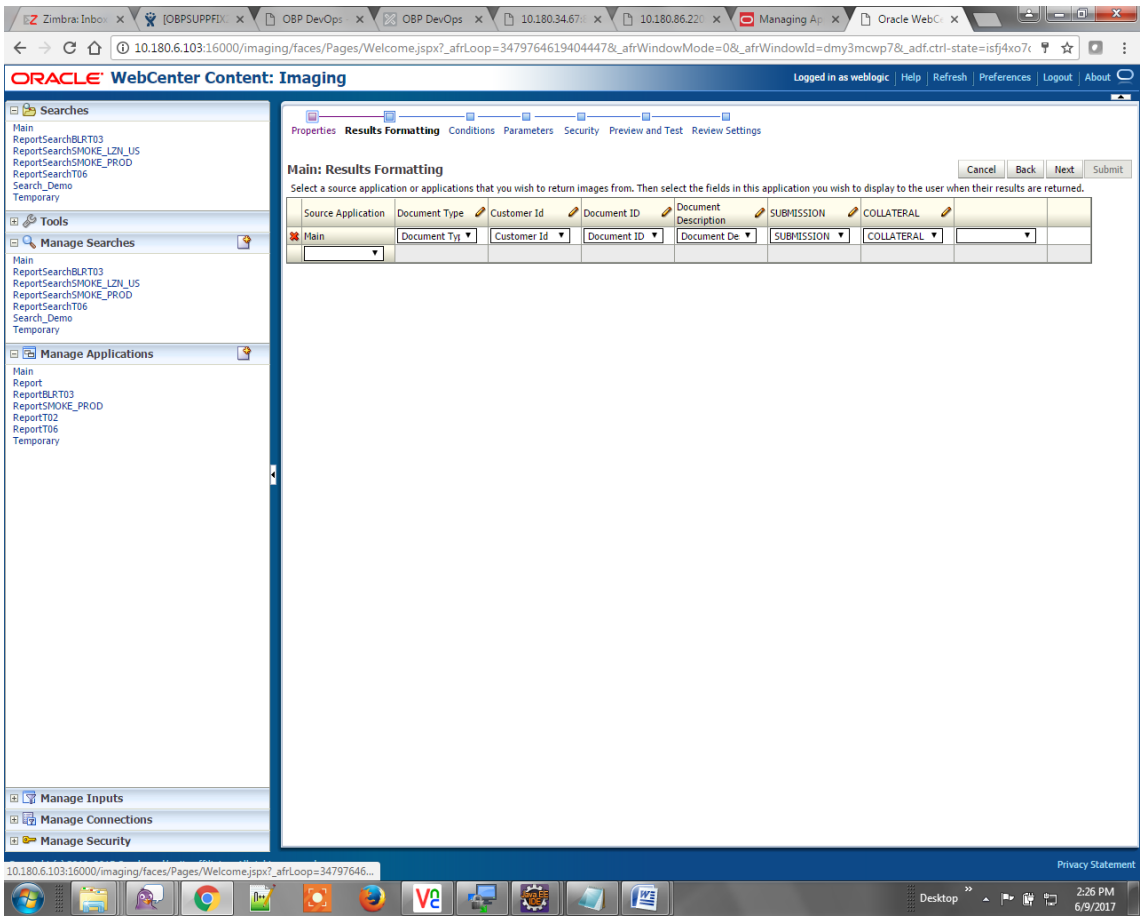
1. Click Manage Searches option and enter the search name with description.

Figure 7–15 Main: Properties



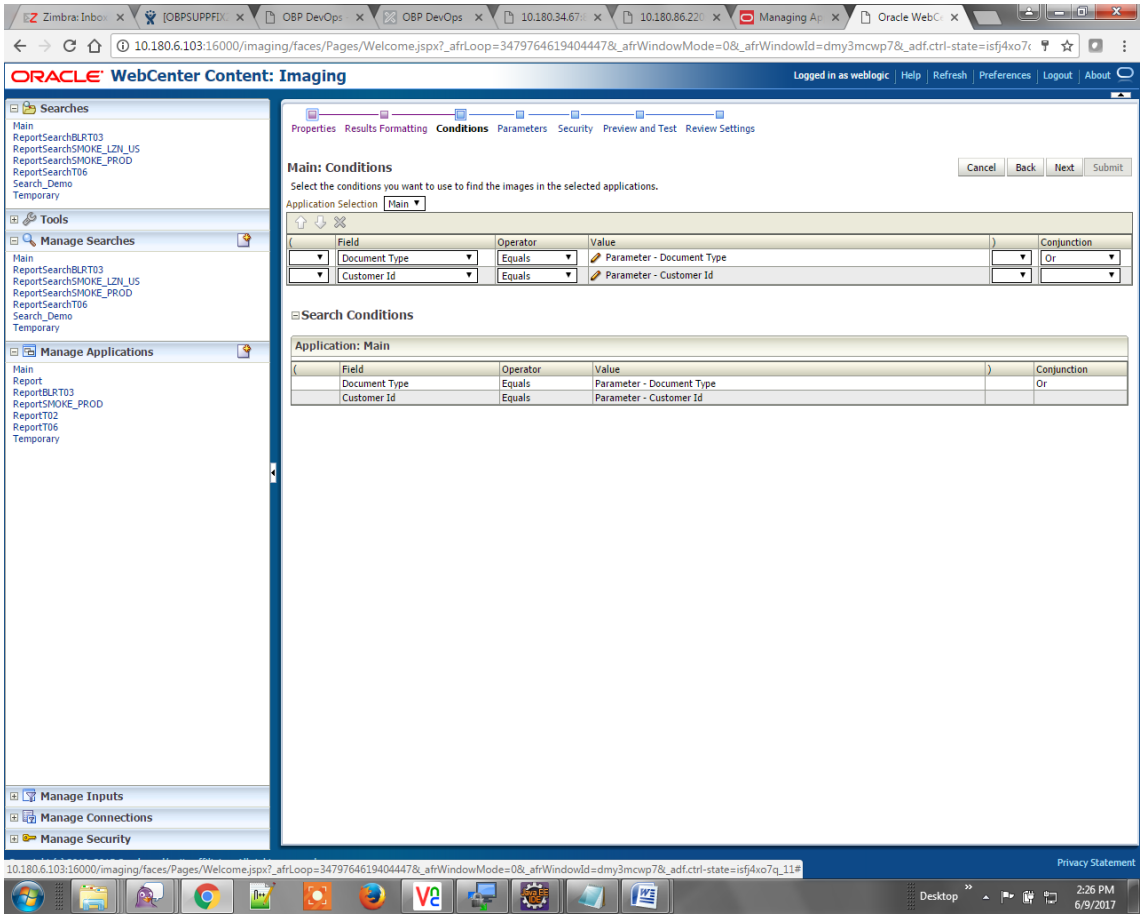
2. Click **Next.**
3. Select the source application along with its field details in the Results Formatting page.

Figure 7–16 Main: Results Formatting



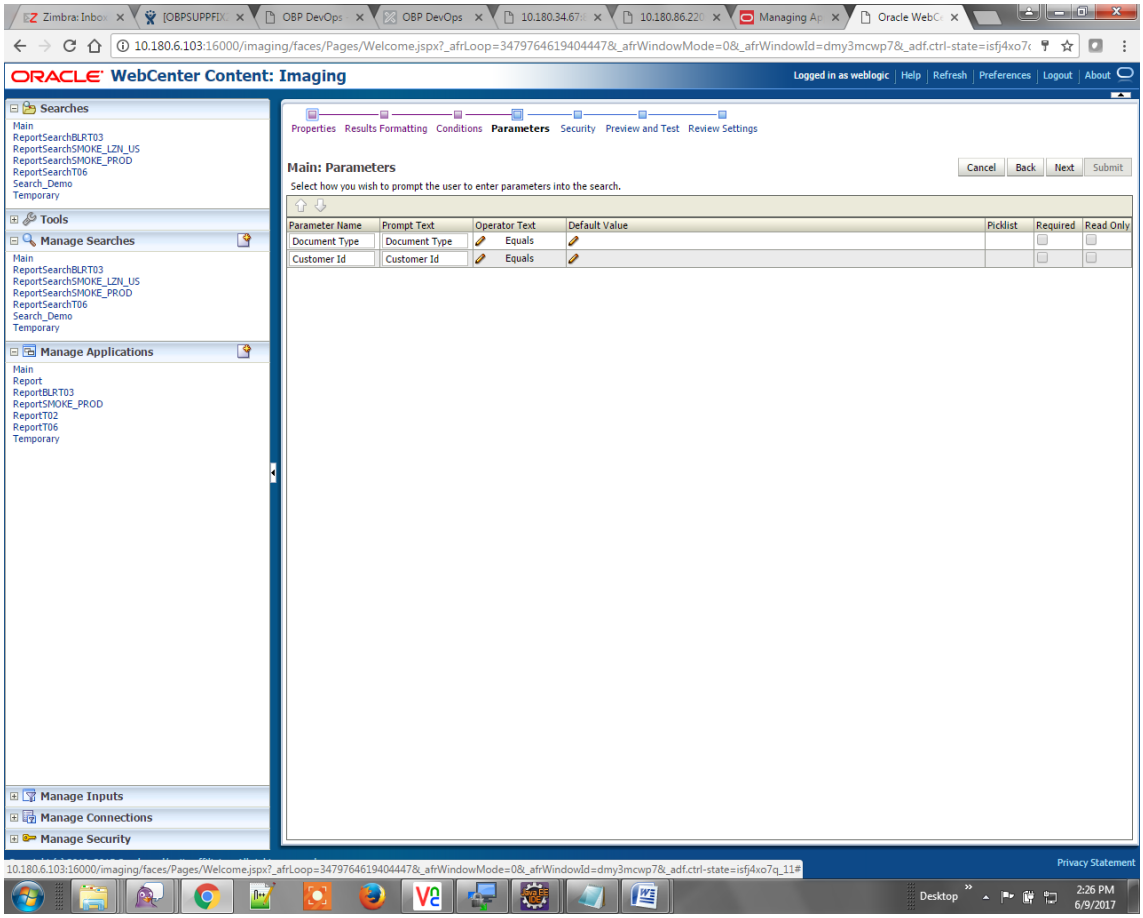
4. Select the appropriate conditions in the Conditions page as shown below.

Figure 7–17 Main: Conditions



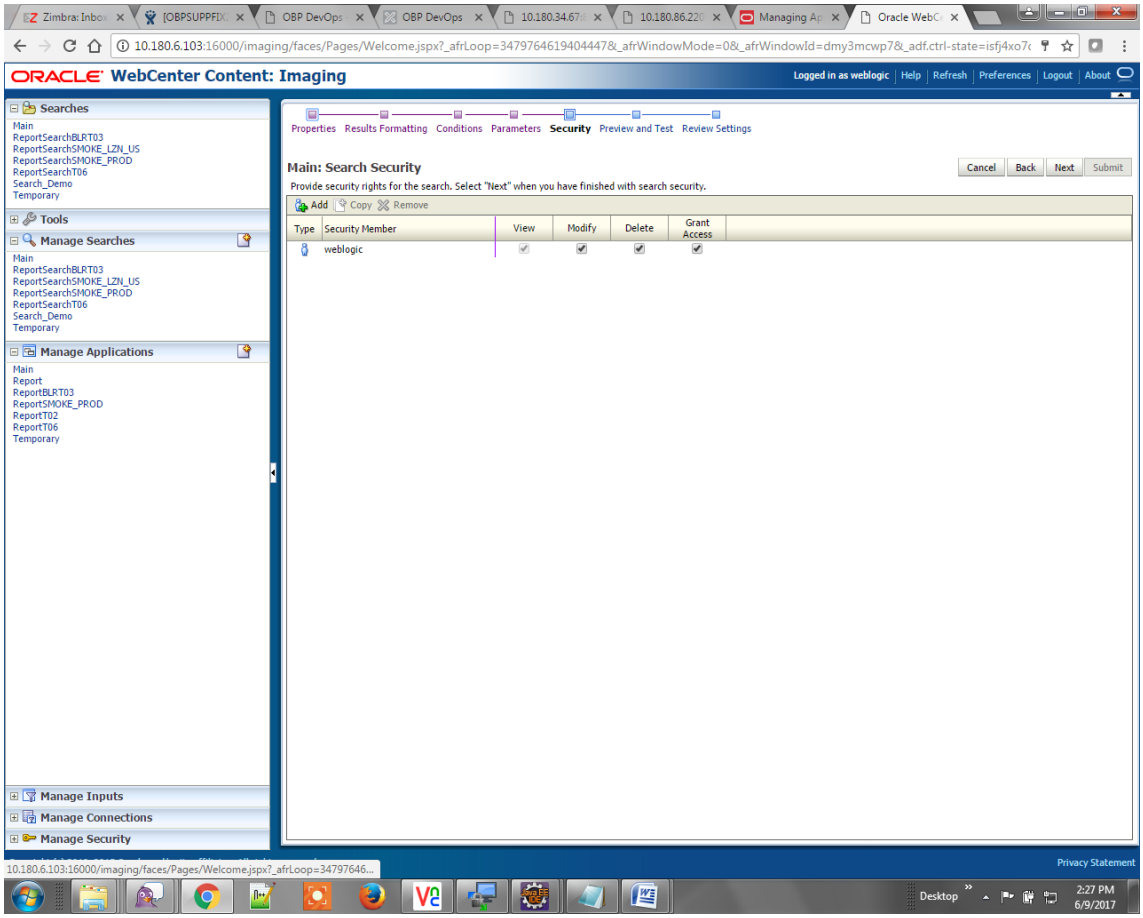
5. Select the appropriate settings in the Parameters page as shown below.

Figure 7–18 Main: Parameters



6. Configure the access rights for users for search in the Search Security page.

Figure 7–19 Main: Search Security



7. Review the summary and click **Submit.**

Figure 7–20 Main: Preview and Test

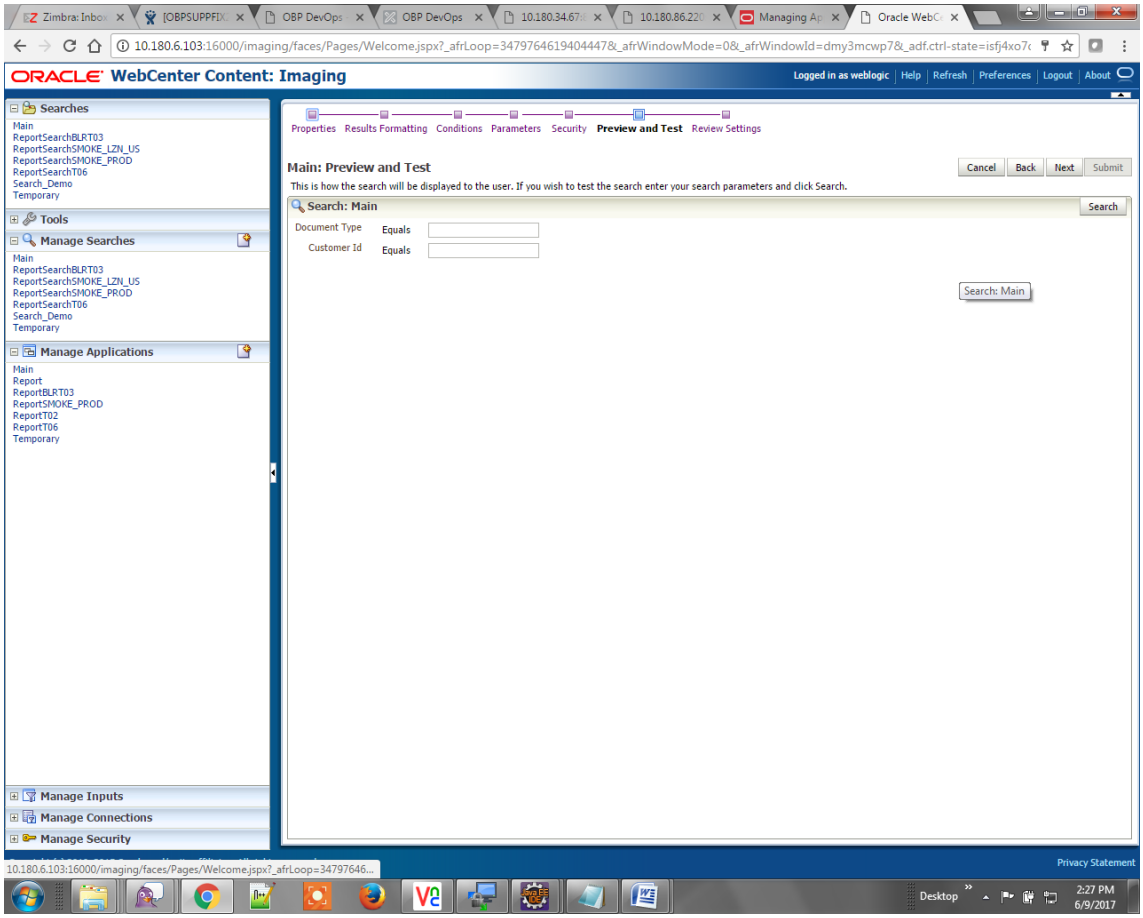
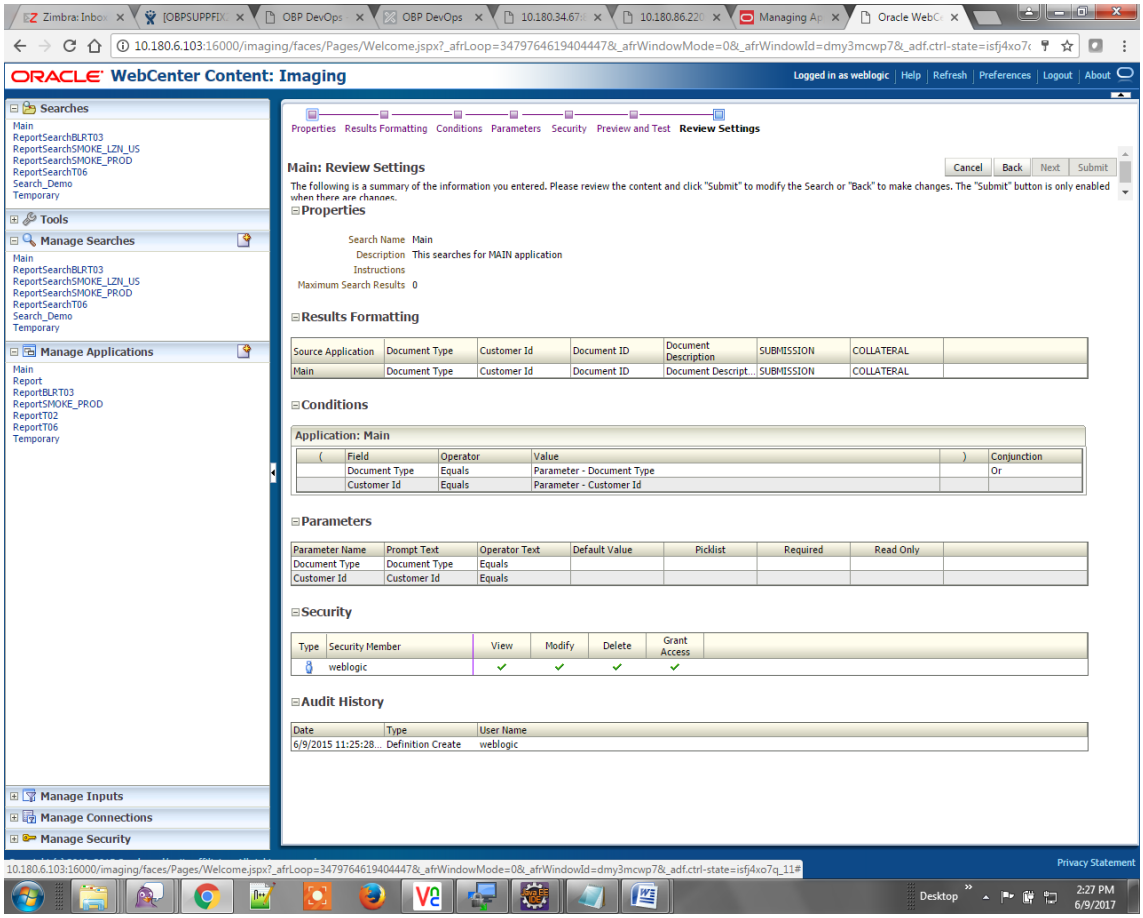


Figure 7–21 Main: Review Settings



7.1.3 Temp Application Configuration

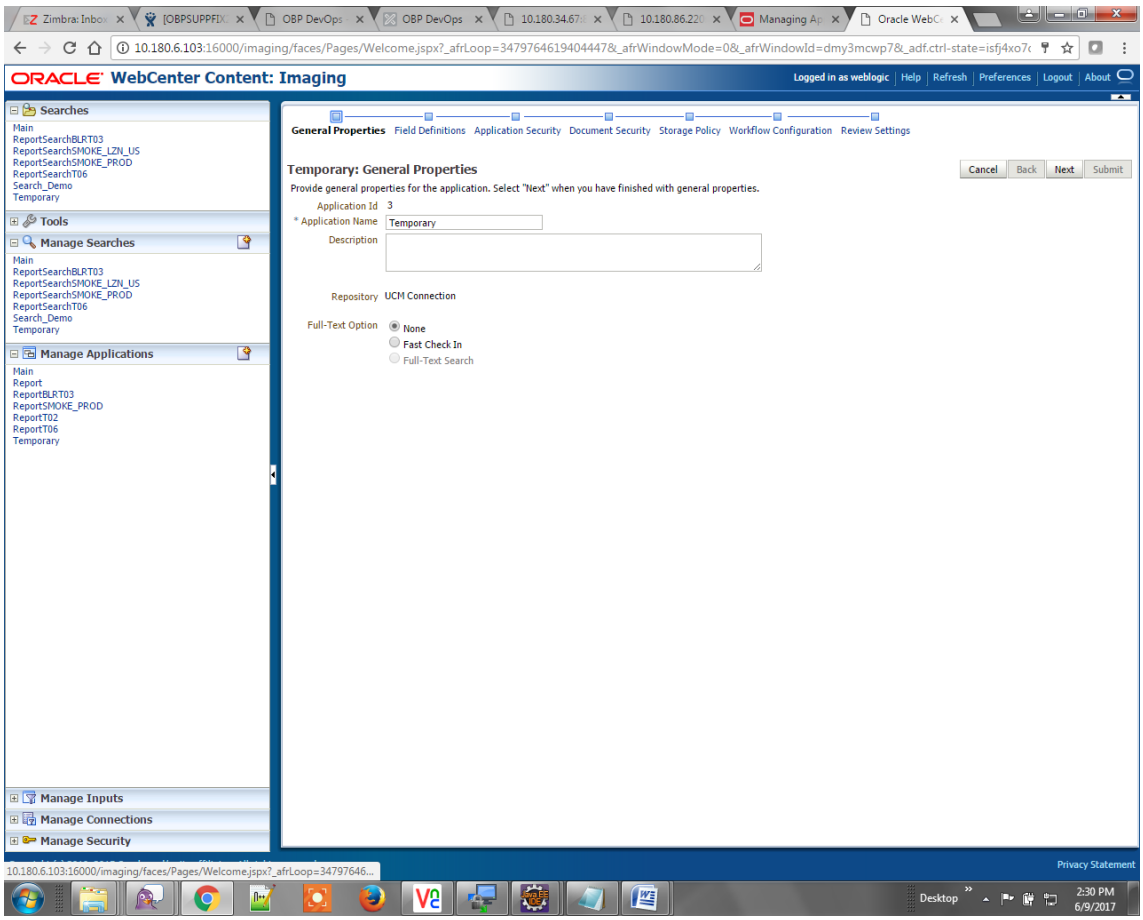
This section provides details about the temp application configuration.

7.1.3.1 Manage Application Configuration

To manage application configuration:

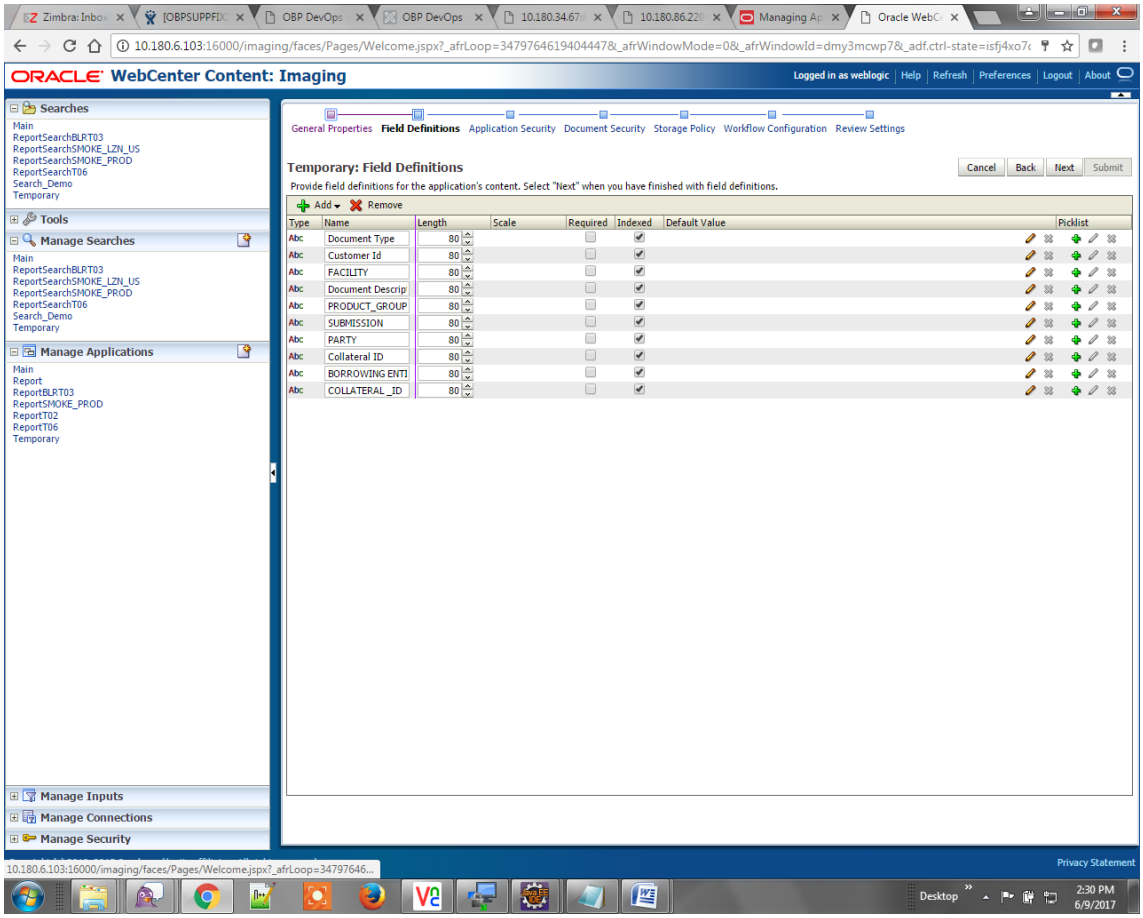
1. Select the Create New Application option.
2. Enter the general properties and click **Next.**

Figure 7–22 Temporary: General Properties



3. Enter the field definition details and click **Next.**

Figure 7–23 Temporary: Field Definitions



4. In Application Security and Document Security pages, select the access rights for users and click **Next.**

Figure 7–24 Temporary: Application Security

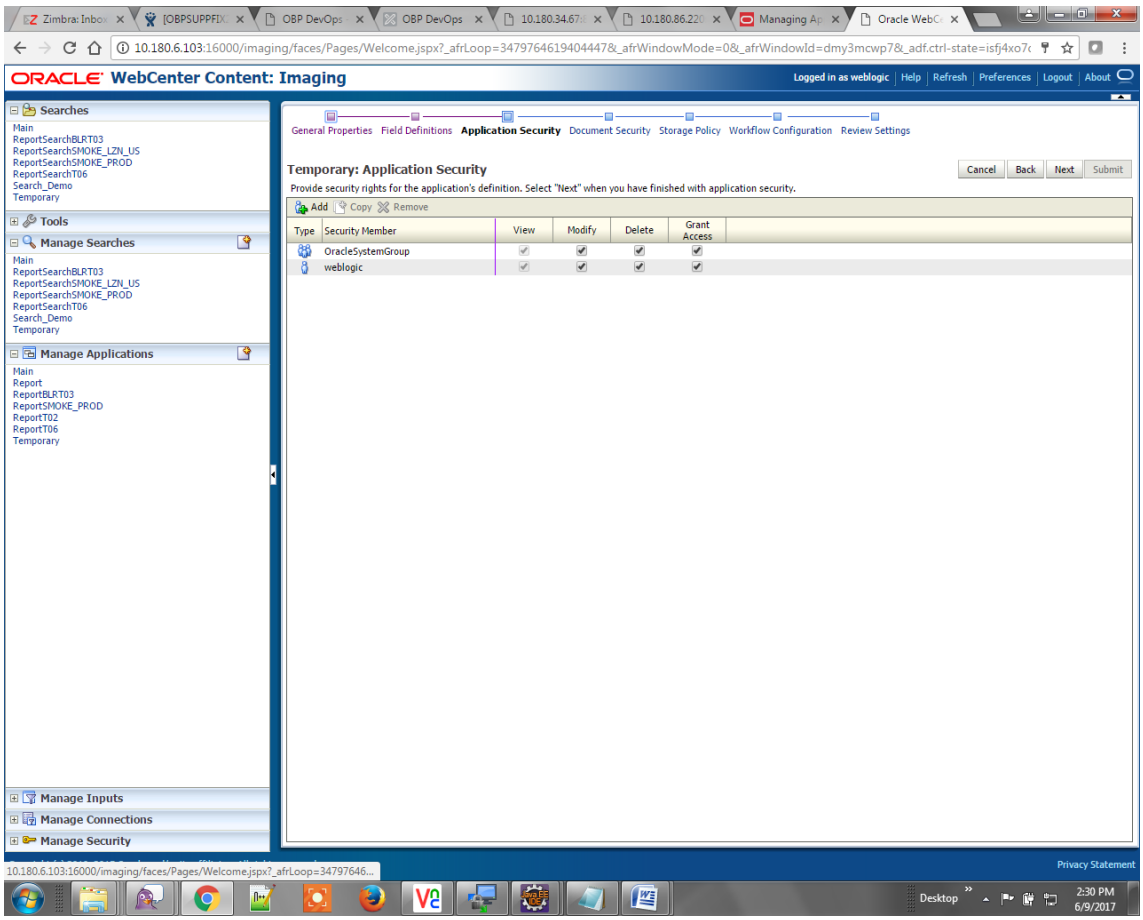
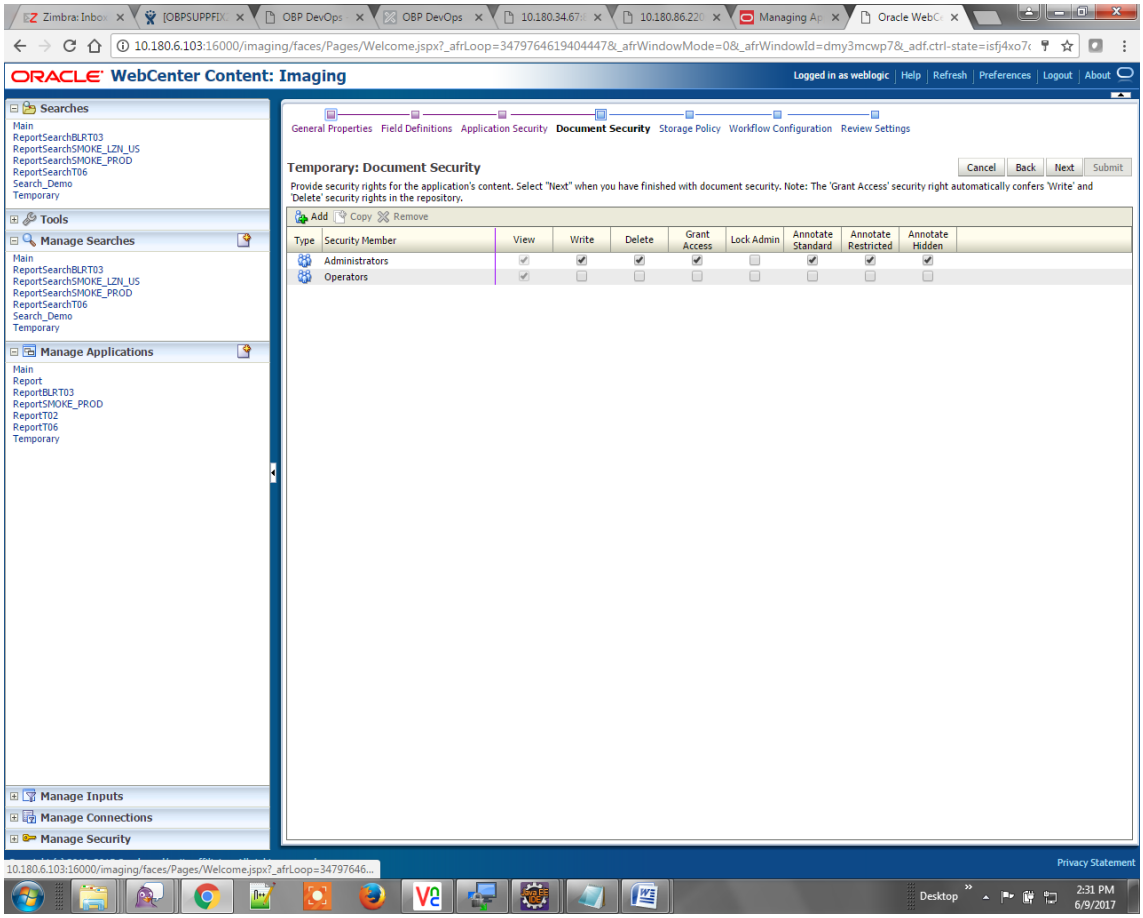
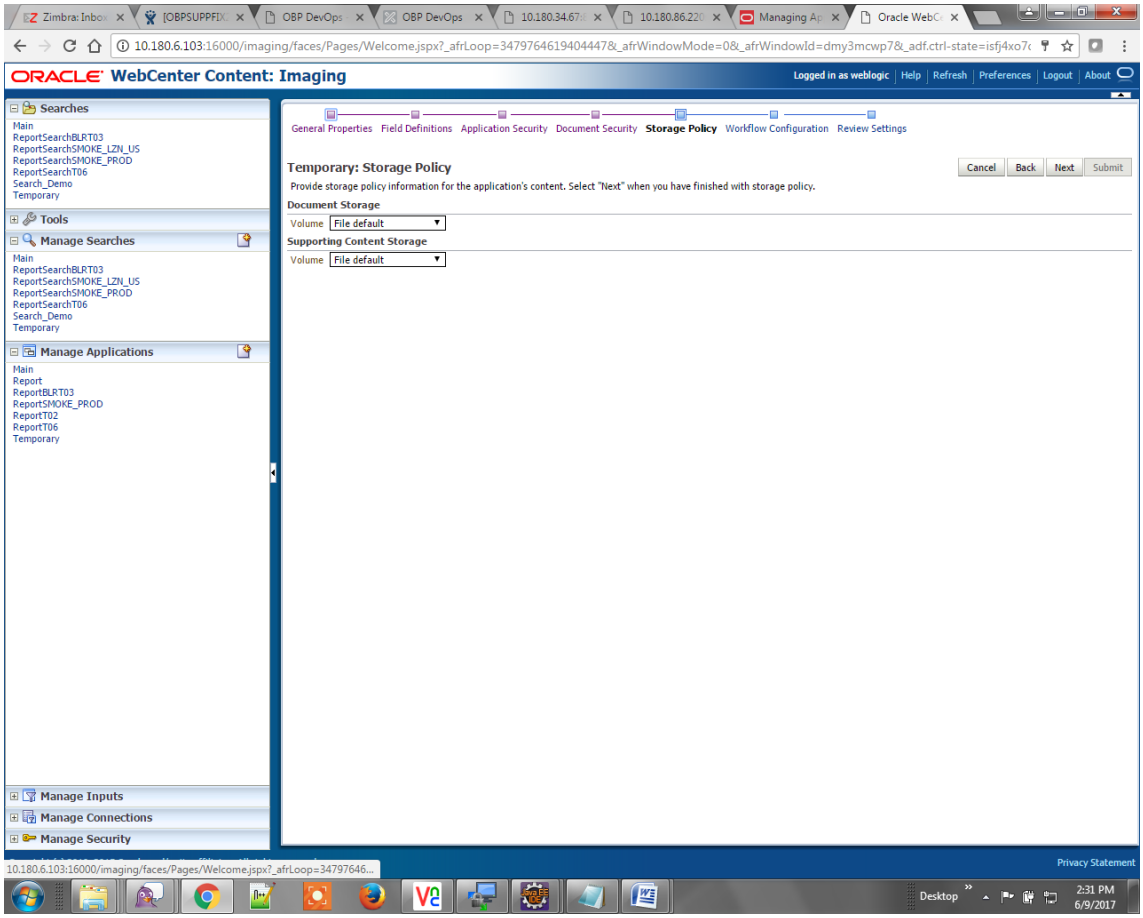


Figure 7–25 Temporary: Document Security



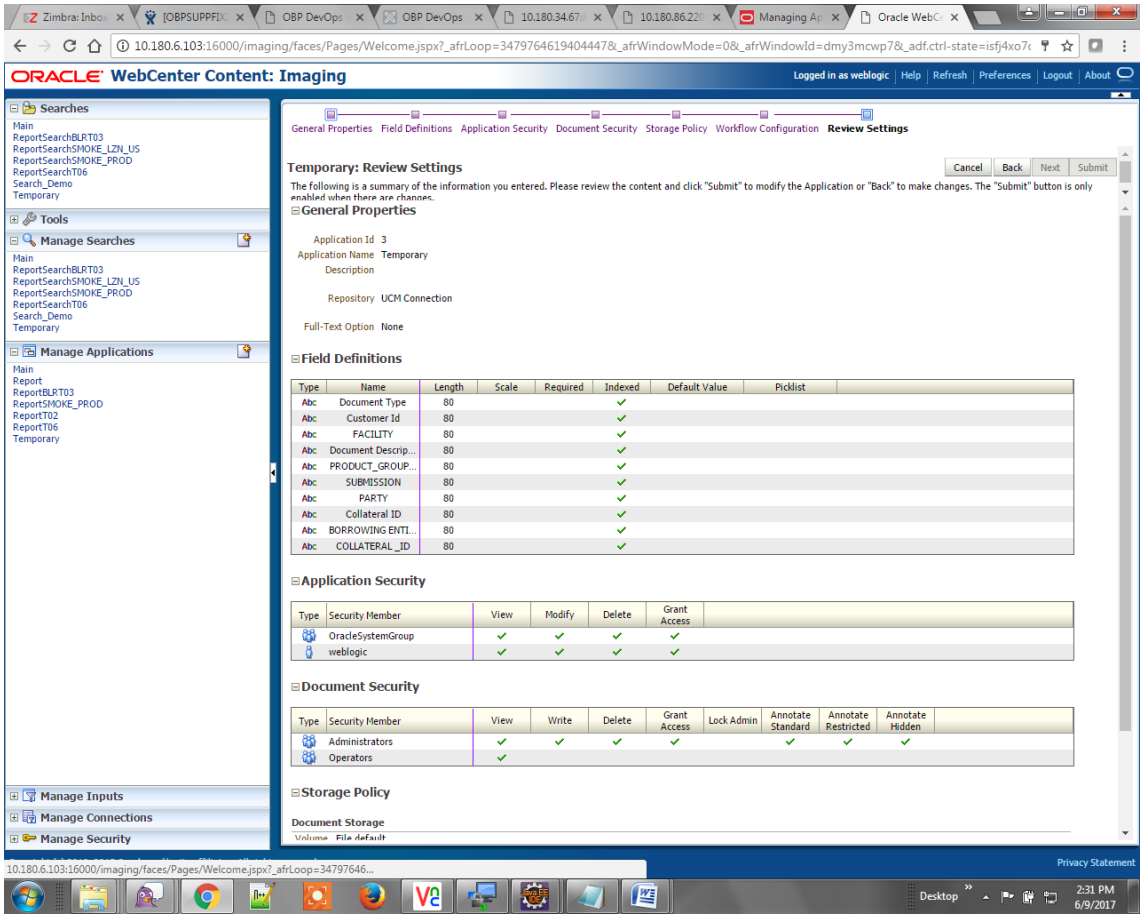
5. In the Storage Policy page, select the file default option has shown below.

Figure 7–26 Temporary: Storage Policy



6. Click **Next.** Skip the Workflow Configuration page.
7. Click **Next.**
8. Review the summary and click **Submit.**

Figure 7–27 Temporary: Review Settings

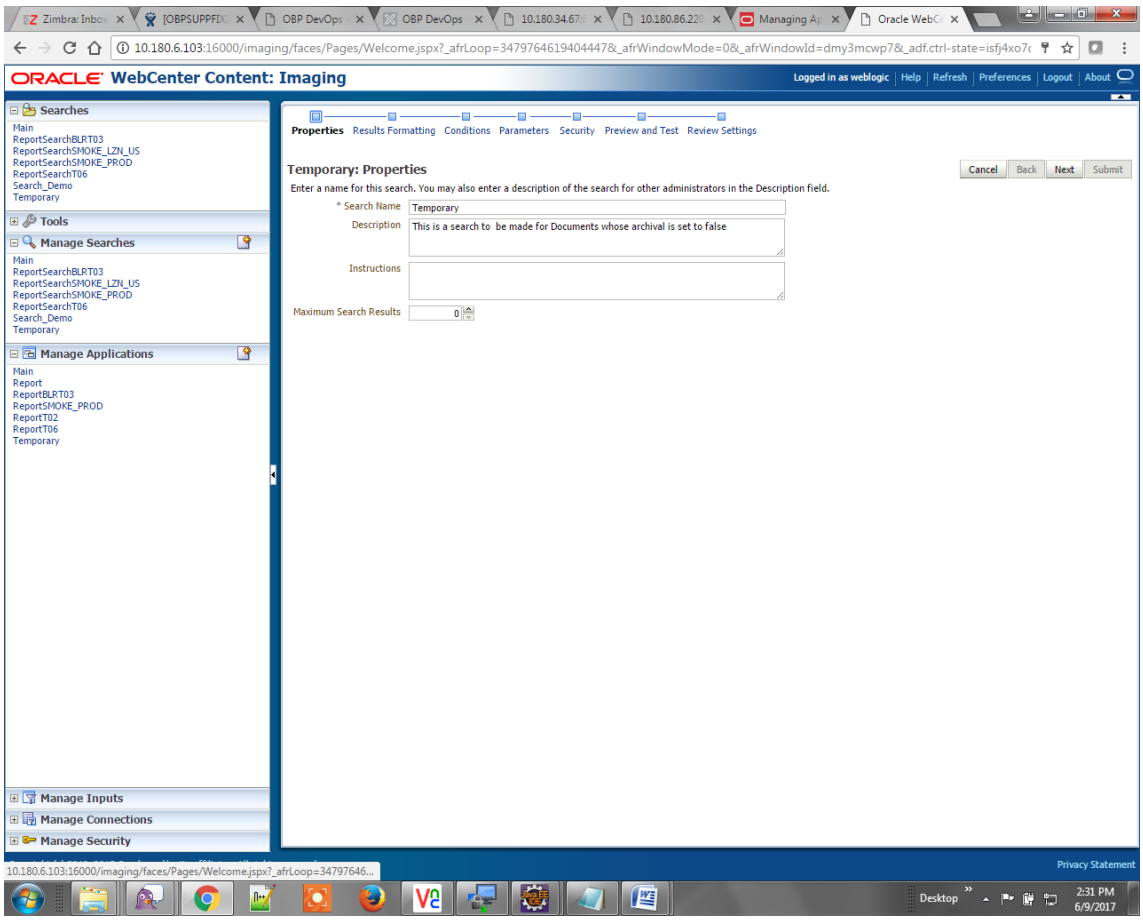


7.1.3.2 Manage Searches

To manage searches:

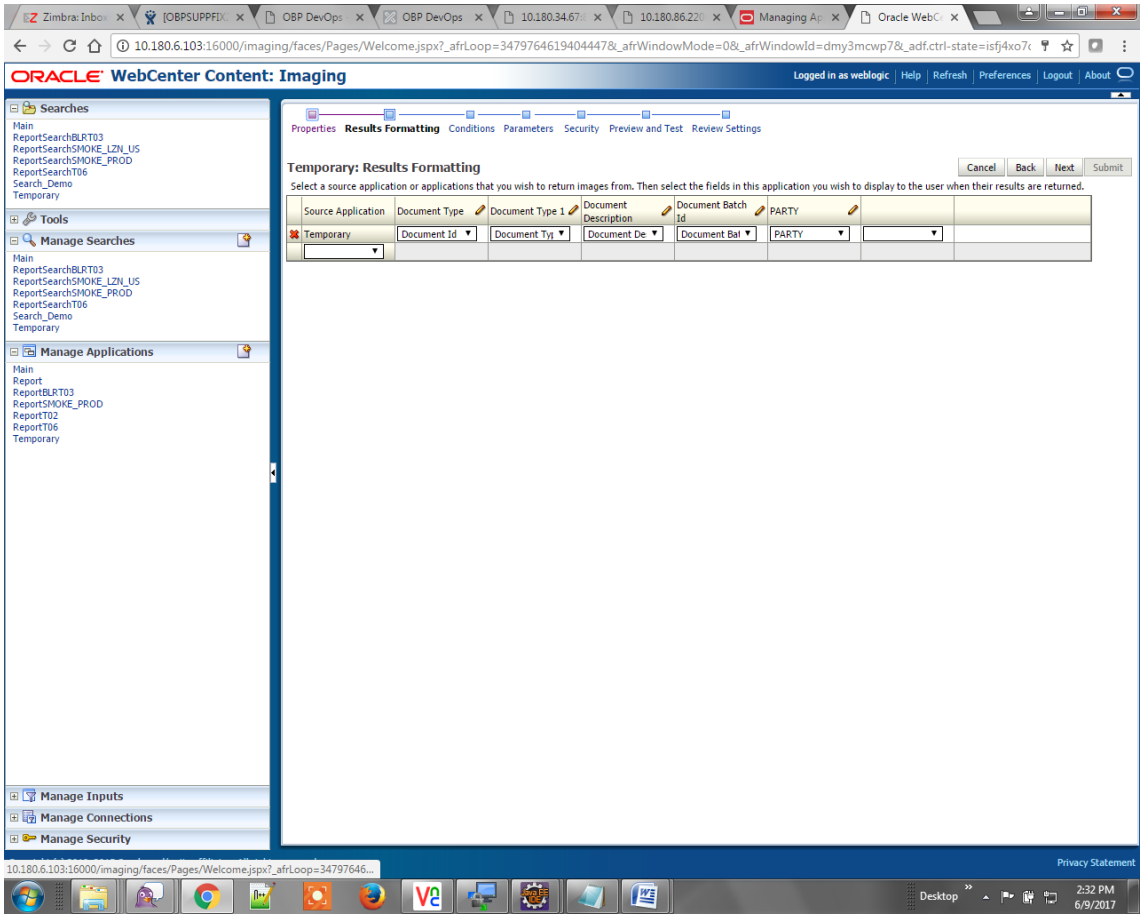
1. Click the Manage Searches option and enter the search name with description.

Figure 7–28 Temporary: Properties



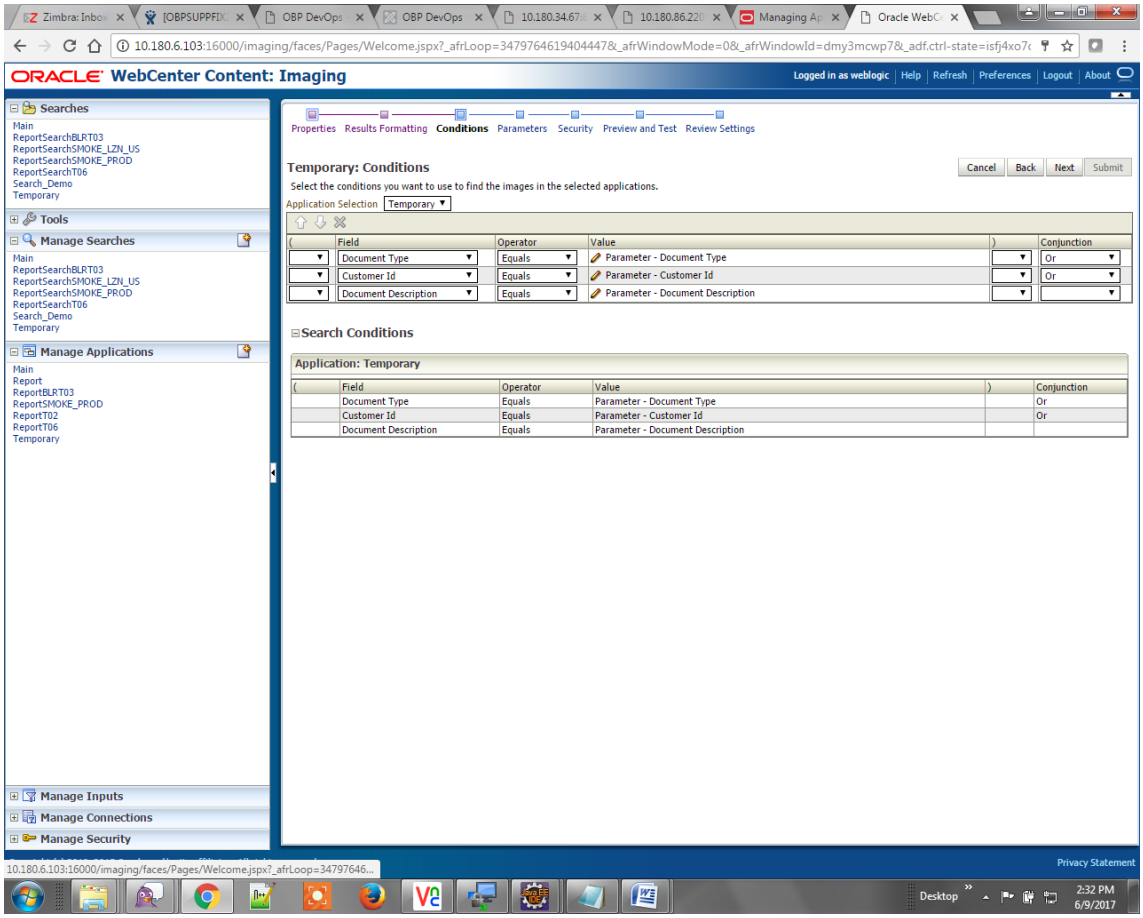
2. Select the source application along with its field details in the Results Formatting page.

Figure 7–29 Temporary: Results Formatting



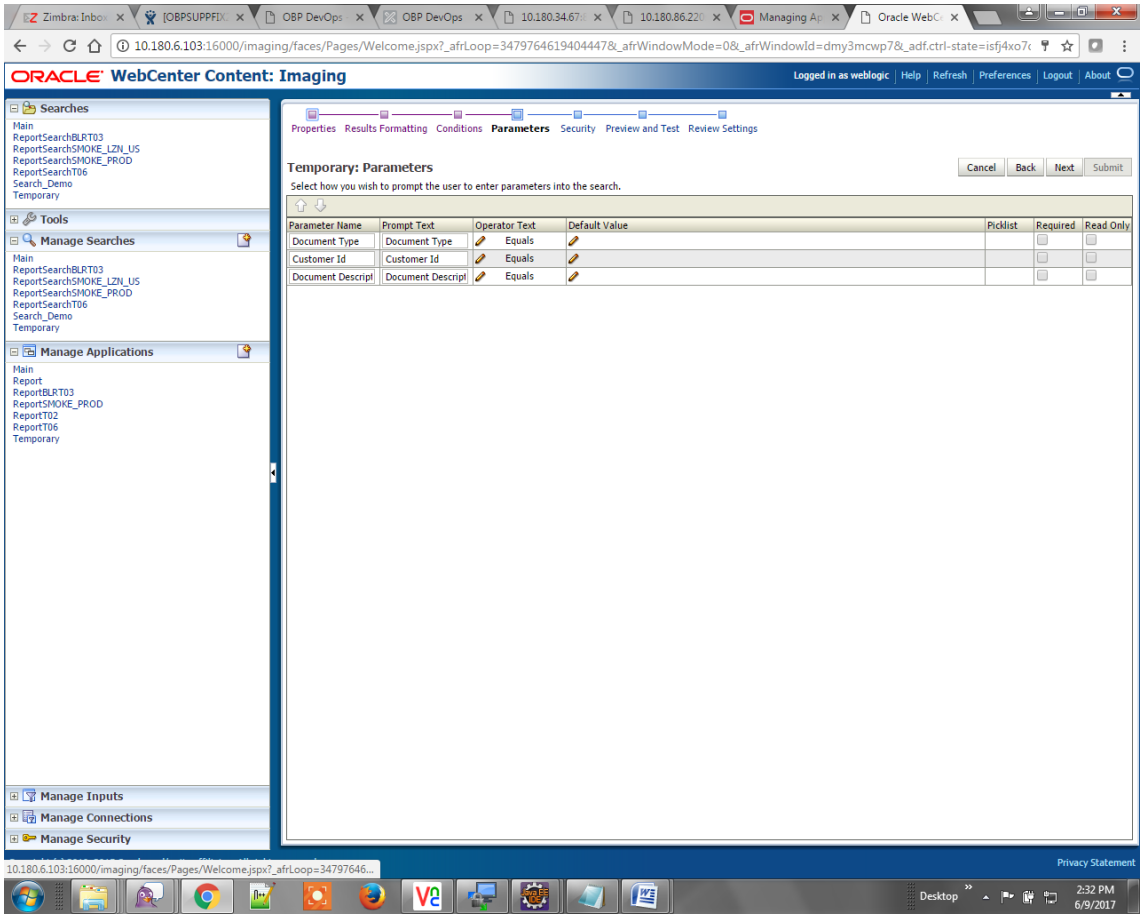
3. Select the appropriate conditions in the Conditions page as shown below.

Figure 7–30 Temporary: Conditions



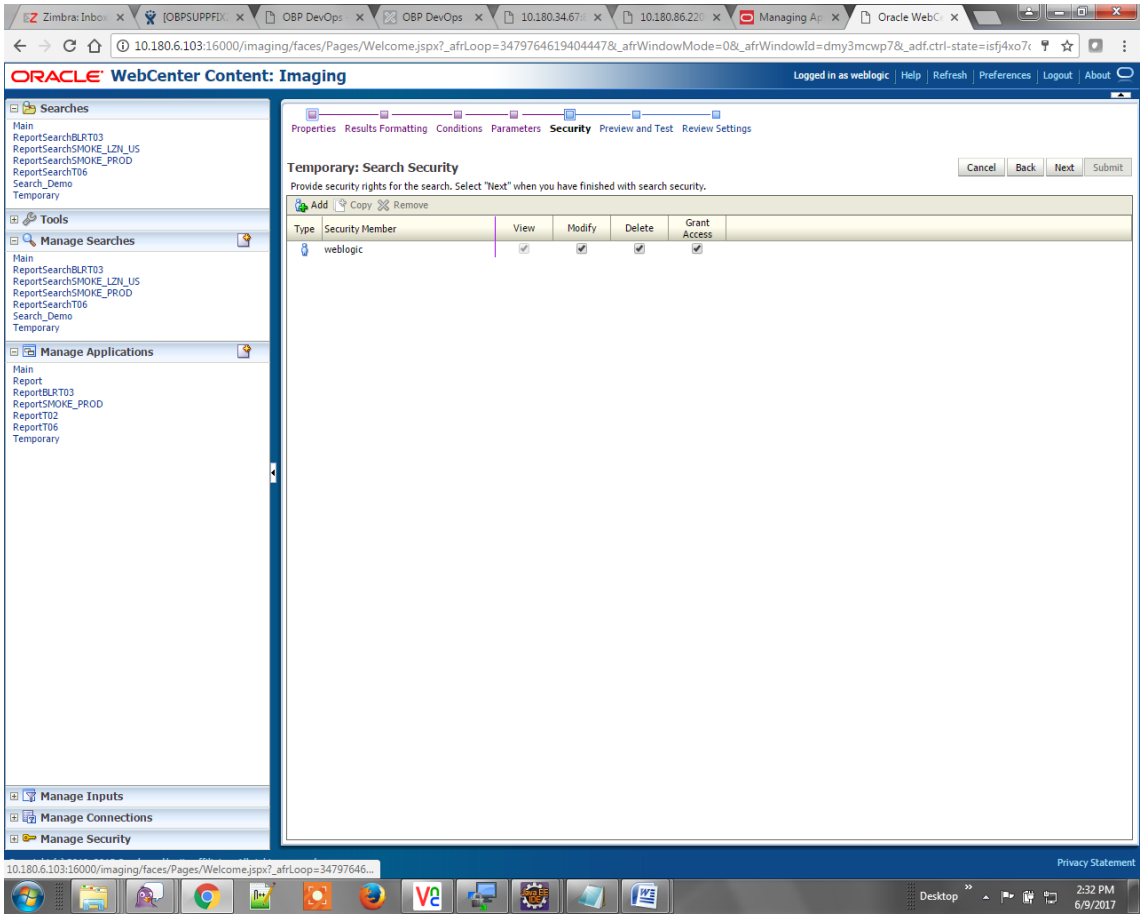
4. Select the appropriate settings in the Parameters page as shown below.

Figure 7–31 Temporary: Parameters



5. Configure the access rights for users for search in the Search Security page.

Figure 7–32 Temporary: Search Security



6. Review the summary and click **Submit.**

Figure 7–33 Temporary: Preview and Test

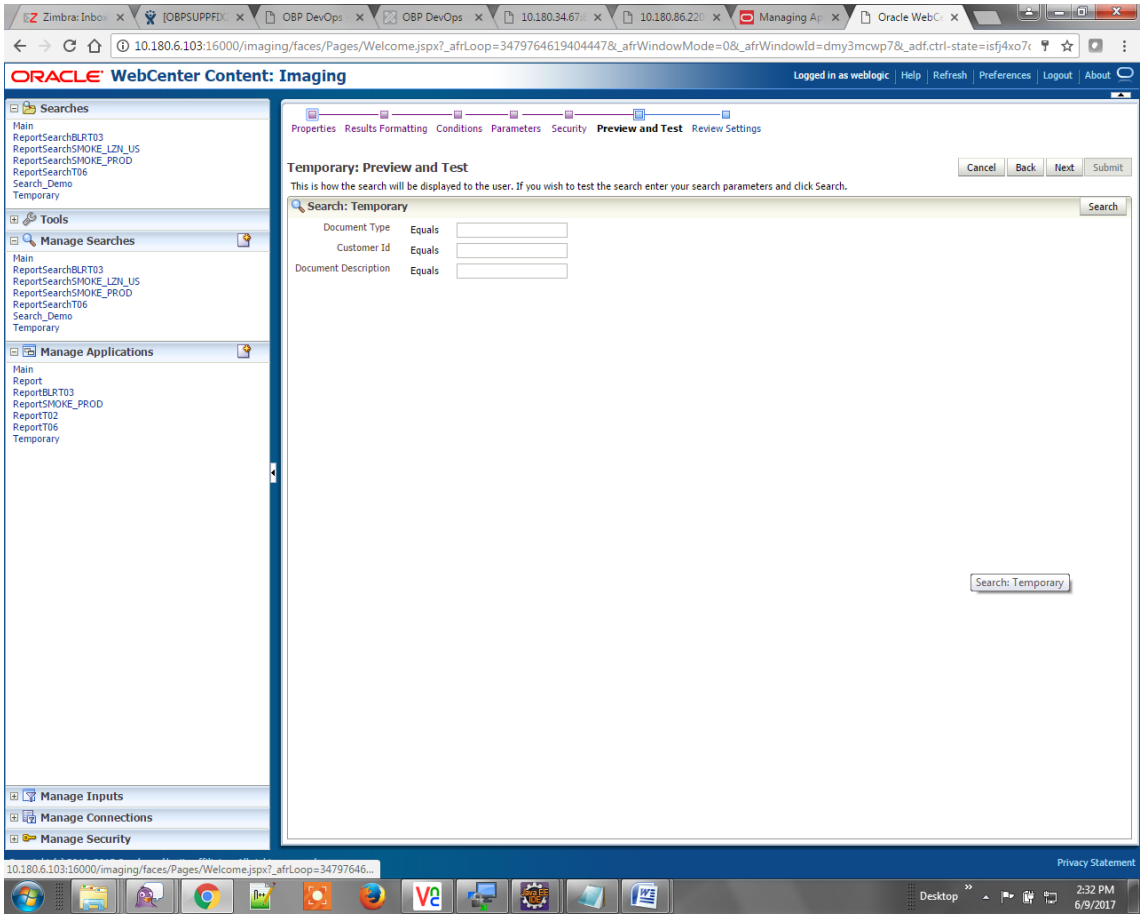
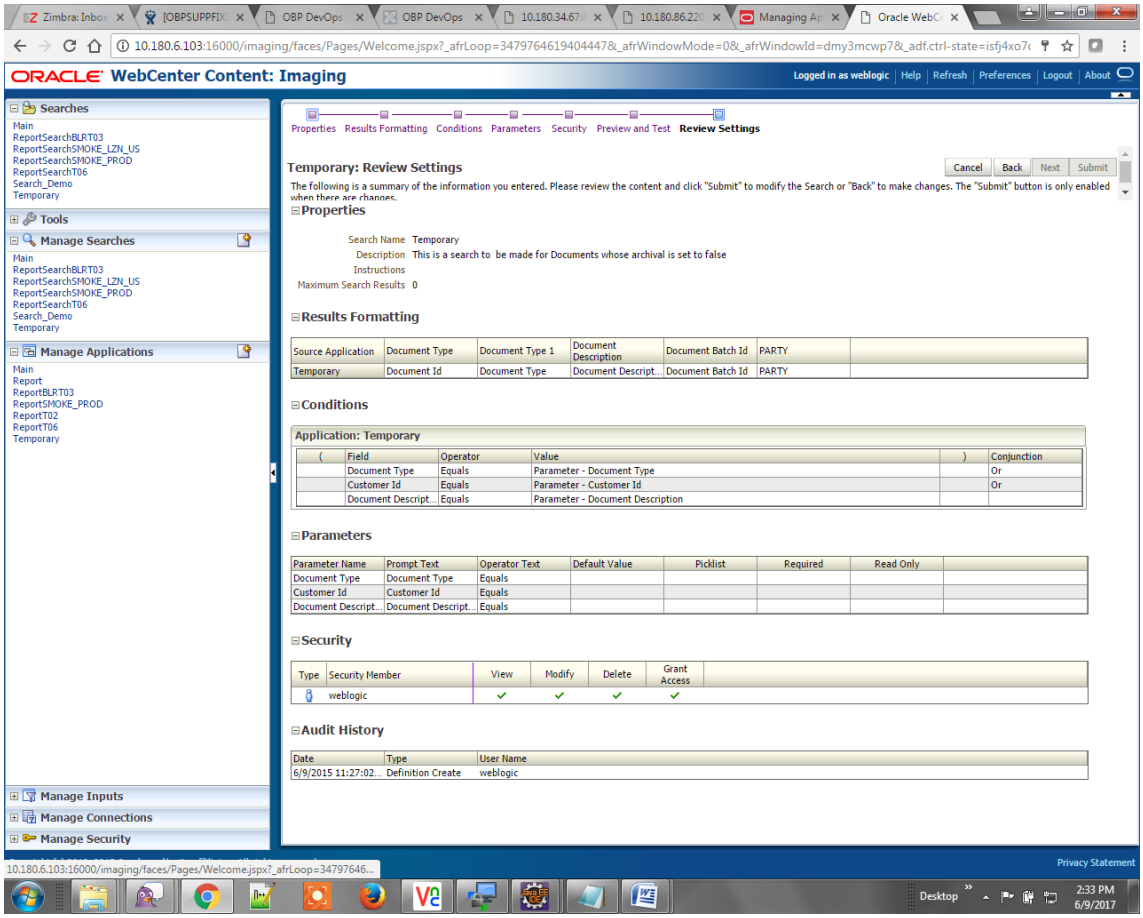


Figure 7–34 Temporary: Review Settings



The application ID generated for the main and temporary applications should be updated in the OBDLOCS DB schema table flx_cm_doc_typ_meta_data using the following sql statements:

> **Note**
>
> Replace the <main application id> with the application ID generated for the IPM application and the <temporary application id> with the application ID generated for the IPM application sql statements with the actual generated.

SQL for Main Application

```
update flx_cm_doc_typ_meta_data
set app_id = '<main application id>'
where doc_typ_id = 'MAIN';
```

SQL for Temp Application

```
update flx_cm_doc_typ_meta_data tp
set app_id = '<temporary application id>'
where doc_typ_id = 'TEMP';
```

7.2 IPM Configuration for Bulk Upload Process Setup

This step is an optional configuration step. It is required only for banks that need to upload documents in bulk. Creation of an input configuration results in defining an input file format and mapping the file input data with the application field definitions. This file format is then understood by the IPM Bulk data upload feature (known as an document upload input agent in IPM), which uploads scanned documents from a shared folder on into IPM.

This upload takes place in the following steps:

A file containing details of the scanned documents to be uploaded is taken as an input from a location on the server. Then IPM uploads the scanned documents as specified in an input definition file.

Then IPM invokes the "IPMBulkUpload" BPEL process deployed on the SOA server as part of the SOA media pack installation process. The BPEL process updates the IPM document reference ID in OBDLOCS for the document record.

7.2.1 Prerequisites

Following are the prerequisites before proceeding with the bulk upload process setup:

1. Application on IPM server is already created on which bulk upload process needs to be configured. For more information to understand the application creation process, see Image Processing and Management Admin Guide.
2. com.ofss.fc.workflow.process.IPMBulkUploadProcess is already deployed on the SOA server.

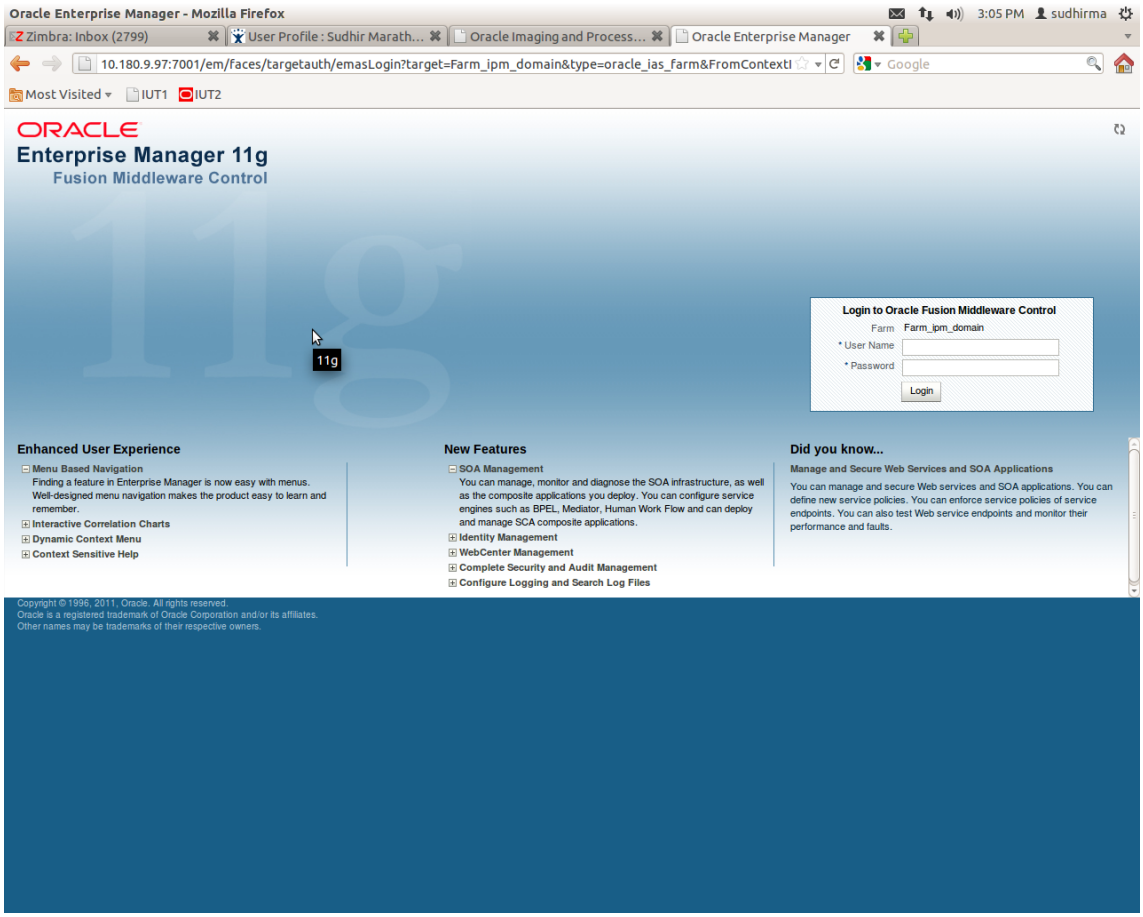
7.2.2 Setting up the Connection Name

To set up a bulk process, start by setting up the connection name, which is used as JNDI for IPM to BPEL connection.

To set up a bulk process:

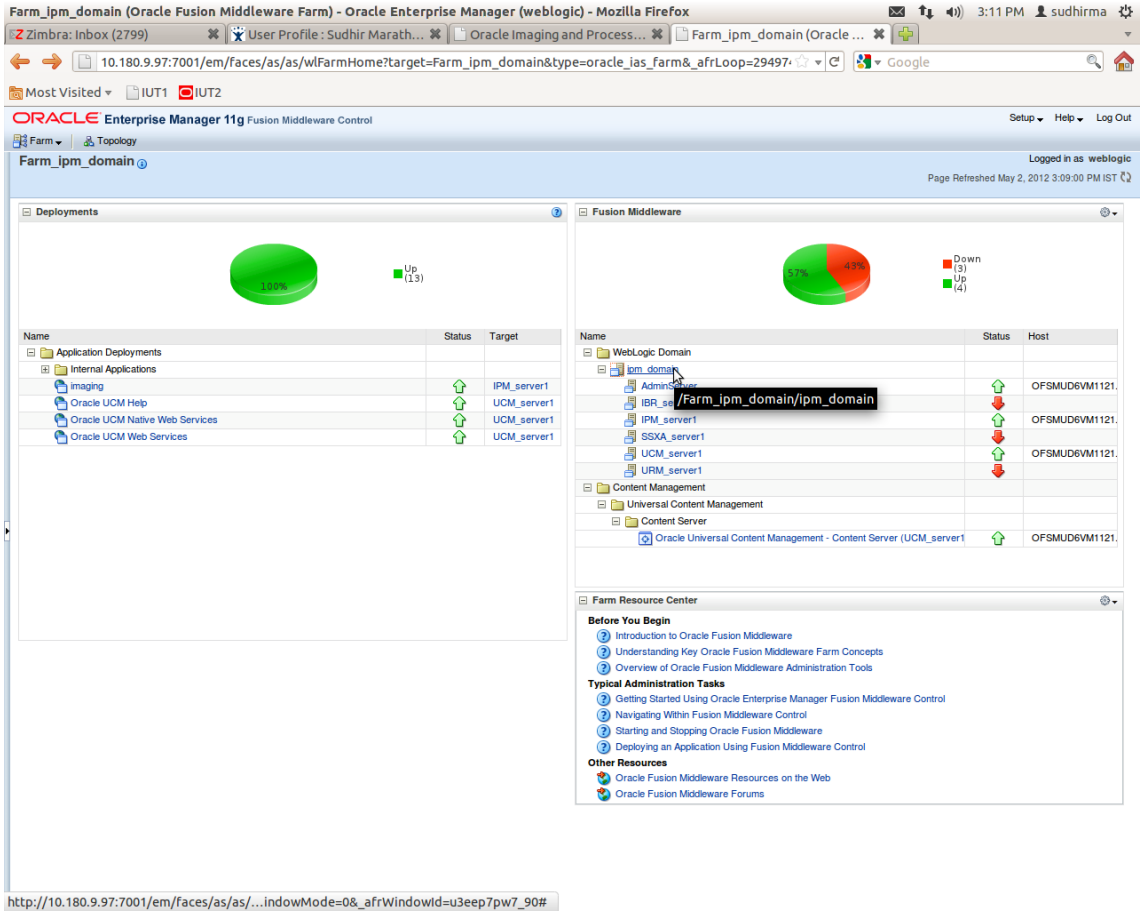
1. Log in to Enterprise Manager (EM) console.

Figure 7–35 EM Console Login



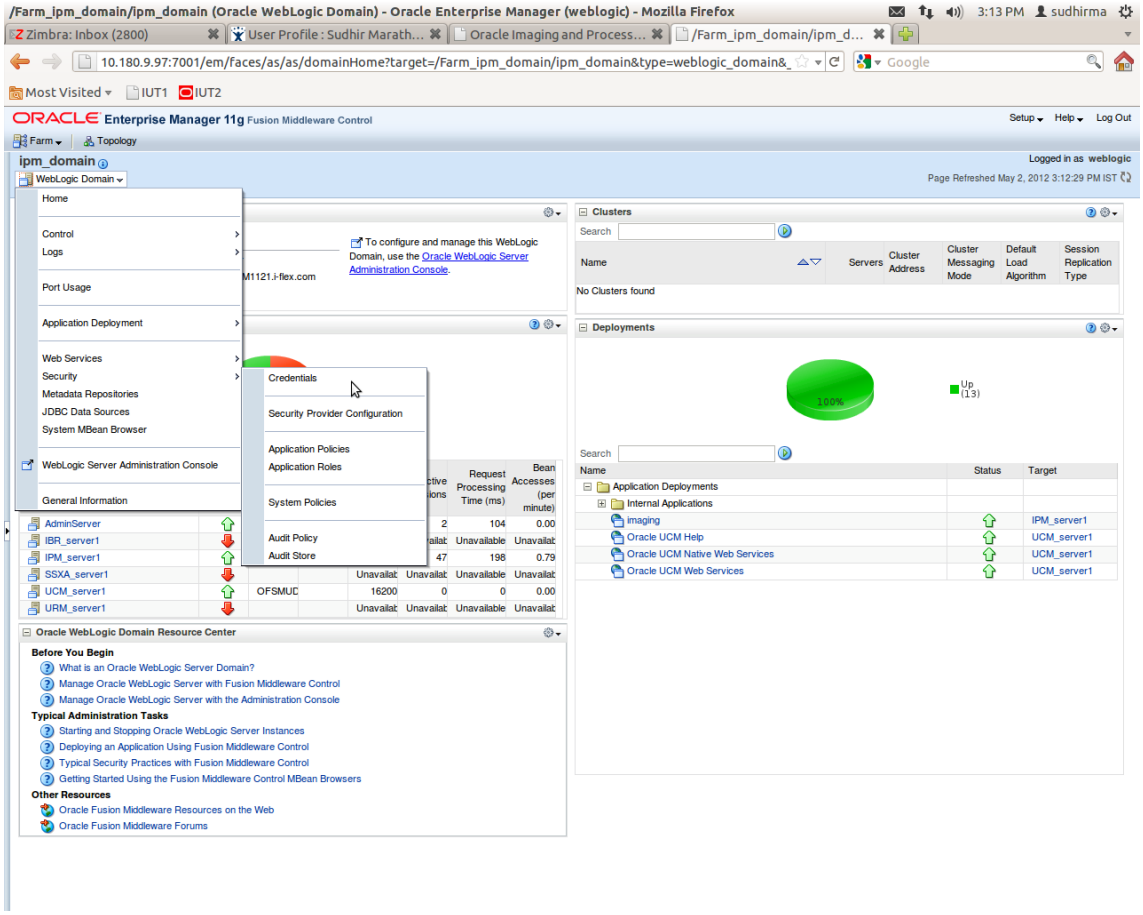
2. In the Name section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 7–36 Click Weblogic Domain: ipm domain



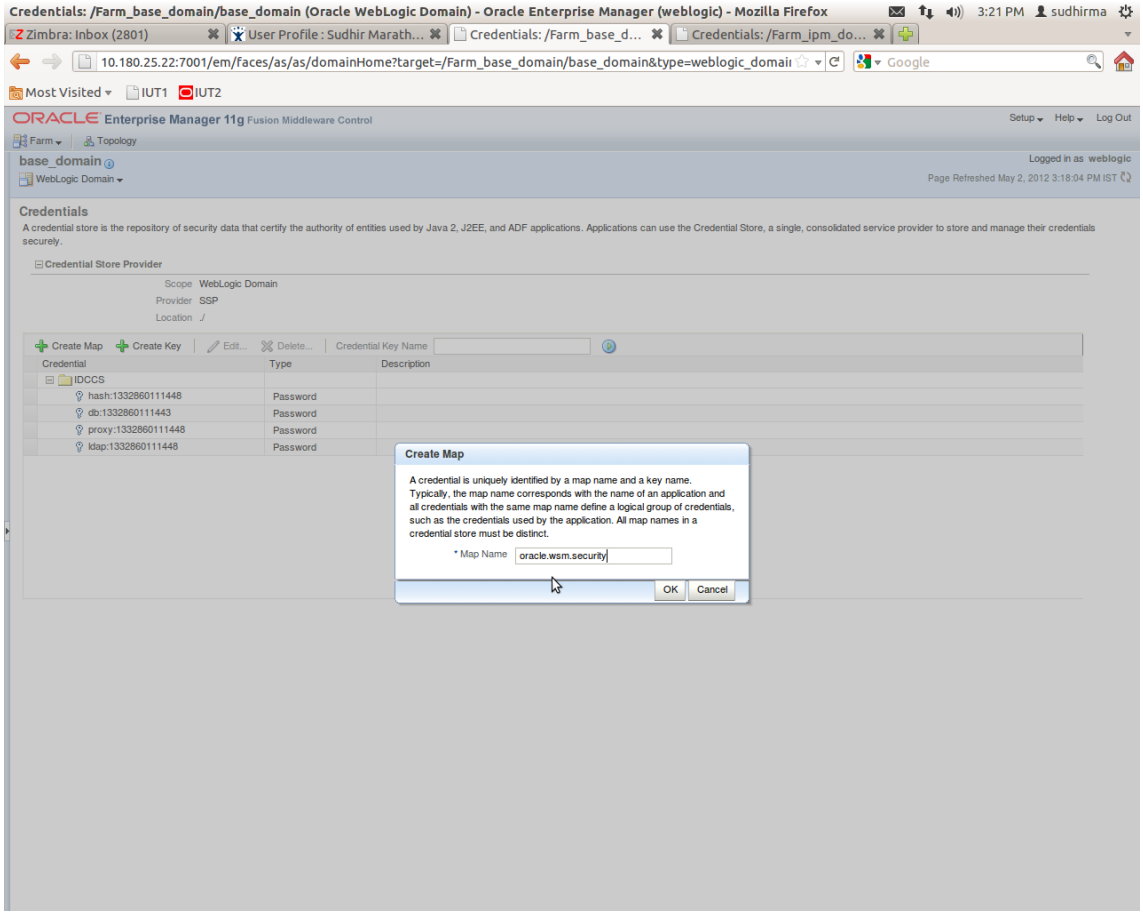
3. In the top menu, **click Weblogic Domain**. The corresponding menu appears.
4. Navigate to **Security > Credentials**. The Credentials page appears.

Figure 7–37 Navigate to Weblogic Domain --> Security --> Credentials



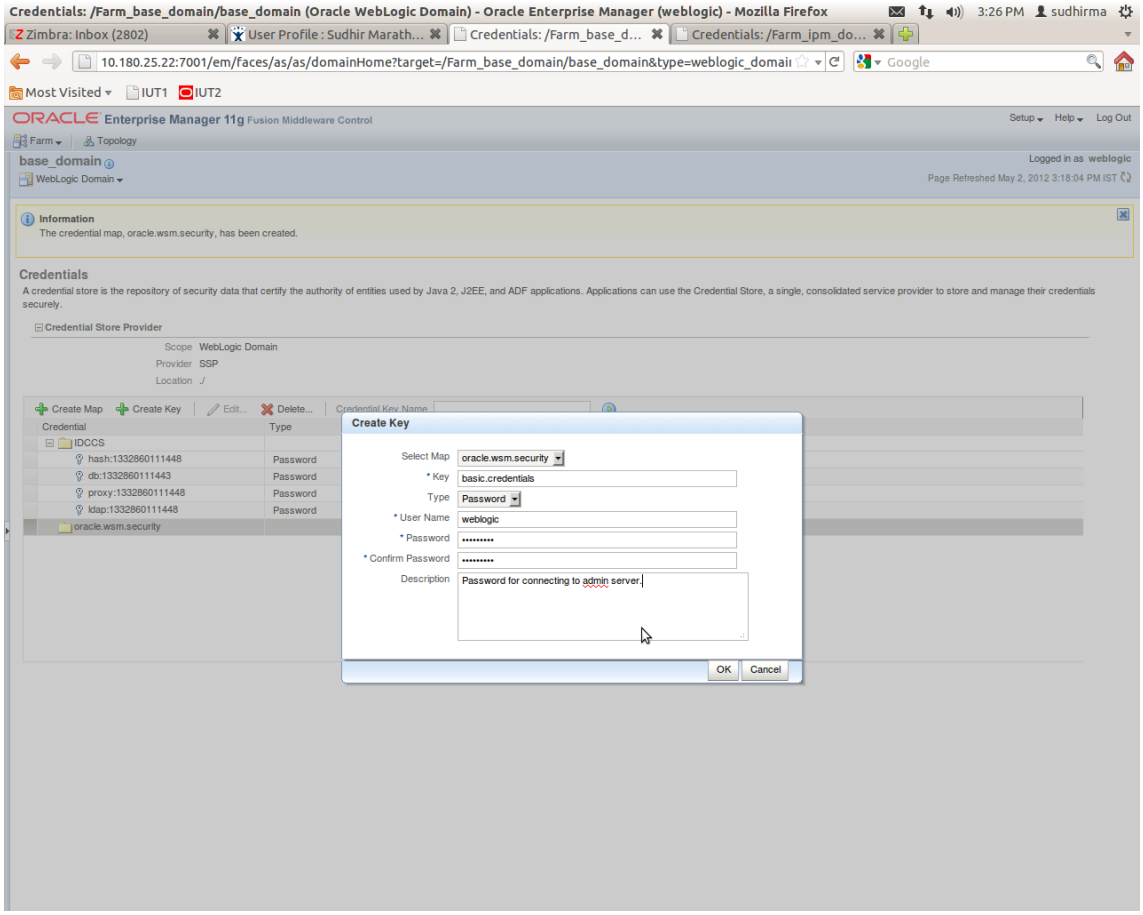
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 7–38 Create Map oracle.wsm.security



6. Click **Create Key** to create a key under the map **oracle.wsm.security.**.

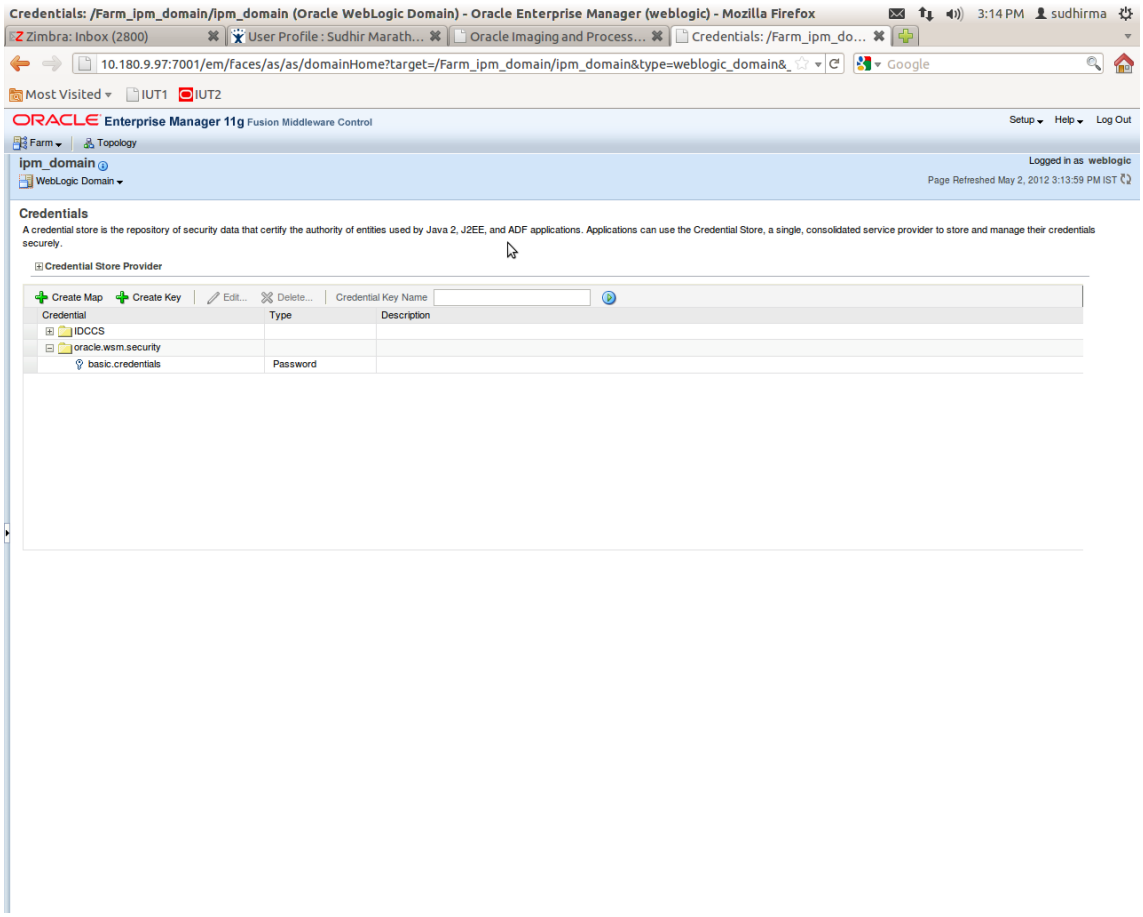
Figure 7–39 Create Key basic.credentials



7. In the **Key** field enter the key name as basic.credentials.
8. In the **Type** field, select the value as Password.
9. Enter the other required details.

10. Click **Ok.** The key is saved.

Figure 7–40 ipm_domain: Credentials Created

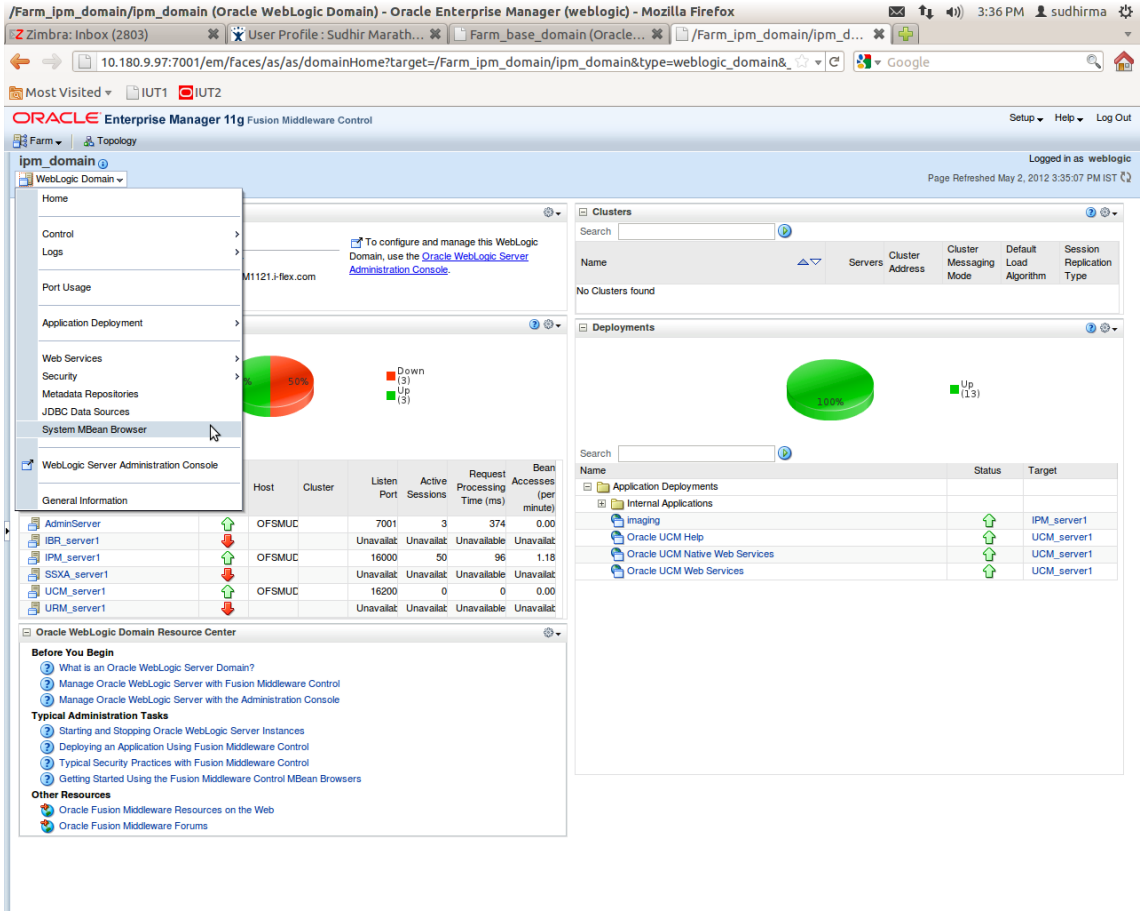


7.2.3 Setting up Input Agent Path

To set up input agent path:

1. Log in to Enterprise Manager (EM) console.
2. In the Name section, under Weblogic domain, click **ipm domain.**
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

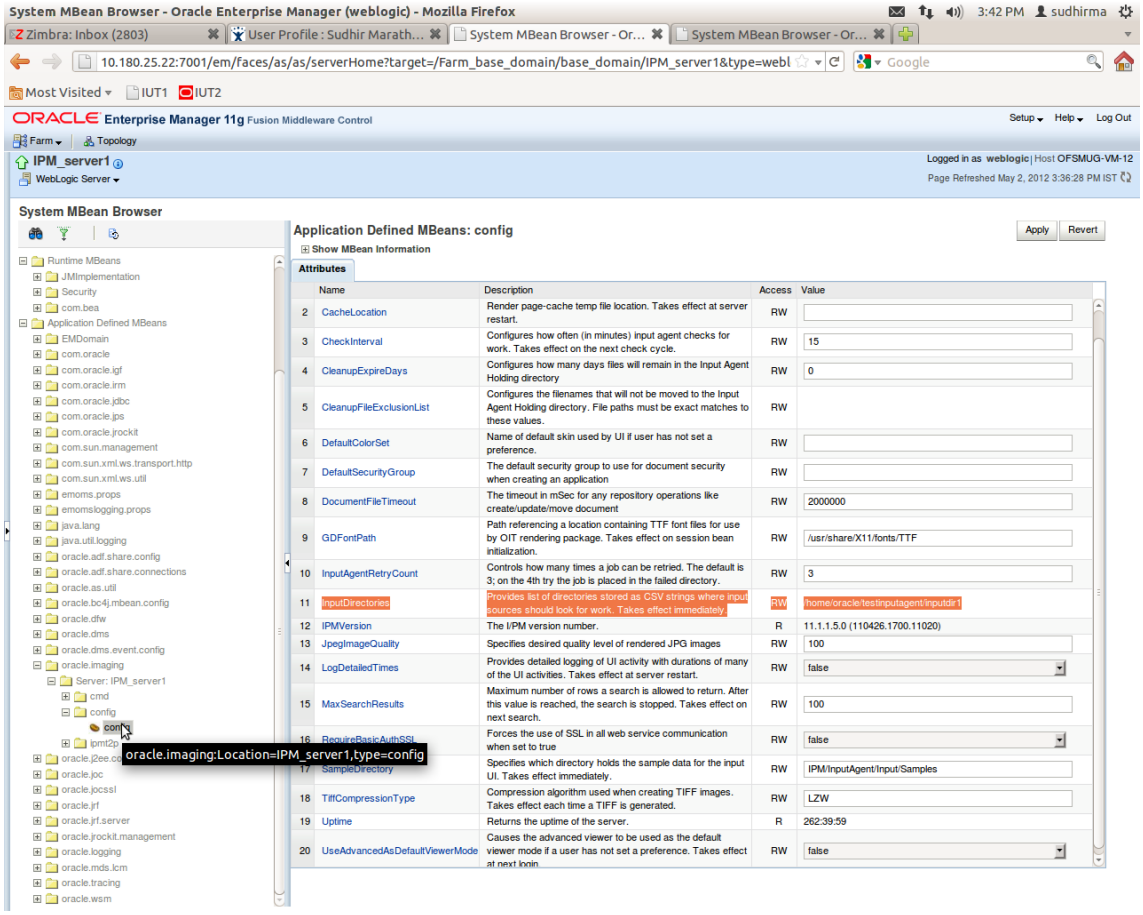
Figure 7–41 Navigate to Weblogic Domain --> System MBean Browser



5. In the left hand pane, navigate to **Application Defined MBeans > oracle.imaging > Server: IPM_ server1 > config.**

6. For the attribute InputDirectories, in the **Value** column enter the value to set the path for input agents.

Figure 7–42 InputDirectories: Enter Input Agent Path



	Name	Description	Access	Value
2	CacheLocation	Render page-cache temp file location. Takes effect at server restart.	RW	
3	CheckInterval	Configures how often (in minutes) input agent checks for work. Takes effect on the next check cycle.	RW	15
4	CleanupExpireDays	Configures how many days files will remain in the Input Agent Holding directory	RW	0
5	CleanupFileExclusionList	Configures the filenames that will not be moved to the Input Agent Holding directory. File paths must be exact matches to these values.	RW	
6	DefaultColorSet	Name of default skin used by UI if user has not set a preference.	RW	
7	DefaultSecurityGroup	The default security group to use for document security when creating an application	RW	
8	DocumentFileTimeout	The timeout in mSec for any repository operations like create/update/move document	RW	2000000
9	GDFontPath	Path referencing a location containing TTF font files for use by OIT rendering package. Takes effect on session bean initialization.	RW	/usr/share/X11/fonts/TTF
10	InputAgentRetryCount	Controls how many times a job can be retried. The default is 3; on the 4th try the job is placed in the failed directory.	RW	3
11	InputDirectories	Provides list of directories stored as CSV strings where input sources should look for work. Takes effect immediately.	RW	/home/oracle/testinputagent/inputdir1
12	IPMVersion	The I/PM version number.	R	11.1.1.5.0 (110426.1700.11020)
13	JpegImageQuality	Specifies desired quality level of rendered JPG images	RW	100
14	LogDetailedTimes	Provides detailed logging of UI activity with durations of many of the UI activities. Takes effect at server restart.	RW	false
15	MaxSearchResults	Maximum number of rows a search is allowed to return. After this value is reached, the search is stopped. Takes effect on next search.	RW	100
16	RequireBasicAuthSSL	Forces the use of SSL in all web service communication when set to true	RW	false
17	SampleDirectory	Specifies which directory holds the sample data for the input UI. Takes effect immediately.	RW	IPM/InputAgent/Input/Samples
18	TiffCompressionType	Compression algorithm used when creating TIFF images. Takes effect each time a TIFF is generated.	RW	LZW
19	Uptime	Returns the uptime of the server.	R	262:39:59
20	UseAdvancedAsDefaultViewerMode	Causes the advanced viewer to be used as the default viewer mode if a user has not set a preference. Takes effect at next login.	RW	false

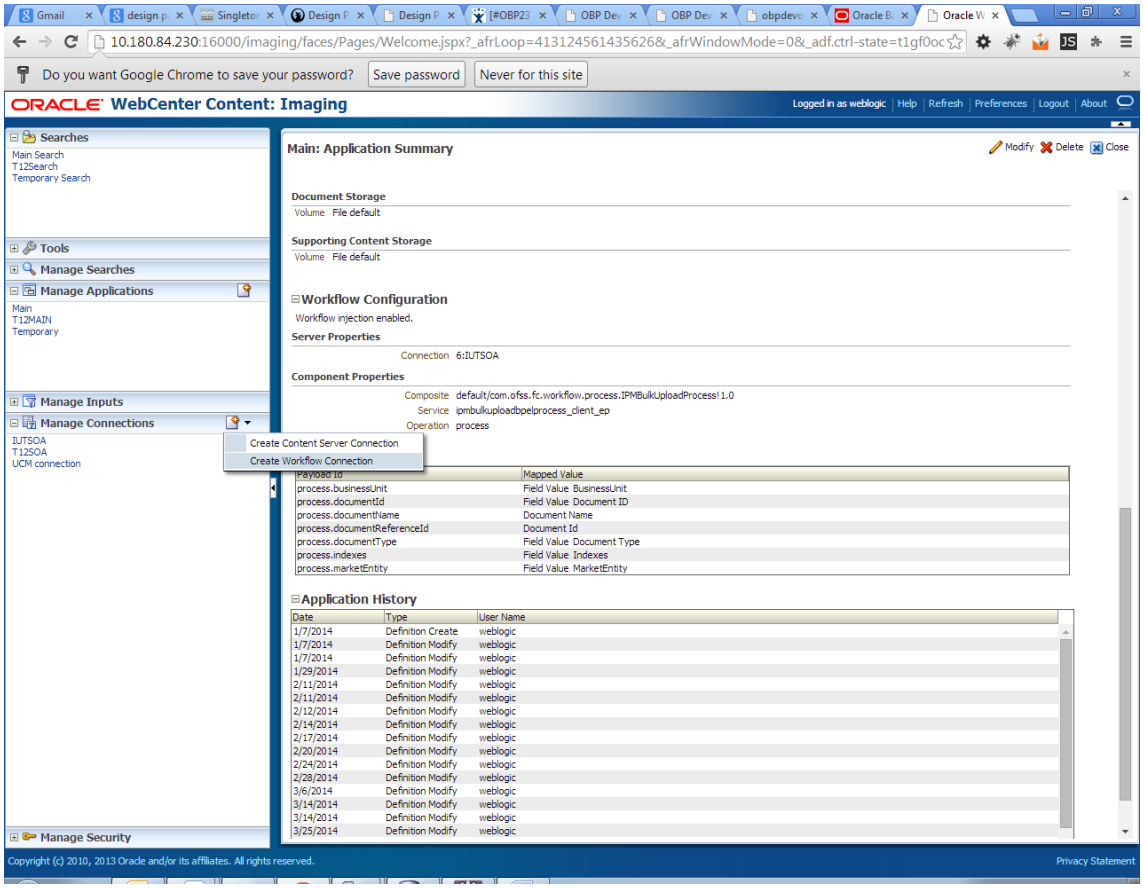
7. Restart IPM server.

7.2.4 Create SOA Connection

To create a SOA Connection:

1. Log in to Image Processing Management (IPM).
2. Navigate to the Manage Connections section.

Figure 7–43 Manage Connections: Create Workflow Connection



3. Click **Create Workflow Connection.**

   Workflow Connection is used to point to the "IPMBulkUpload" BPEL process deployed on the SOA server as part of the SOA media pack installation process.

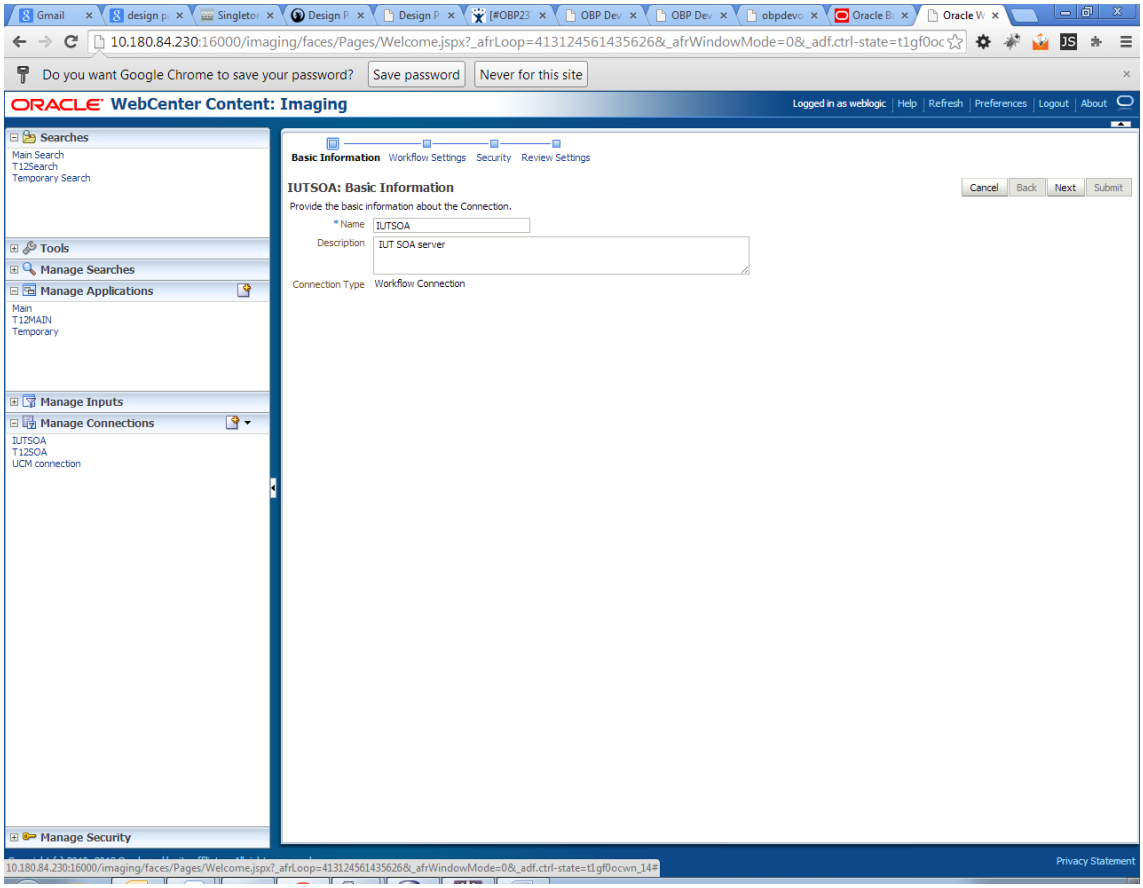
   `OBP_IPM_SOA_CONN_NAME`

   `SOA_MANAGED_SERVER_LISTEN_ADDRESS`

   `SOA_MANAGED_SERVER_LISTEN_PORT`

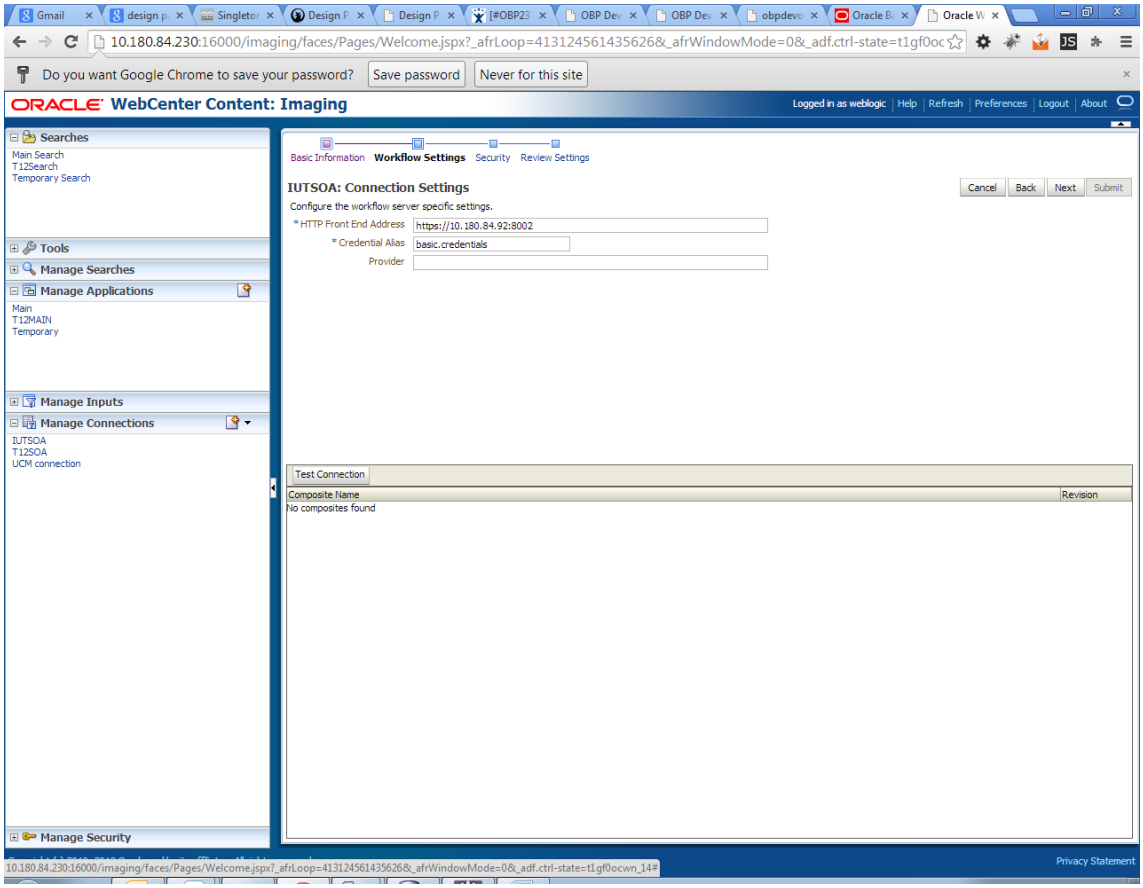
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 7–44 IUTSOA: Basic Information



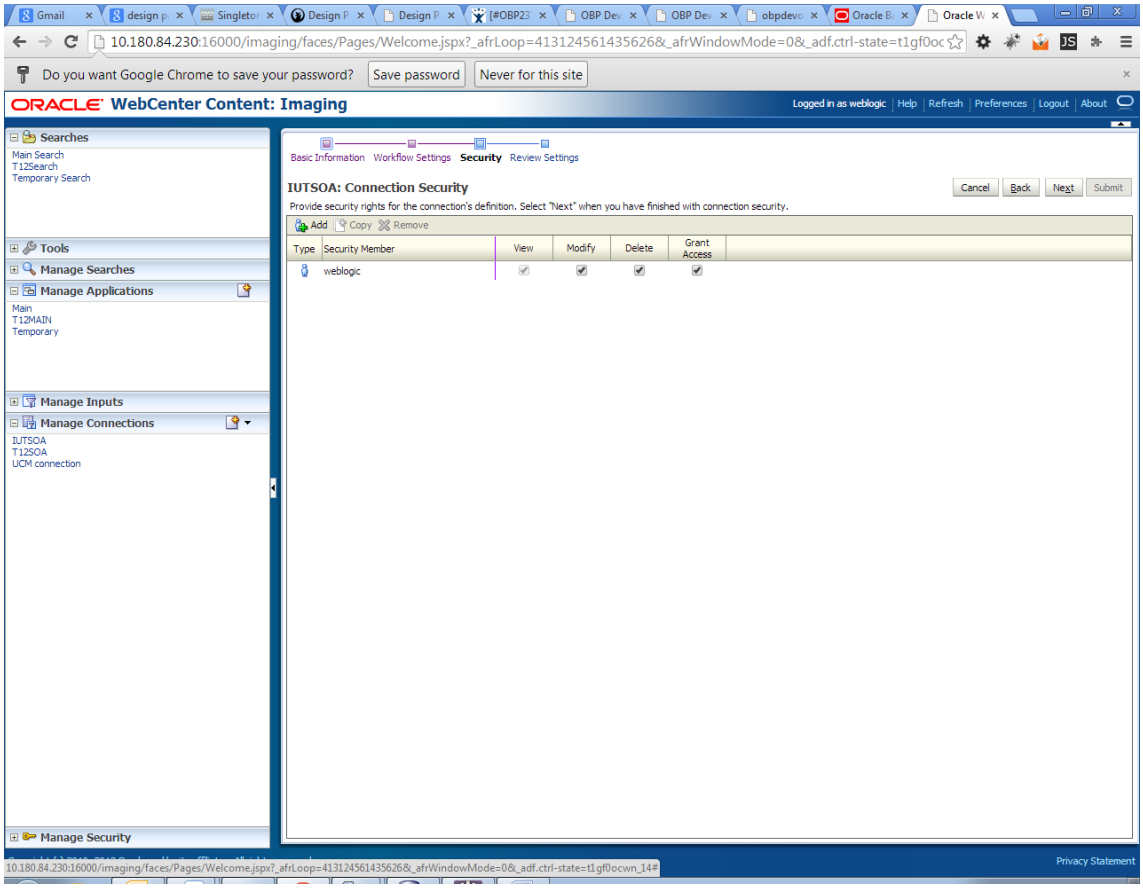
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 7–45 IUTSOA: Workflow Settings



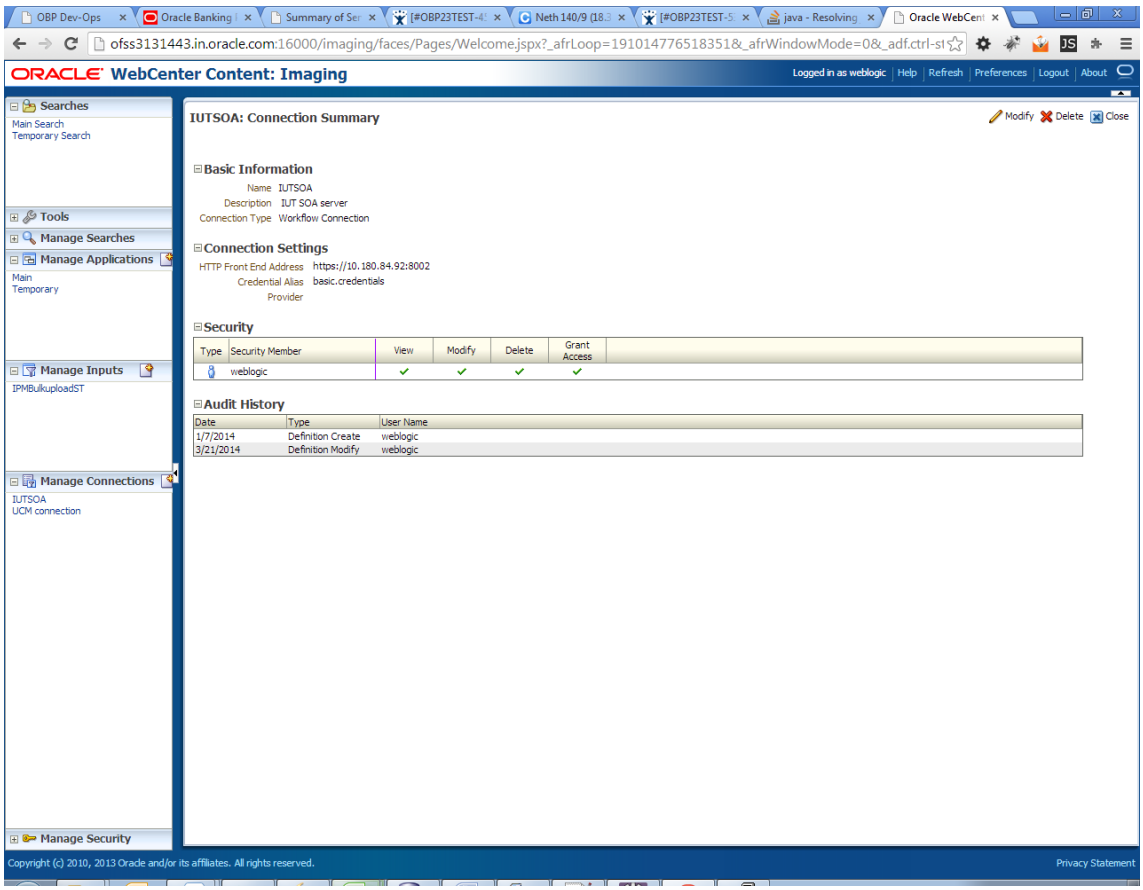
6. In the **Credential Alias** field, enter the value as **basic.credentials**.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 7–46 IUTSOA: Connection Security



8. Provide the requisite security rights to the connection's definition.
9. Click **Submit.**
10. Click **Next**. The Review Settings page appears.

Figure 7–47 IUTSOA: Review Settings

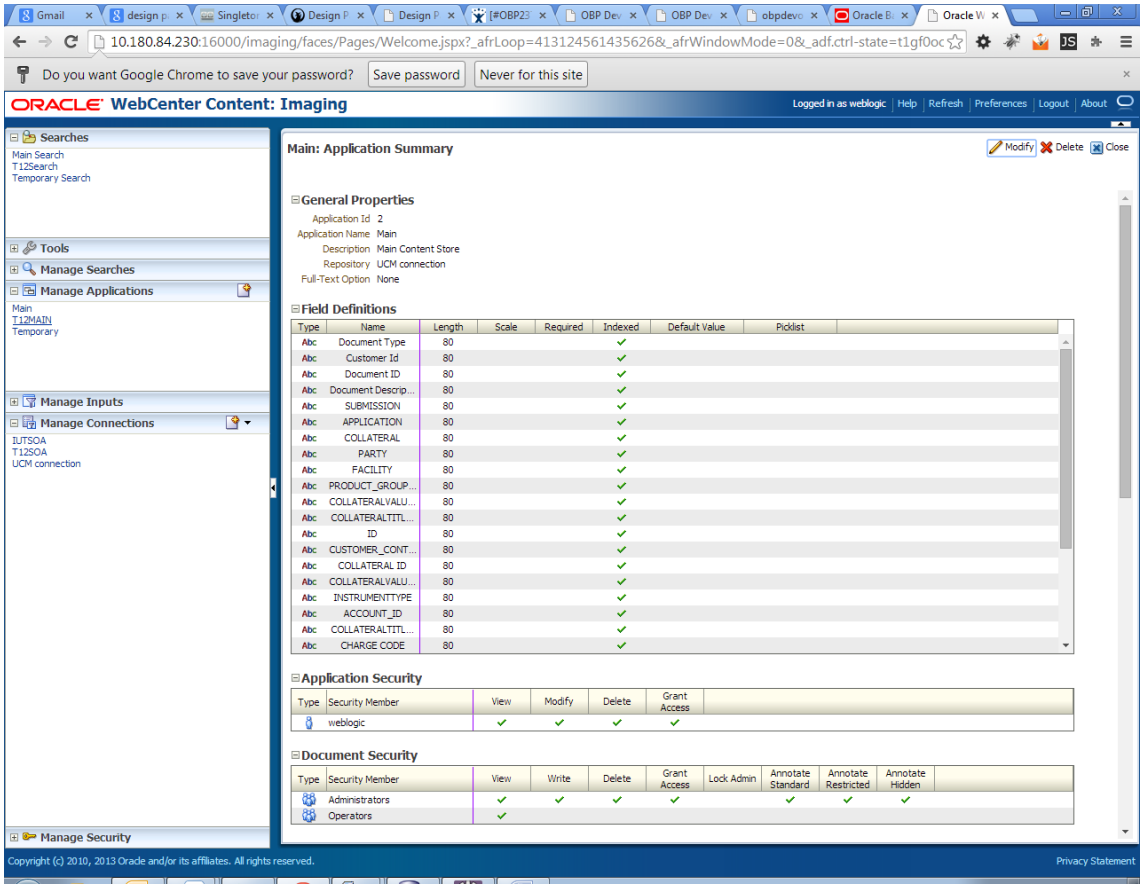


7.2.5 Manage Workflow Configuration

To manage workflow configuration:

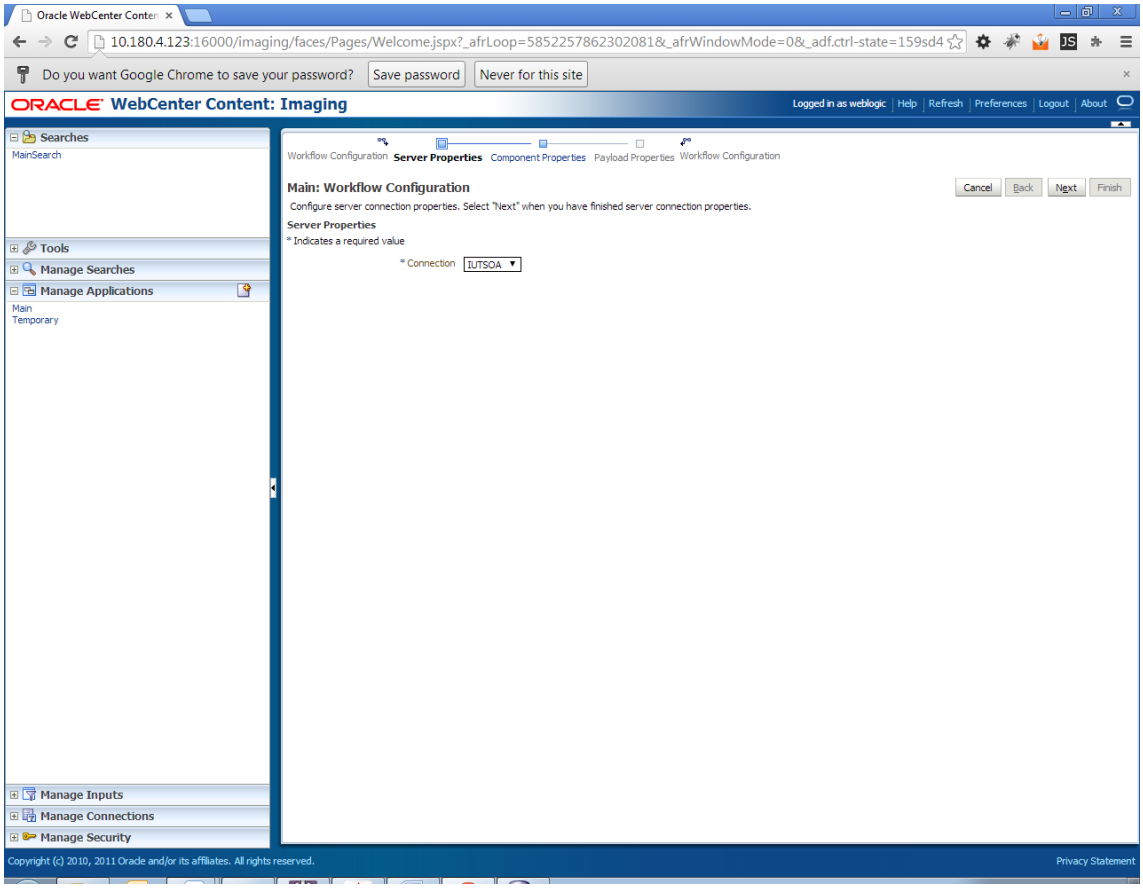
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Applications** section.

Figure 7–48 Main: Application Summary



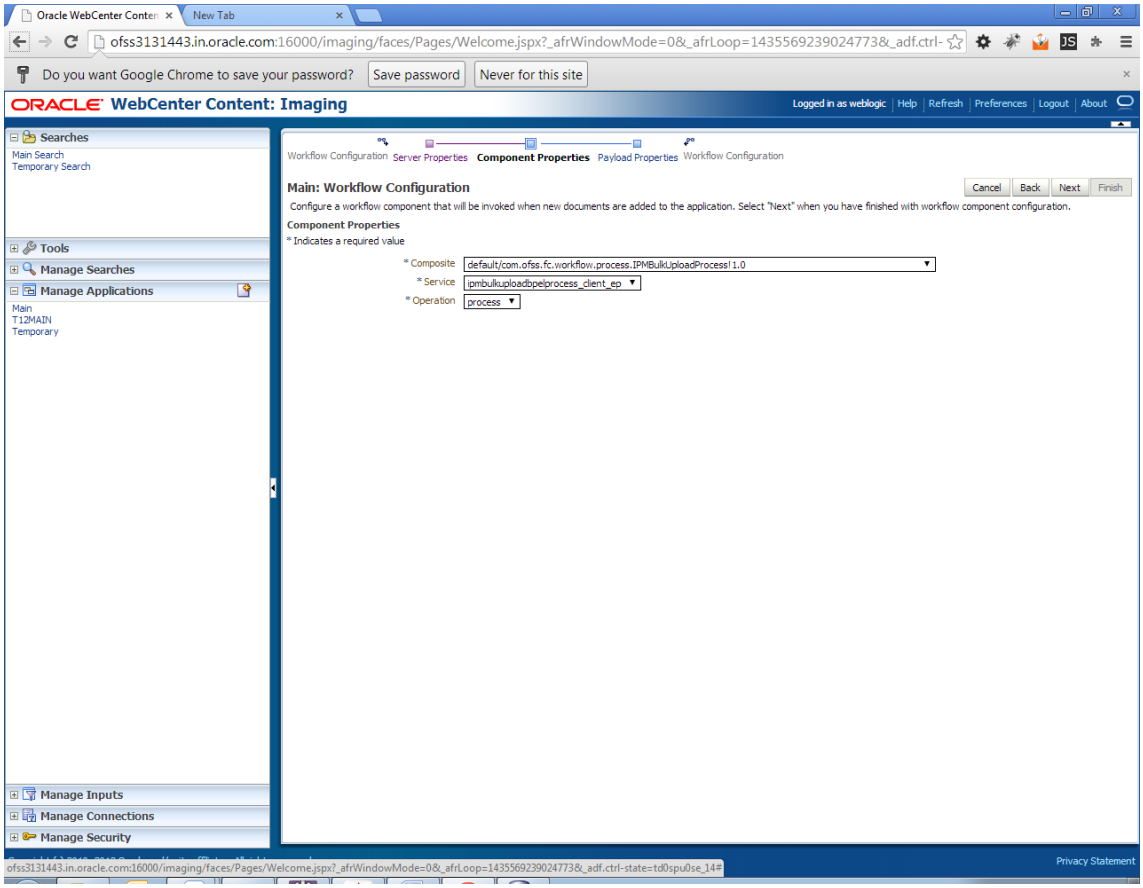
3. Select the application for which workflow configuration has to be done as shown in Figure 7–48.
4. Click **Modify.**
5. Navigate to the Workflow Configuration section.
6. Click the **Add/Modify** button.
7. In the Server Properties section, select the connection (IUTSOA) which was created in **Manage Connections** section from the **Connection** list.

Figure 7–49 Manage Applications - Server Properties



8. Click **Next.**
9. In the Component Properties section, select the Composite, Service and Operation values.
10. From the Composite list, select default/com.ofss.fc.workflow.process.IPMBulkUploadProcess!1.0 from the list of process.
11. From the Service list, select ipmbulkuploadbpelprocess_client_ep.
12. From the **Operation** list, select **process.**

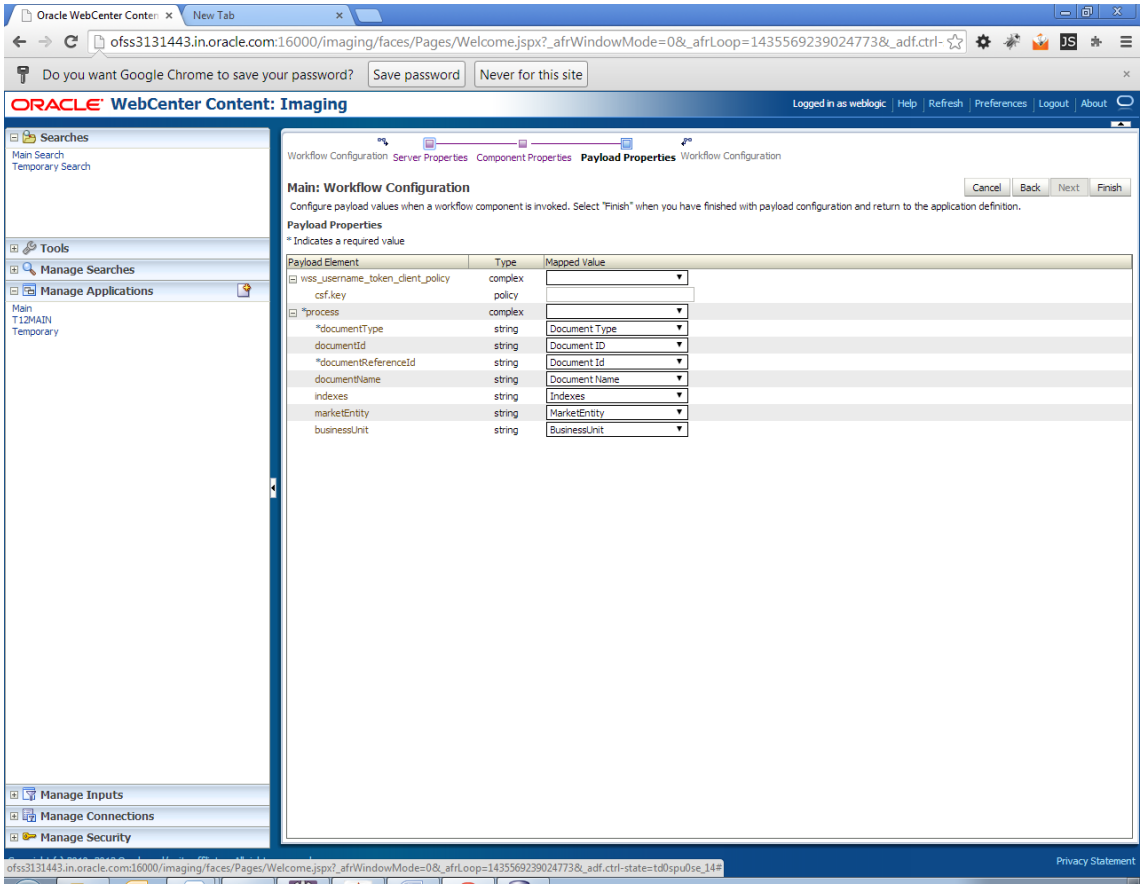
Figure 7–50 Manage Applications - Component Properties



13. Click **Next**.
14. In the Payload Properties section, map the payload elements with mapped value as shown in following figure.
15. Map the process fields with application field definitions.

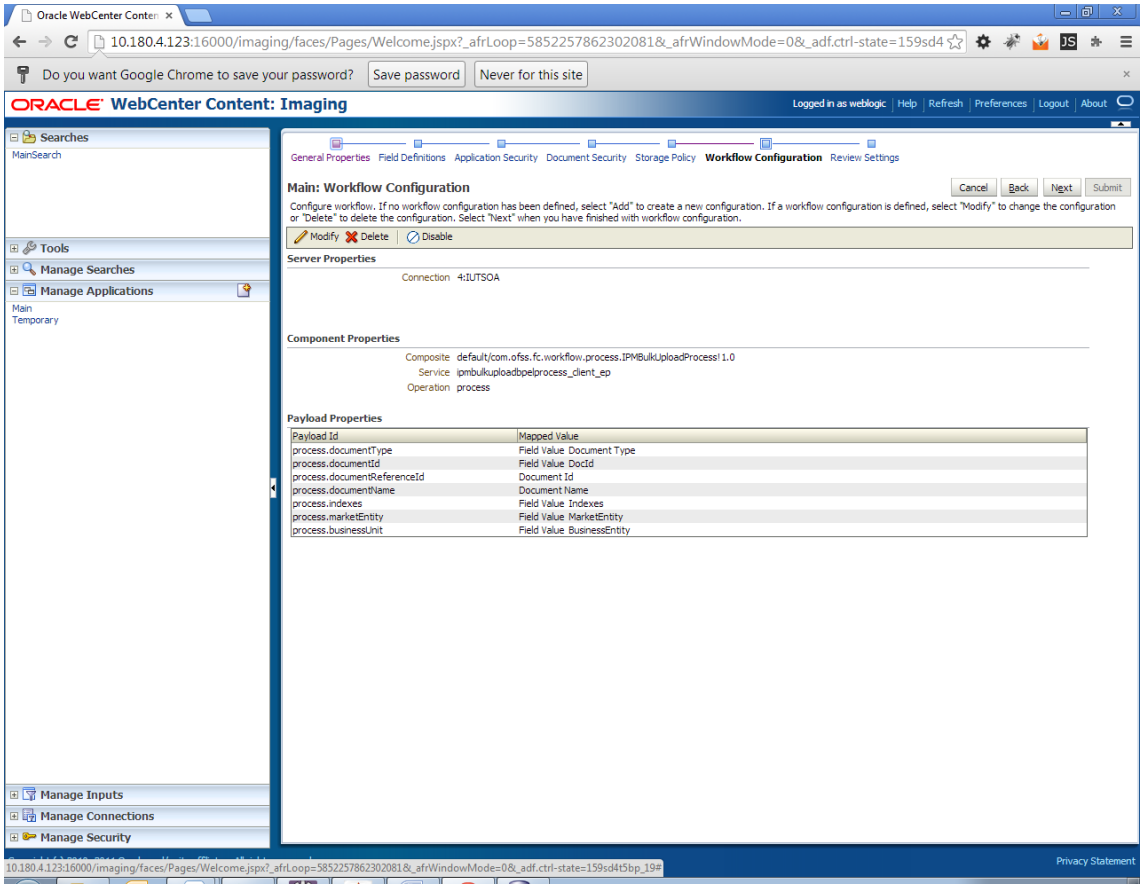
> **Note**
>
> The document ReferenceId is mapped to Document Id (IPM internal field), whereas documentId is mapped to doc Id which is application field.

Figure 7–51 Manage Applications - Payload Properties



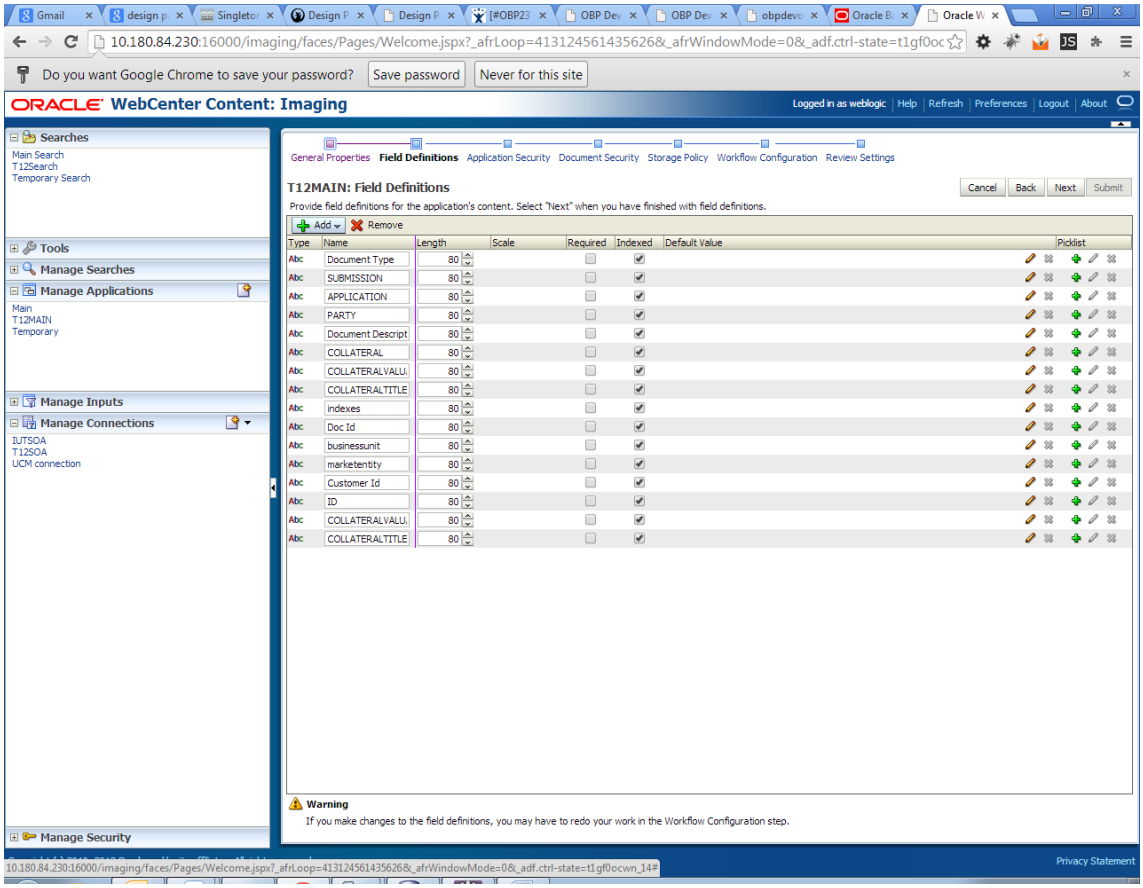
16. Click **Next.**
17. Complete the Workflow Configuration. Click **Next.**

Figure 7–52 Manage Applications - Workflow Configuration



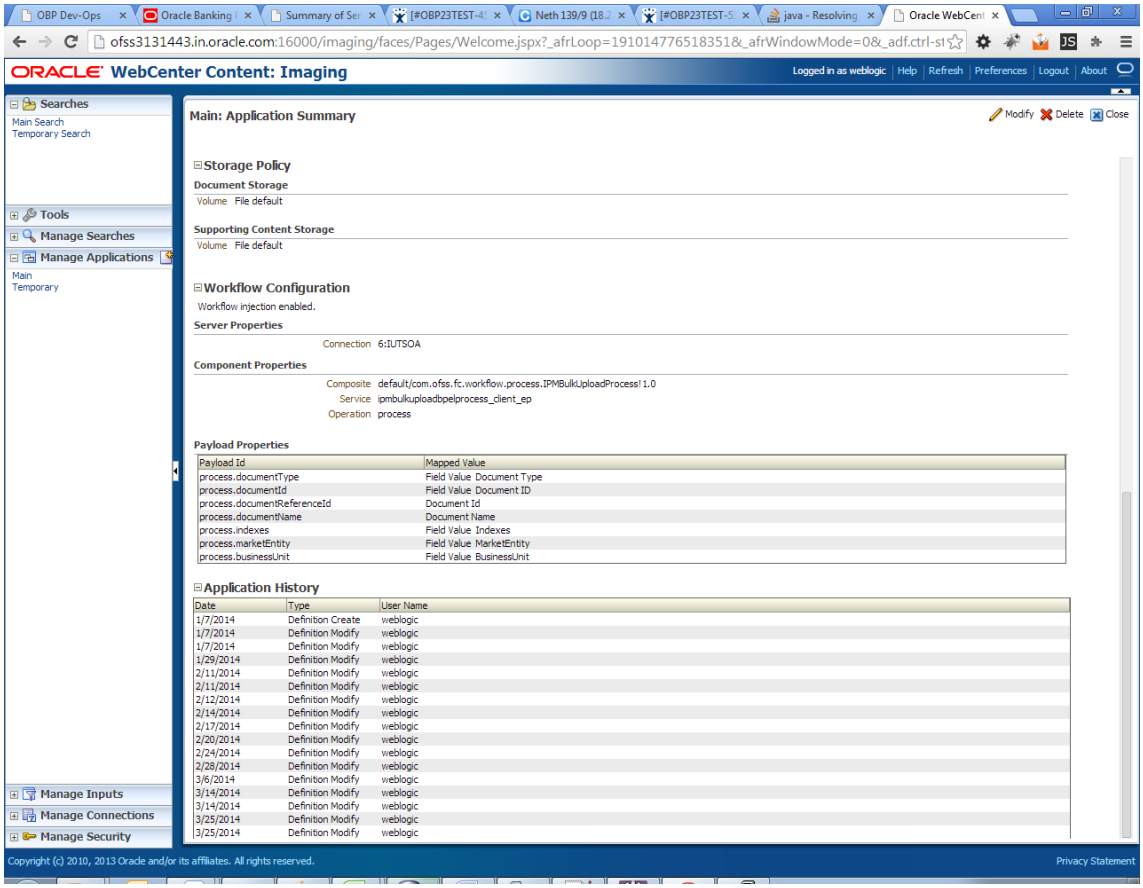
18. Add all those fields which are not present in the application as shown below.

Figure 7–53 Field Definitions



The Main Application Summary appears as shown Figure 7–54.

Figure 7–54 Main: Application Summary

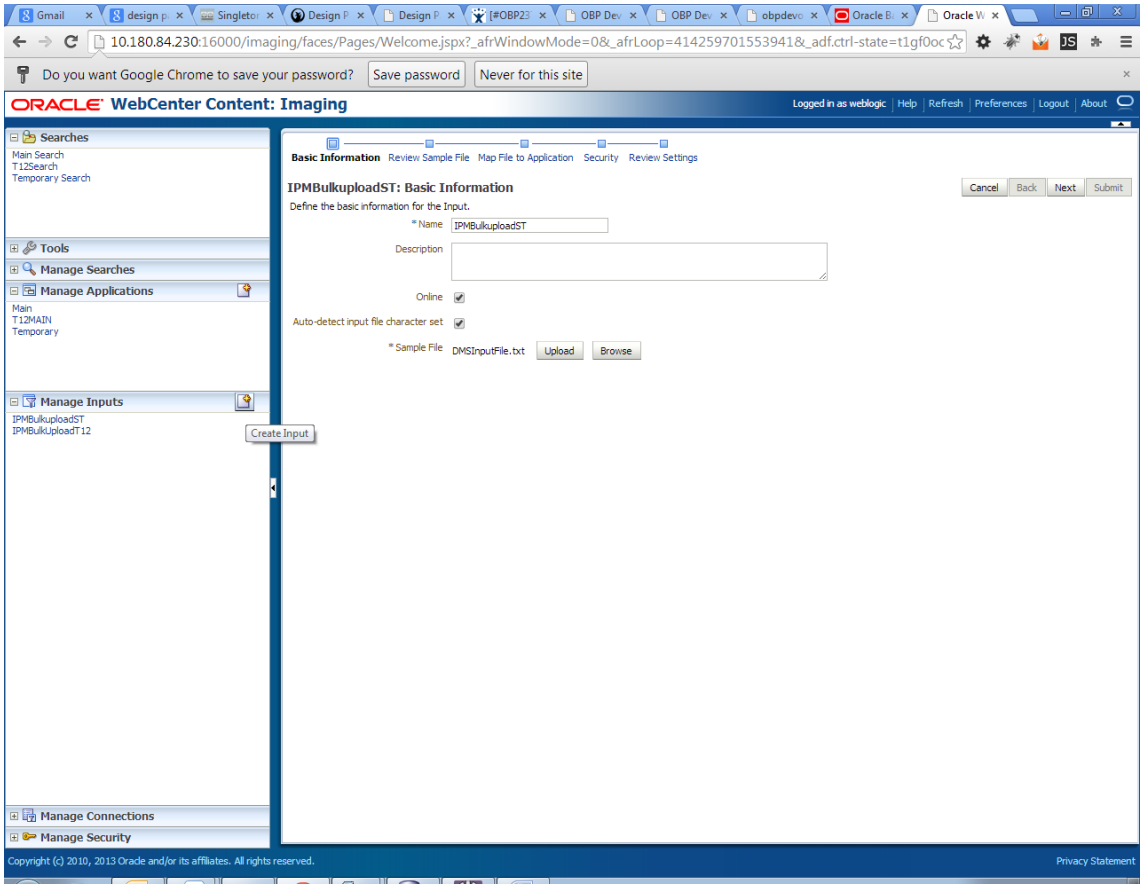


7.2.6 Manage Inputs for Input Agents

To manage workflow configuration:

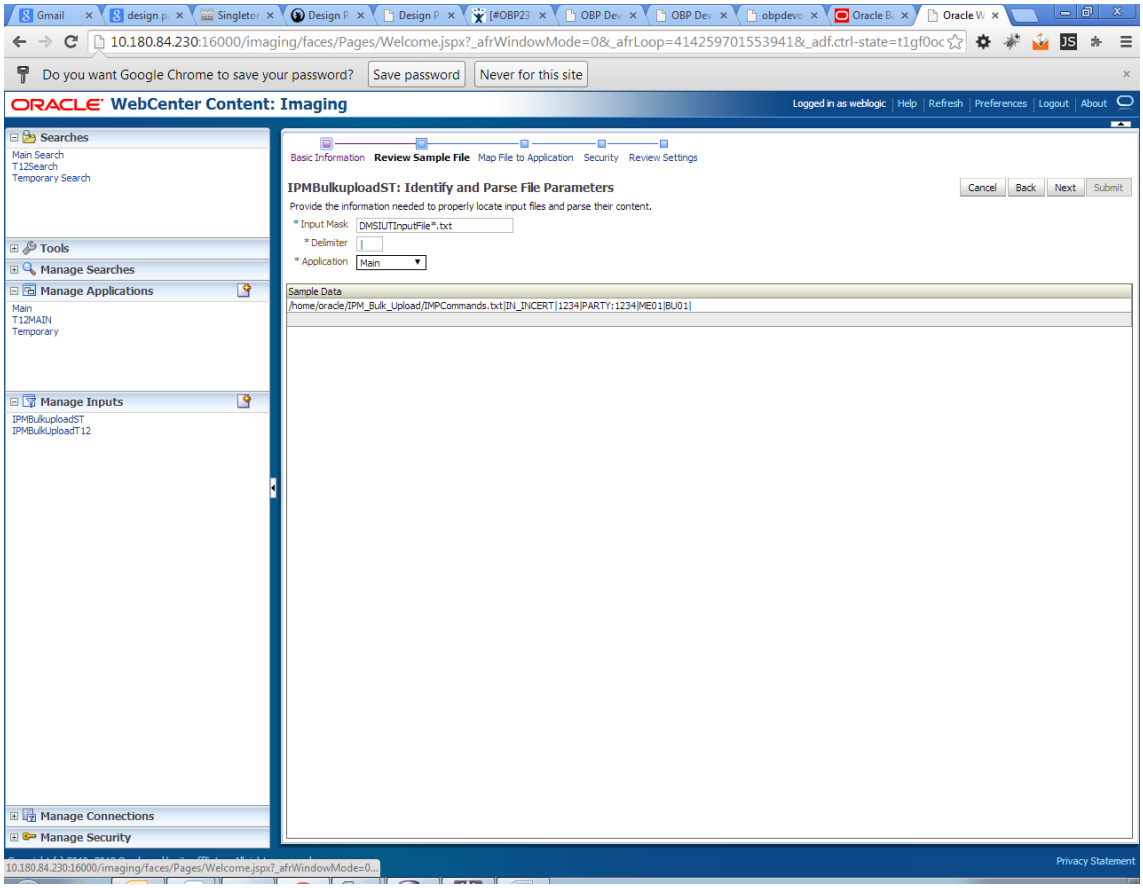
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Inputs** section.

Figure 7–55 Input Agent: Basic Information



3. Define an input agent by entering a **Name**. For example, **bulkUploadInput**.
4. Define Input Mask as DMSInputSampleFile.txt.

Figure 7–56 Input Agent: Input Mask



5. Upload the attached sample file.

   For example, name the sample file as DMSInputSampleFile.txt and add the following content to the sample file.

   ```
   /home/oracle/IPM_Bulk_Upload/IMPCommands.txt|IN_
   INCERT|1234|PARTY:1234|ME01|BU01|
   ```

6. In the **Input Mask** field enter the value which should be the same as the name given in table flx_fw_config_all_b.

   select prop_value from flx_fw_config_all_b where category_id = 'reports' and `prop_id='BULK_UPLOAD_FILE_NAME_PREFIX';`

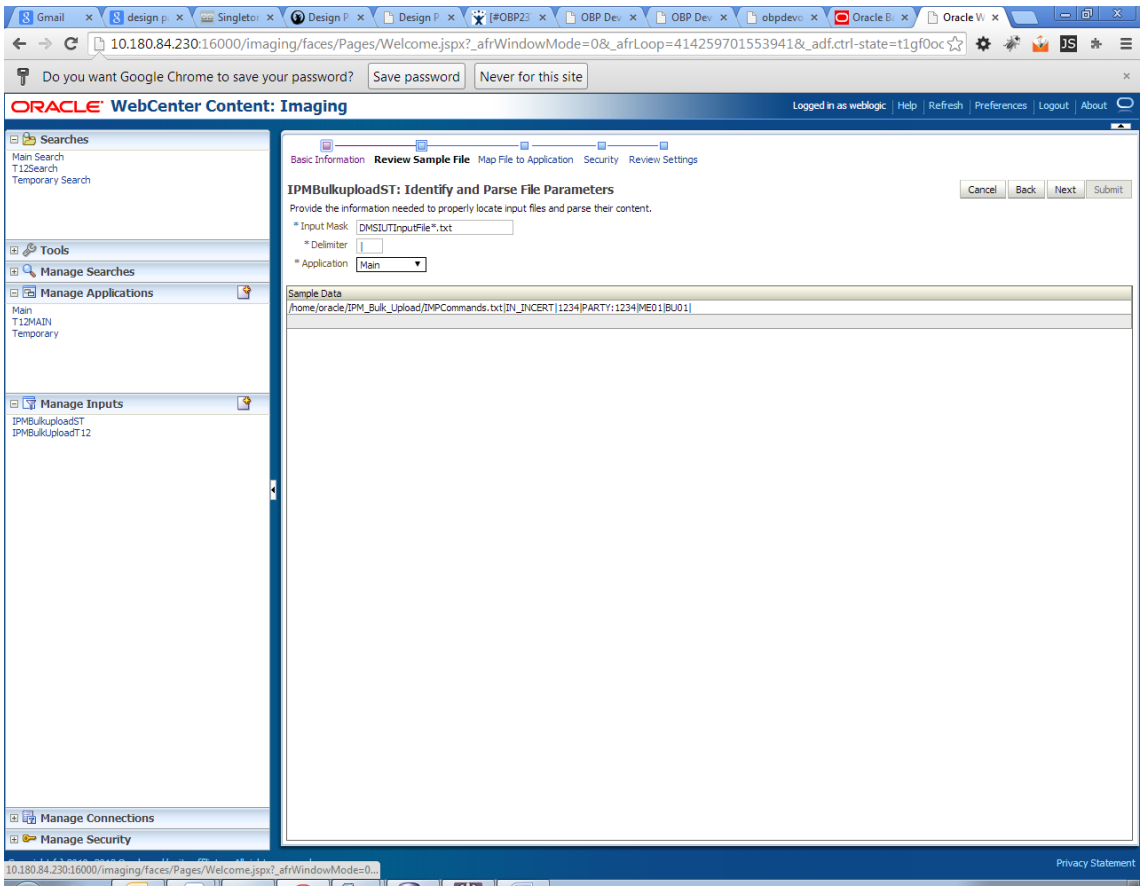
   Note

   Input Mask name should have a * (asterisk character) to enable the process to read all the files whose prefix is same as the input mask value.

7. In the **Delimeter** field, enter the delimiter value as | (vertical bar character).

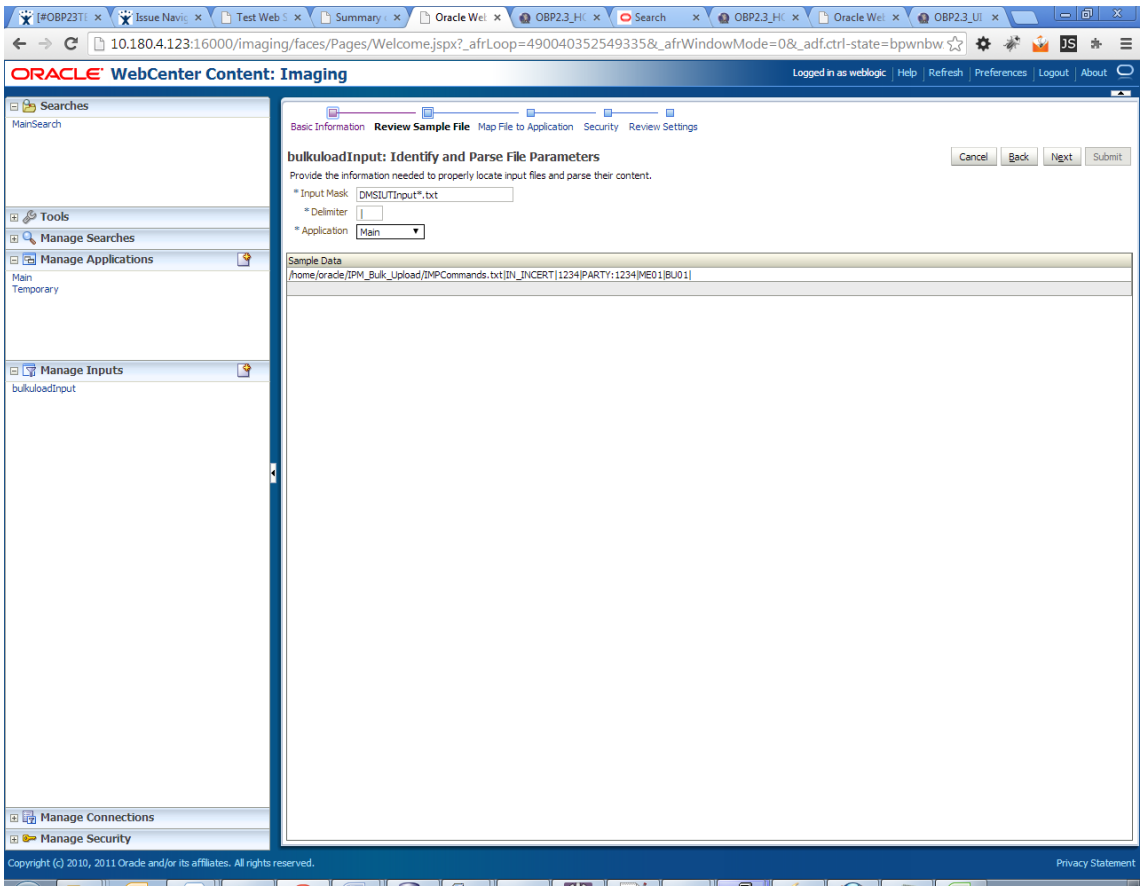
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 7–57 Input Agent: File Parameters



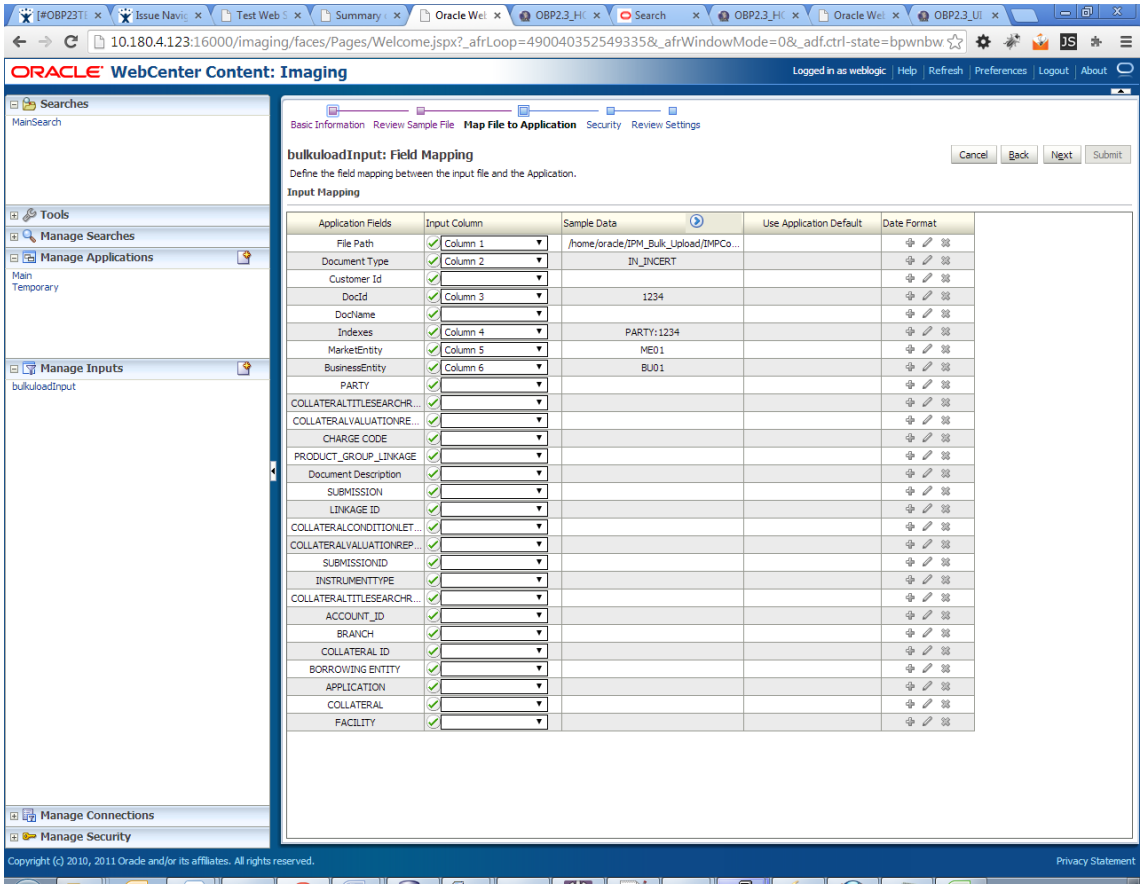
9. In the Field Mapping section, map the **Application Fields.**

Figure 7–58 Input Agent: Fields Mapping



10. After completion of the procedure, the Input Summary appears. The Input agent should have the settings similar to those shown in Figure 7–59.

Figure 7–59 Input Agent: Summary



Note

Do not forget to toggle online, else the input agent will not pick up any file for processing.

7.2.7 Additional Steps

1. Update user and bankcode as follows:

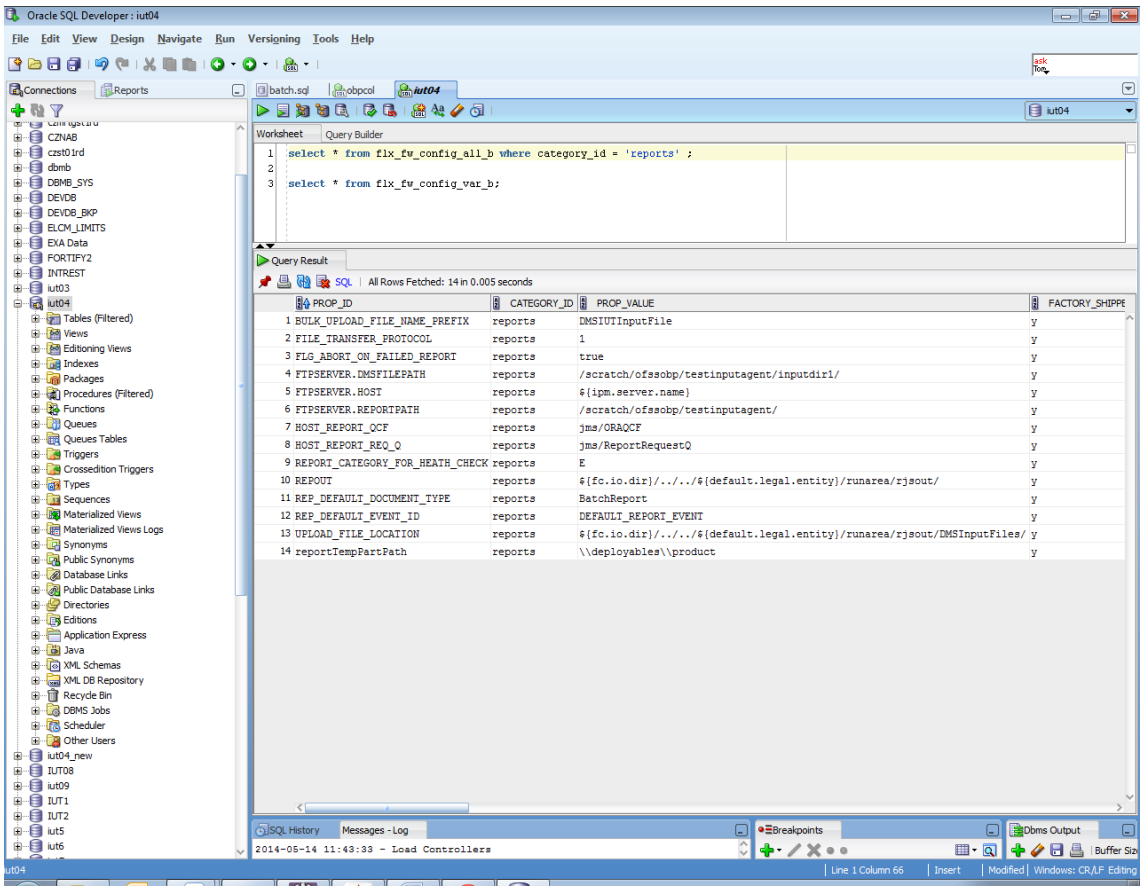
```
update flx_fw_config_all_b set prop_value='48' where prop_
value='335' and category_id like 'contentmanager%';
update flx_fw_config_all_b set prop_value='ofssuser' where
prop_id='userId' and category_id like 'contentmanager%';
```

2. In the flx_fw_config_all_b table, the values for **PROP_ID** should be the same as mentioned for the path in IPM server.

Table 7–1 PROP ID Values

PROP_ID	PROP_VALUE
FTPSERVER.DMSFILEPATH=/scratch/ofssobp/testinputagent/inputdir1/	Path in IPM config
FTPSERVER.REPORTPATH=/scratch/reports/	Path where files will be FTP
FTPSERVER.HOST	IPM IP
BULK_UPLOAD_FILE_NAME_PREFIX	Input Mask name given in 1.5 Manage Inputs for Input Agents section.

Figure 7–60 flx_fw_config_all_b table



3. FTP service on IPM server should be running and FTP user should be created on host user connectors.

7.2.8 SSL Handshake Resolution

For resolving the SSLHandshake between IPM and SOA server:

1. Save the SOA server Certificate. SOA certificate needs to be saved in Base64 (.cer) format for import to IPM server.
2. Import the SOA server certificate on IPM server with following command.

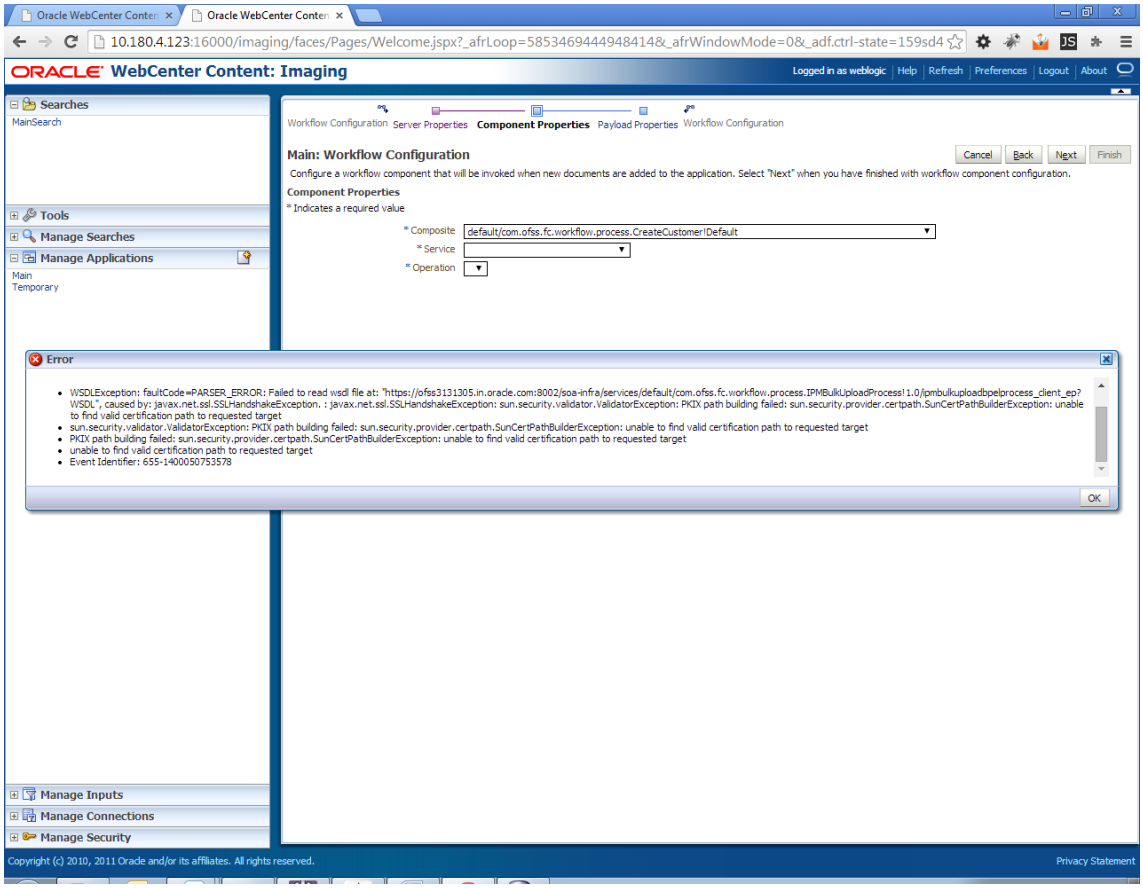
   Copy certificate at following path on IPM server.

   keytool -import -noprompt -trustcacerts -alias UI_SSL_trustself -file SOACert.cer -keystore cacerts -storepass changeit
3. Security policy for IPMbulkuploadProcess can been removed (if required).

   Security for called method

   com.ofss.fc.app.content.service.DocumentContentApplicationService.documentUpload (SessionContext, DocumentDTO) needs to be removed (for Development environment).

Figure 7–61 SSL Handshake Resolution



7.3 IPM Report Upload Setup

This section describes the configuration on IPM server, which is required for bulk report upload on IPM.

7.3.1 Prerequisites

Following are the prerequisites before proceeding with bulk upload process setup:

1. Application on IPM server on which bulk upload process needs to be configured must be created. For more information to understand the application creation process, see Image Processing and Management Admin Guide.
2. com.ofss.fc.workflow.process.ReportIPMRefStoreProcess must be deployed on SOA server.

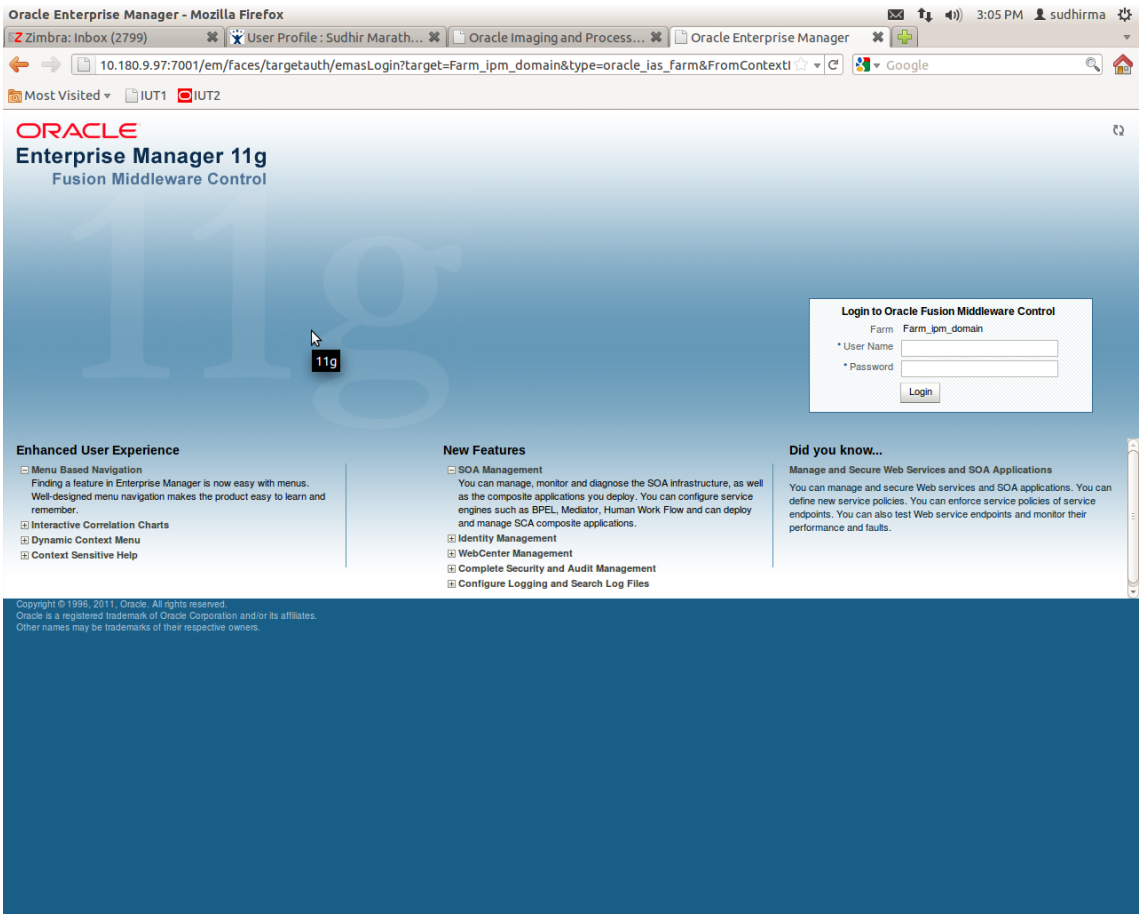
7.3.2 Setting up the Connection Name

To set up a bulk process we need to start by setting up the connection name, which is used as JNDI for IPM to BPEL connection.

To set up a bulk process:

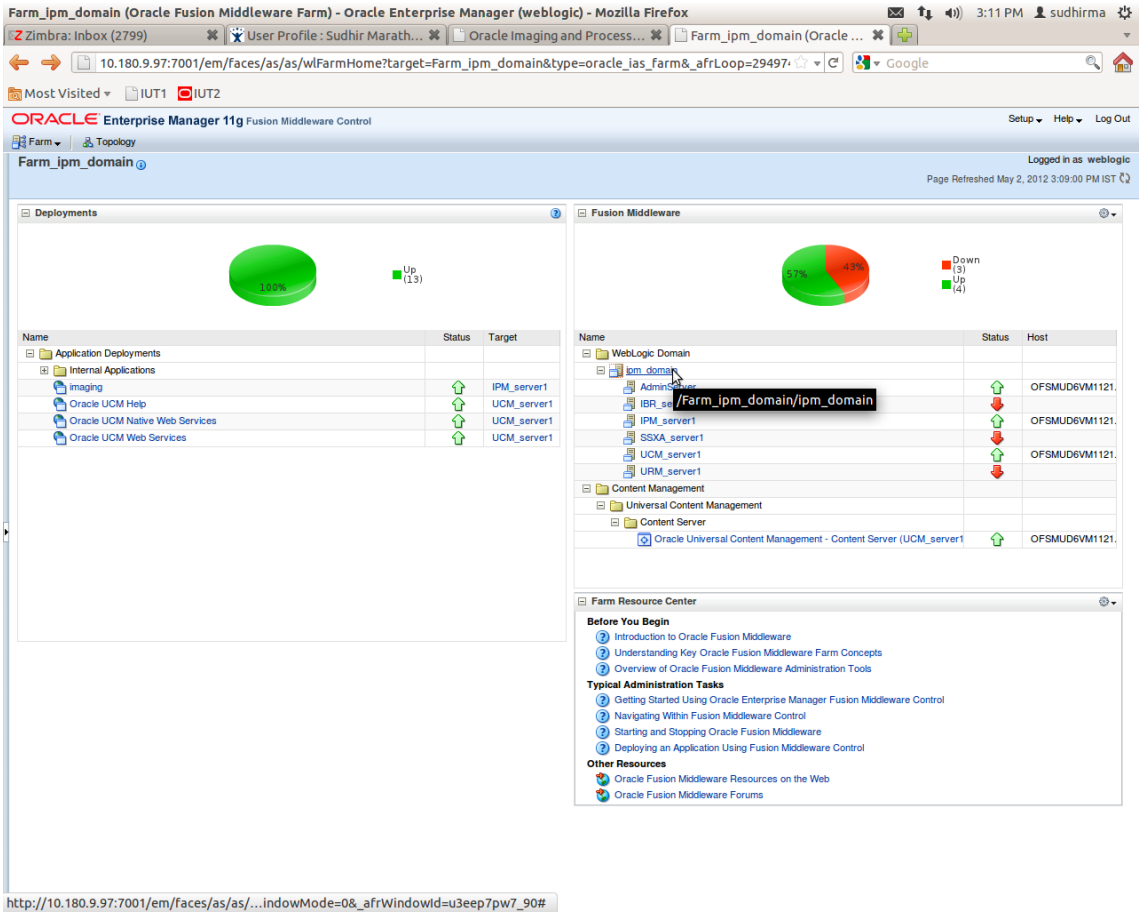
1. Log in to Enterprise Manager (EM) console.

Figure 7–62 Log in to Enterprise Manager (EM) console



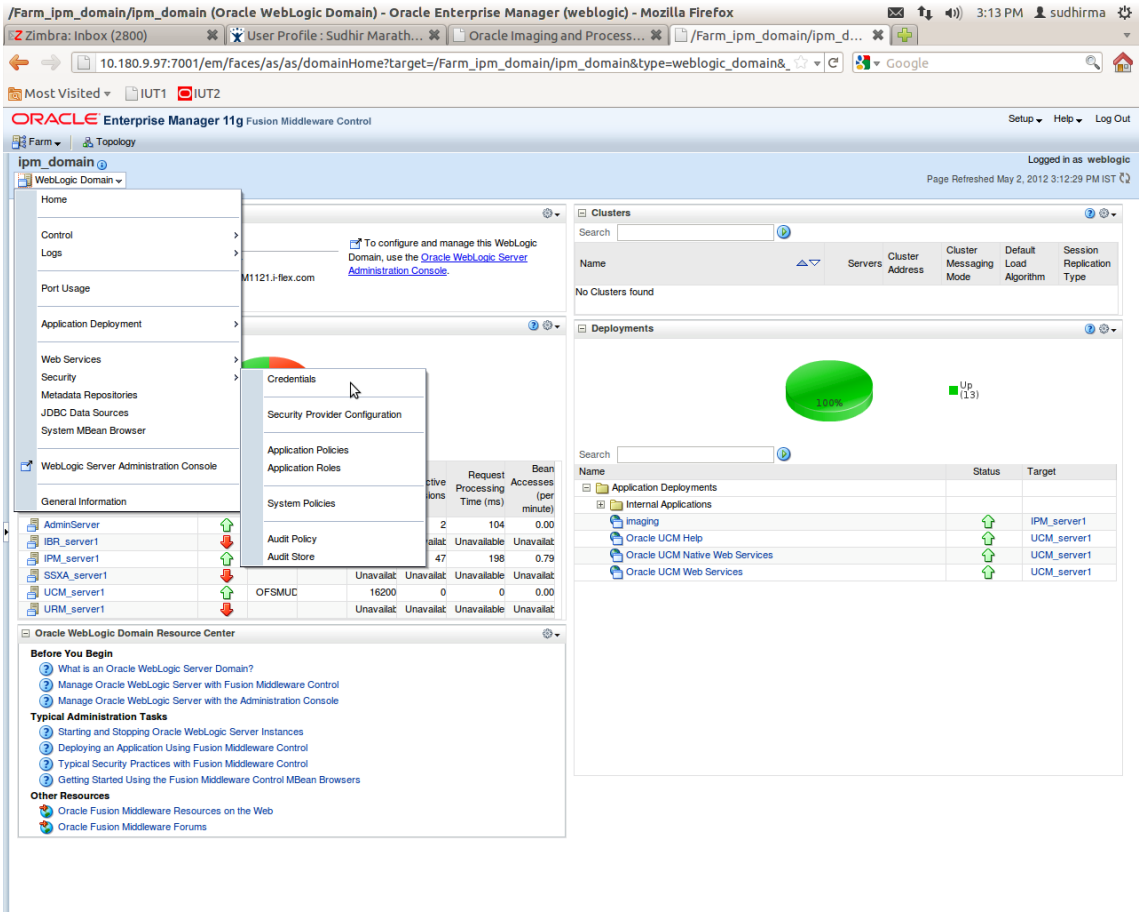
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 7–63 Click Weblogic Domain: ipm domain



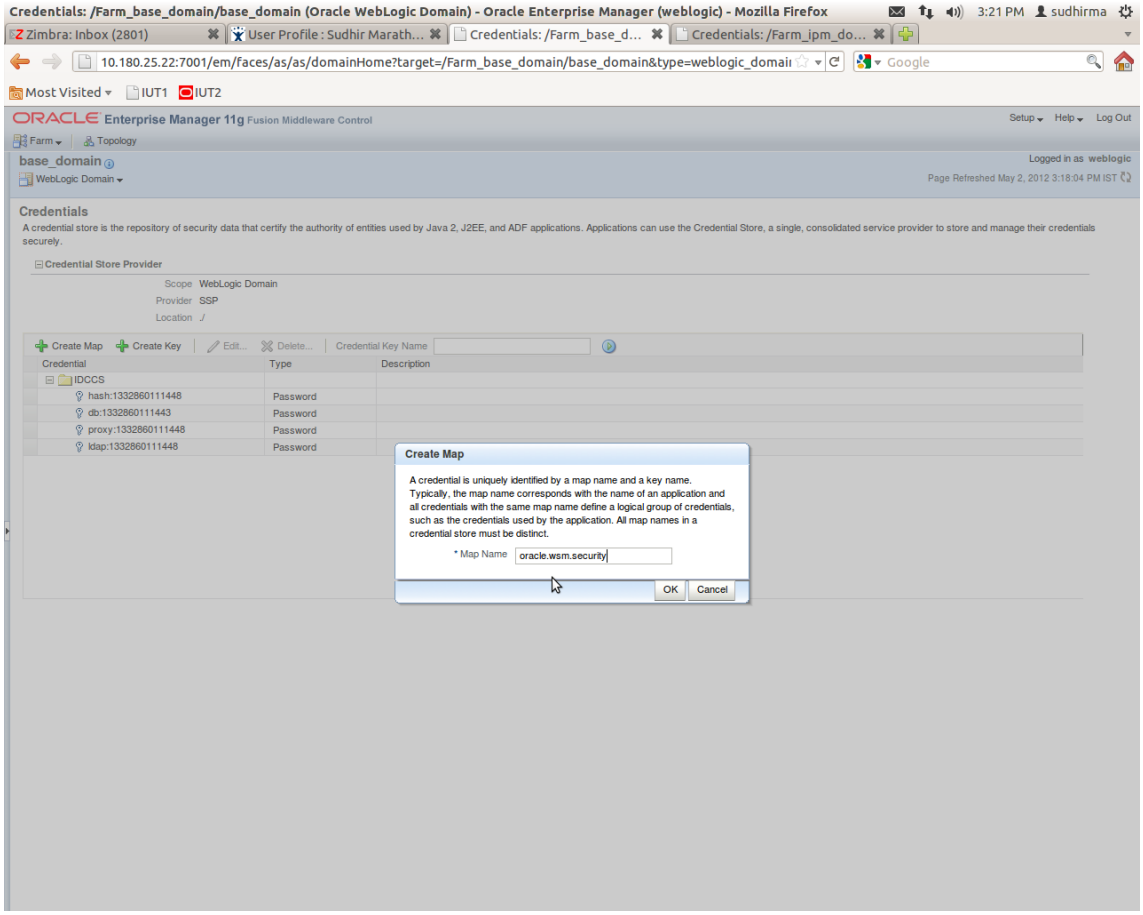
3. In the top menu, click **Weblogic Domain.** The corresponding menu appears.
4. Navigate to **Security > Credentials.** The Credentials page appears.

Figure 7–64 Navigate to Weblogic Domain --> Security --> Credentials



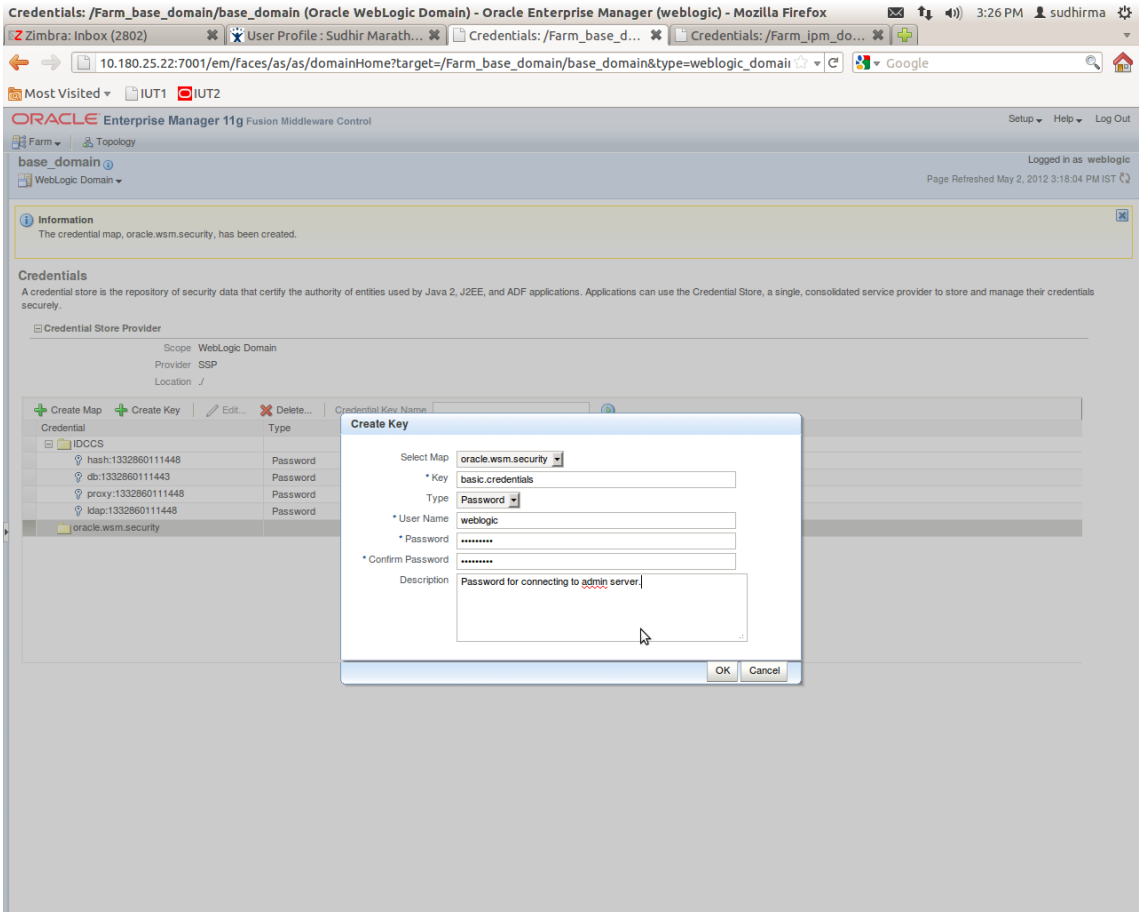
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 7–65 Create Map oracle.wsm.security



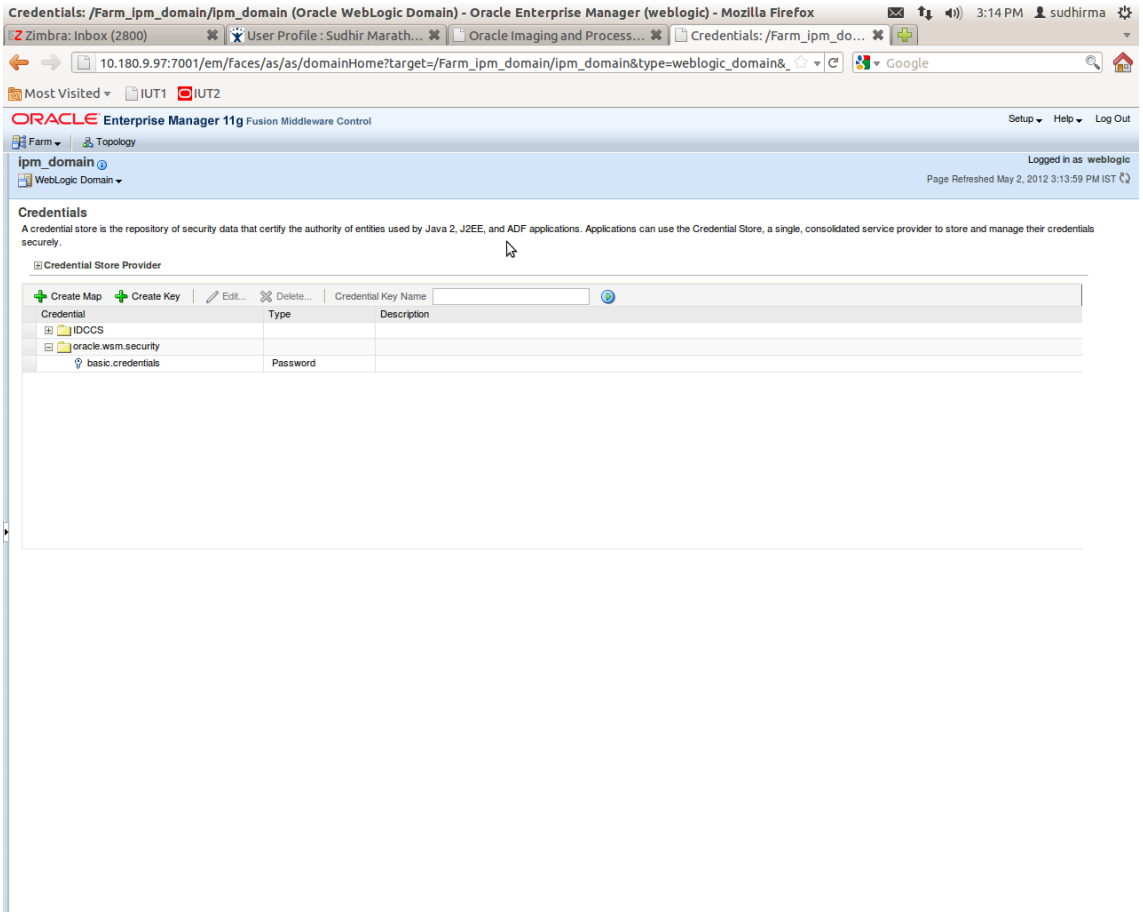
6. Click **Create Key** to create a key under the map **oracle.wsm.security.**

Figure 7–66 Create Key: basic.credentials



7. In the **Key** field, enter the key name as basic.credentials.
8. In the **Type** field, select the value as Password.
9. Enter the other required details.
10. Click **Ok.** The key is saved.

Figure 7–67 ipm_domain: Credentials Created

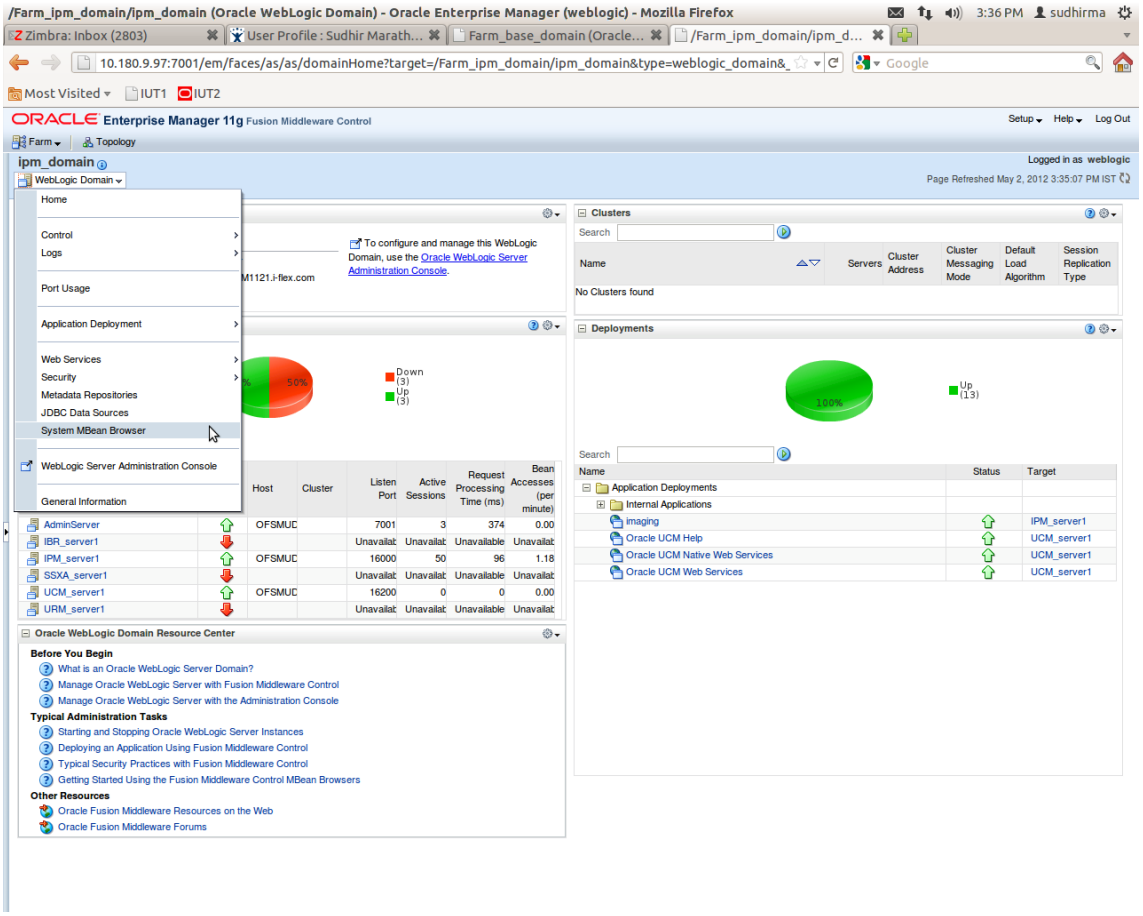


7.3.3 Setting up Input Agent Path

To set up input agent path:

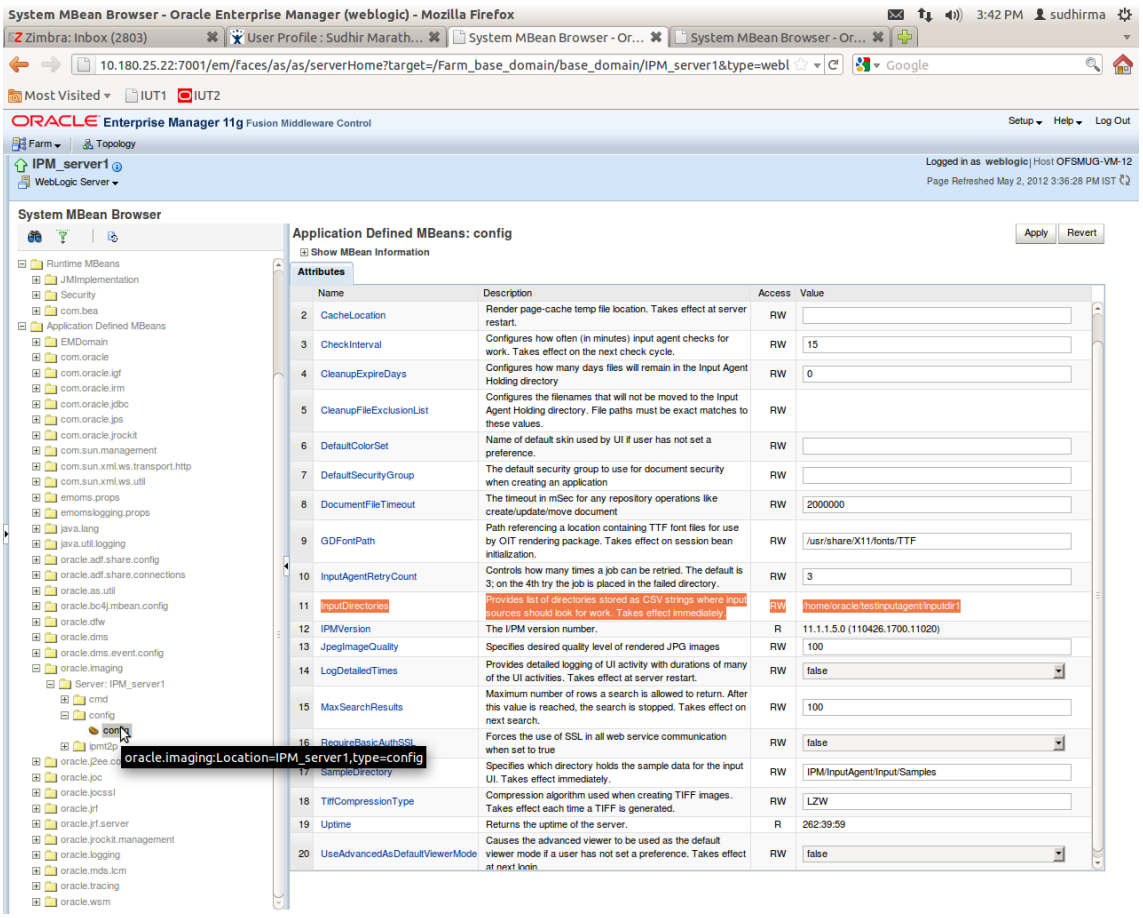
1. Log in to Enterprise Manager (EM) console.
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain**.
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

Figure 7–68 Navigate to Weblogic Domain --> System MBean Browser



5. In the left hand pane, navigate to **Application Defined MBeans > oracle.imaging > Server: IPM_server1 > config.**
6. For the attribute InputDirectories, in the **Value** column enter the value to set the path for input agents.
7. Change the highlighted path value to /scratch/ofssobp/testinputagent/inputdir1.

Figure 7–69 InputDirectories: Enter Input Agent Path



	Name	Description	Access	Value
2	CacheLocation	Render page-cache temp file location. Takes effect at server restart.	RW	
3	CheckInterval	Configures how often (in minutes) input agent checks for work. Takes effect on the next check cycle.	RW	15
4	CleanupExpireDays	Configures how many days files will remain in the Input Agent Holding directory	RW	0
5	CleanupFileExclusionList	Configures the filenames that will not be moved to the Input Agent Holding directory. File paths must be exact matches to these values.	RW	
6	DefaultColorSet	Name of default skin used by UI if user has not set a preference.	RW	
7	DefaultSecurityGroup	The default security group to use for document security when creating an application	RW	
8	DocumentFileTimeout	The timeout in mSec for any repository operations like create/update/move document	RW	2000000
9	GDFontPath	Path referencing a location containing TTF font files for use by OIT rendering package. Takes effect on session bean initialization.	RW	/usr/share/X11/fonts/TTF
10	InputAgentRetryCount	Controls how many times a job can be retried. The default is 3; on the 4th try the job is placed in the failed directory.	RW	3
11	InputDirectories	Provides list of directories stored as CSV strings where input sources should look for work. Takes effect immediately.	RW	/home/oracle/testinputagent/inputdir1
12	IPMVersion	The I/PM version number.	R	11.1.1.5.0 (110426.1700.11020)
13	JpegImageQuality	Specifies desired quality level of rendered JPG images	RW	100
14	LogDetailedTimes	Provides detailed logging of UI activity with durations of many of the UI activities. Takes effect at server restart.	RW	false
15	MaxSearchResults	Maximum number of rows a search is allowed to return. After this value is reached, the search is stopped. Takes effect on next search.	RW	100
16	RequireBasicAuthSSL	Forces the use of SSL in all web service communication when set to true	RW	false
17	SampleDirectory	Specifies which directory holds the sample data for the input UI. Takes effect immediately.	RW	IPM/InputAgent/Input/Samples
18	TiffCompressionType	Compression algorithm used when creating TIFF images. Takes effect each time a TIFF is generated.	RW	LZW
19	Uptime	Returns the uptime of the server.	R	262:39:59
20	UseAdvancedAsDefaultViewerMode	Causes the advanced viewer to be used as the default viewer mode if a user has not set a preference. Takes effect at next login	RW	false

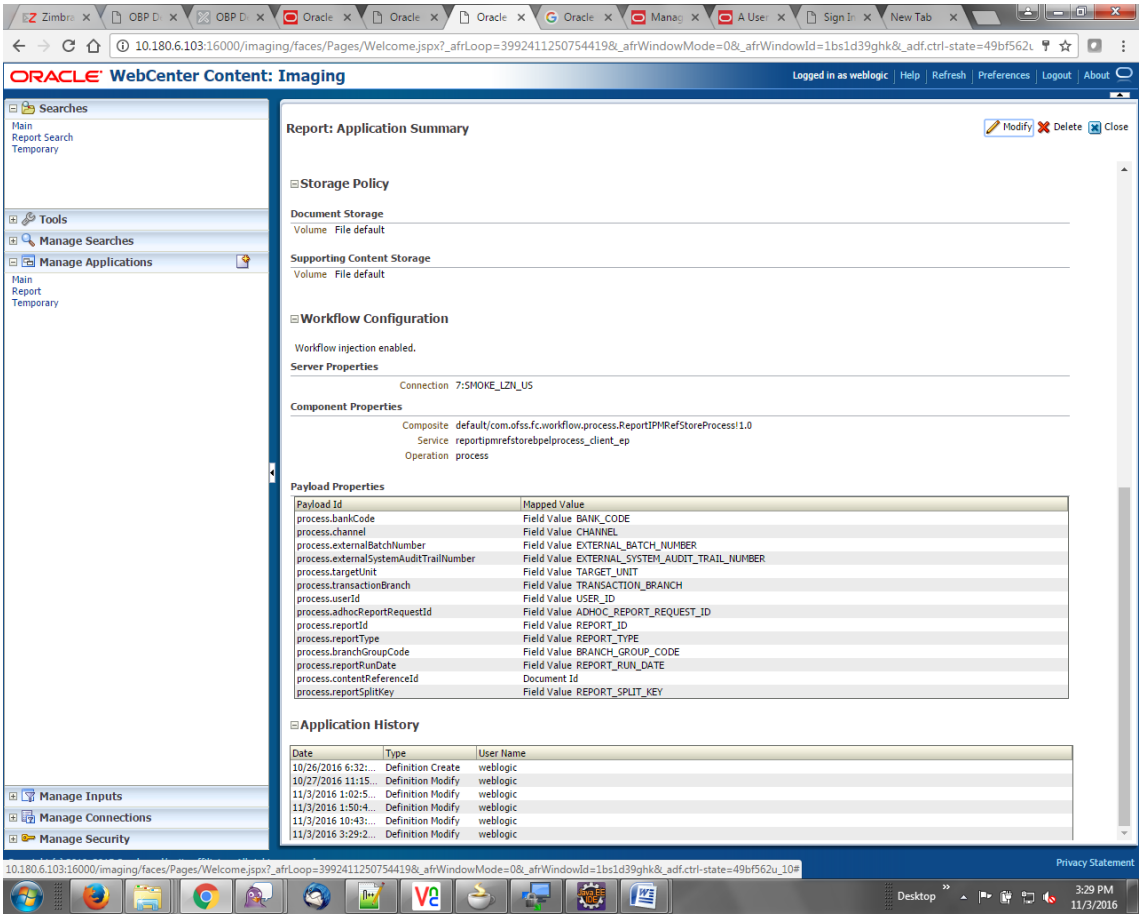
8. Restart IPM server.

7.3.4 Create SOA Connection

To create a SOA Connection:

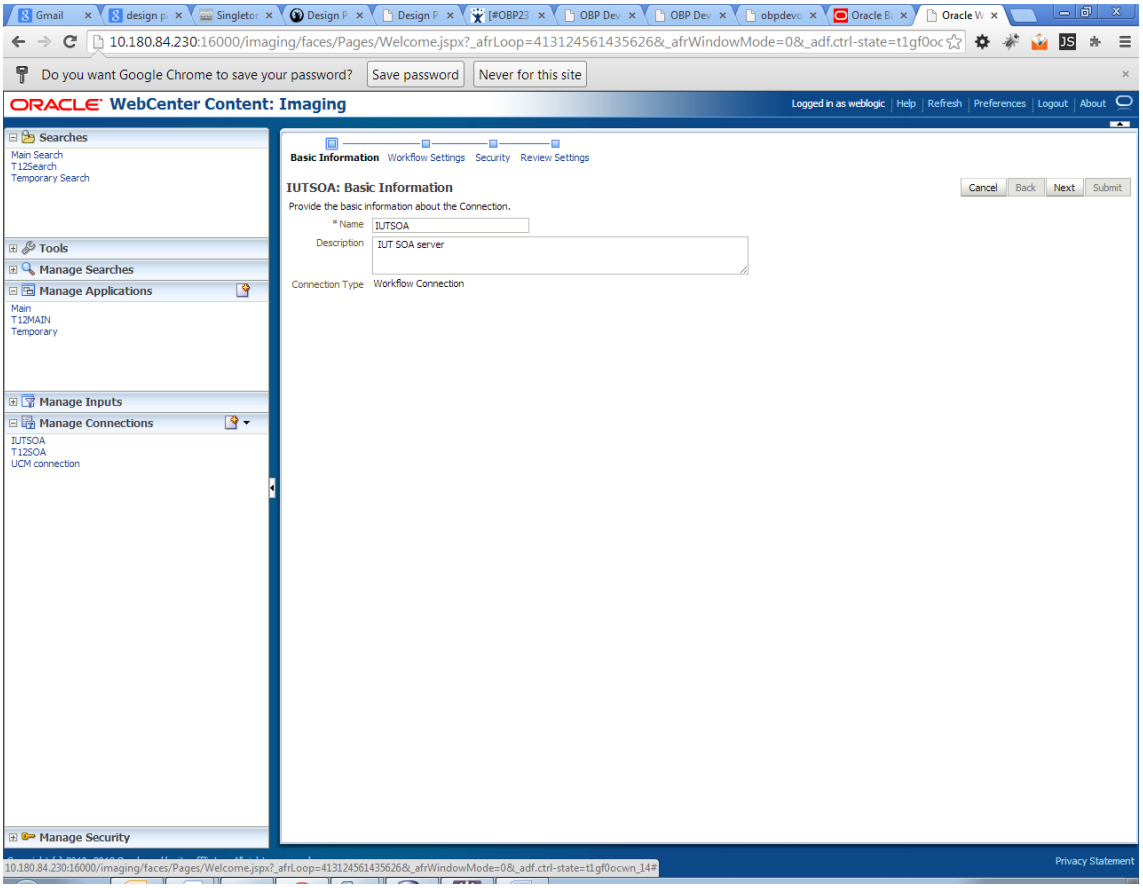
1. Log in to Image Processing Management (IPM).
2. Navigate to the Manage Connections section.

Figure 7–70 Manage Connections: Create Workflow Connection



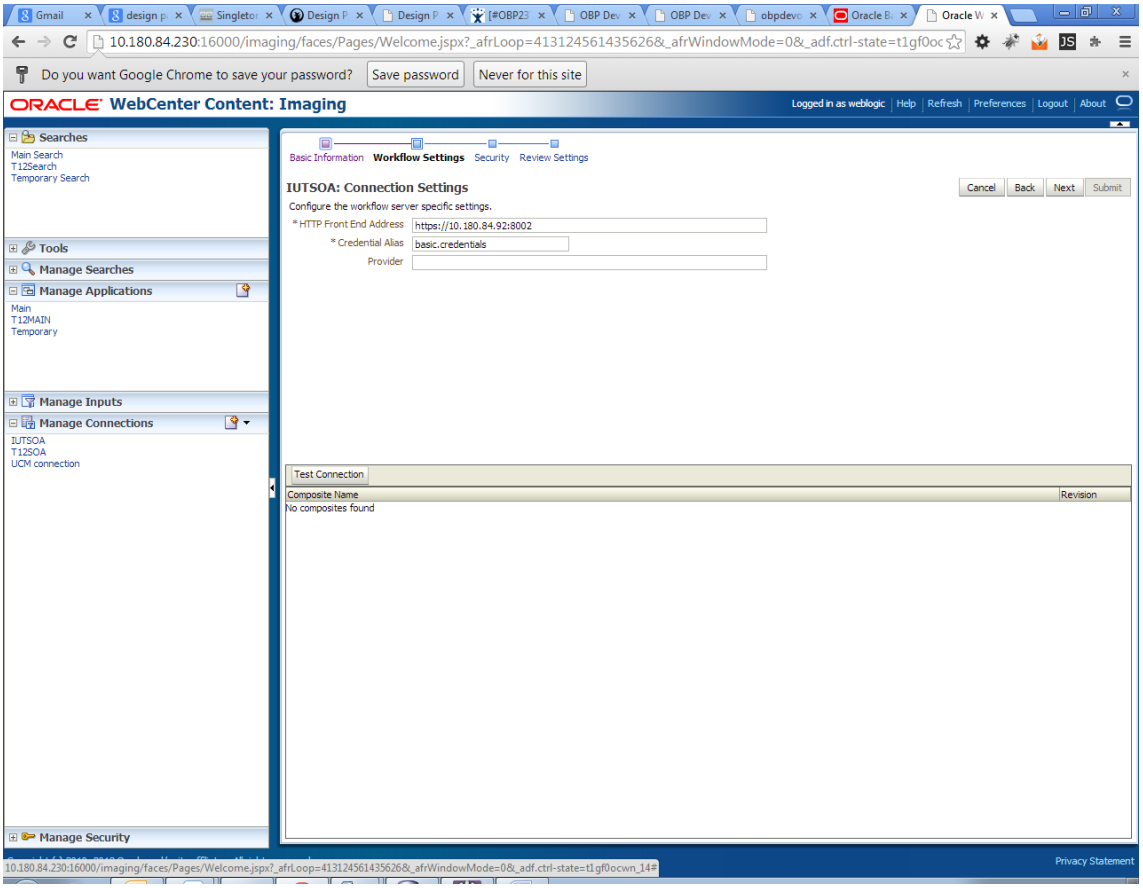
3. Click **Create Workflow Connection.**
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 7–71 IUTSOA: Basic Information



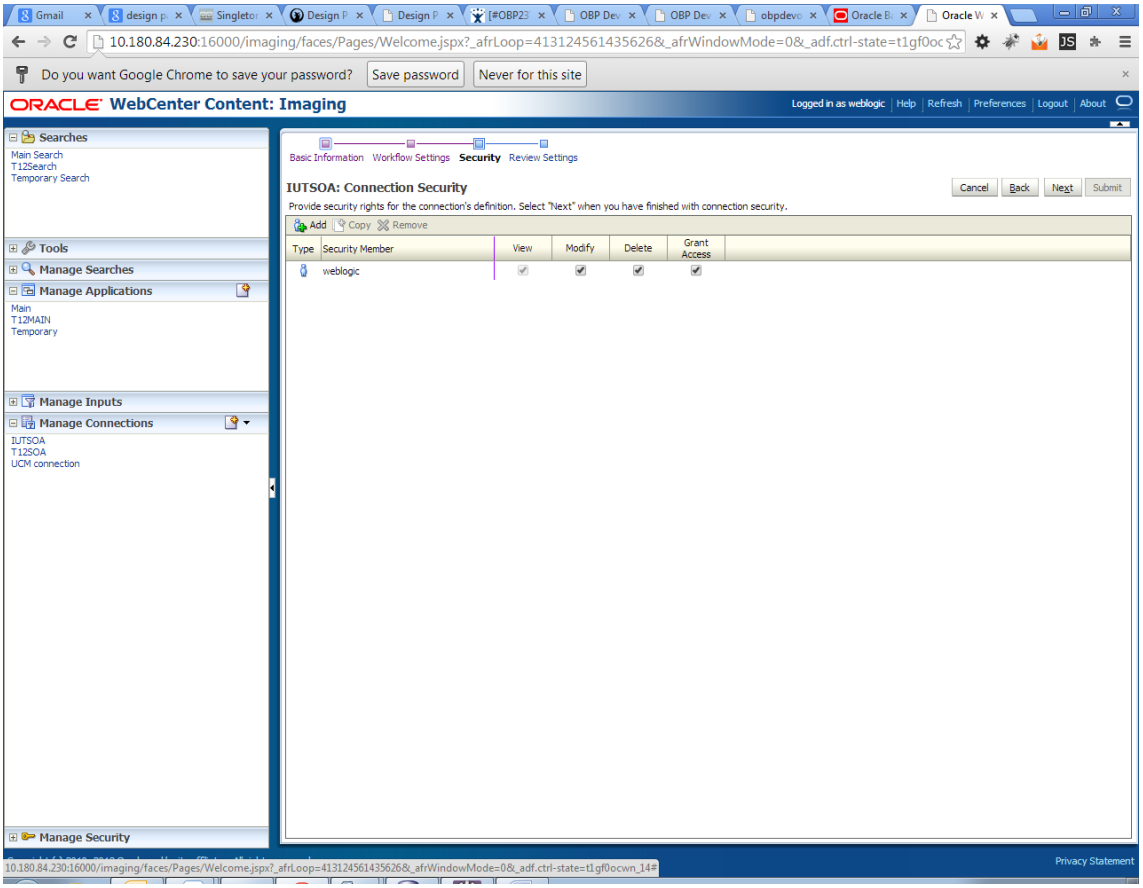
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 7–72 IUTSOA: Workflow Settings



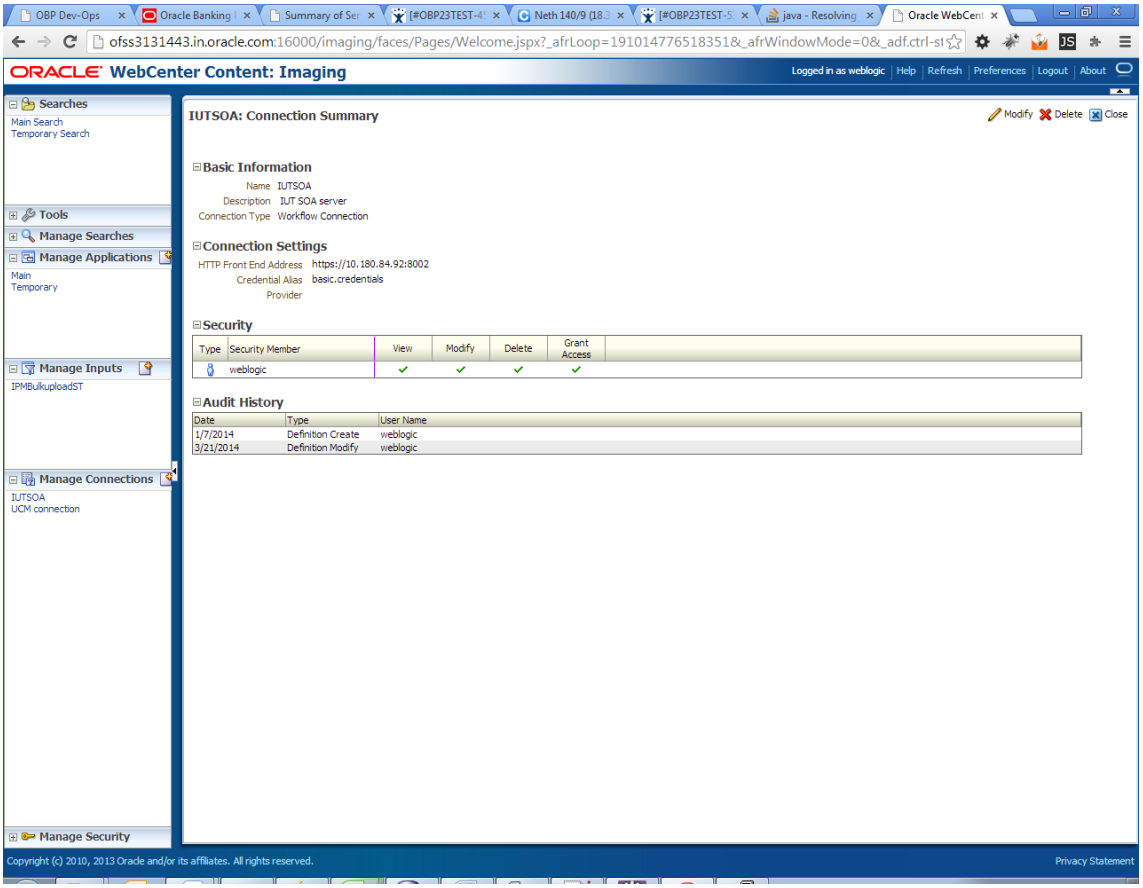
6. In the **Credential Alias** field, enter the value as basic.credentials.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 7–73 IUTSOA: Connection Security



8. Provide the requisite security rights to the connection's definition.
9. Click **Submit.**
10. Click **Next.** The Review Settings page appears.

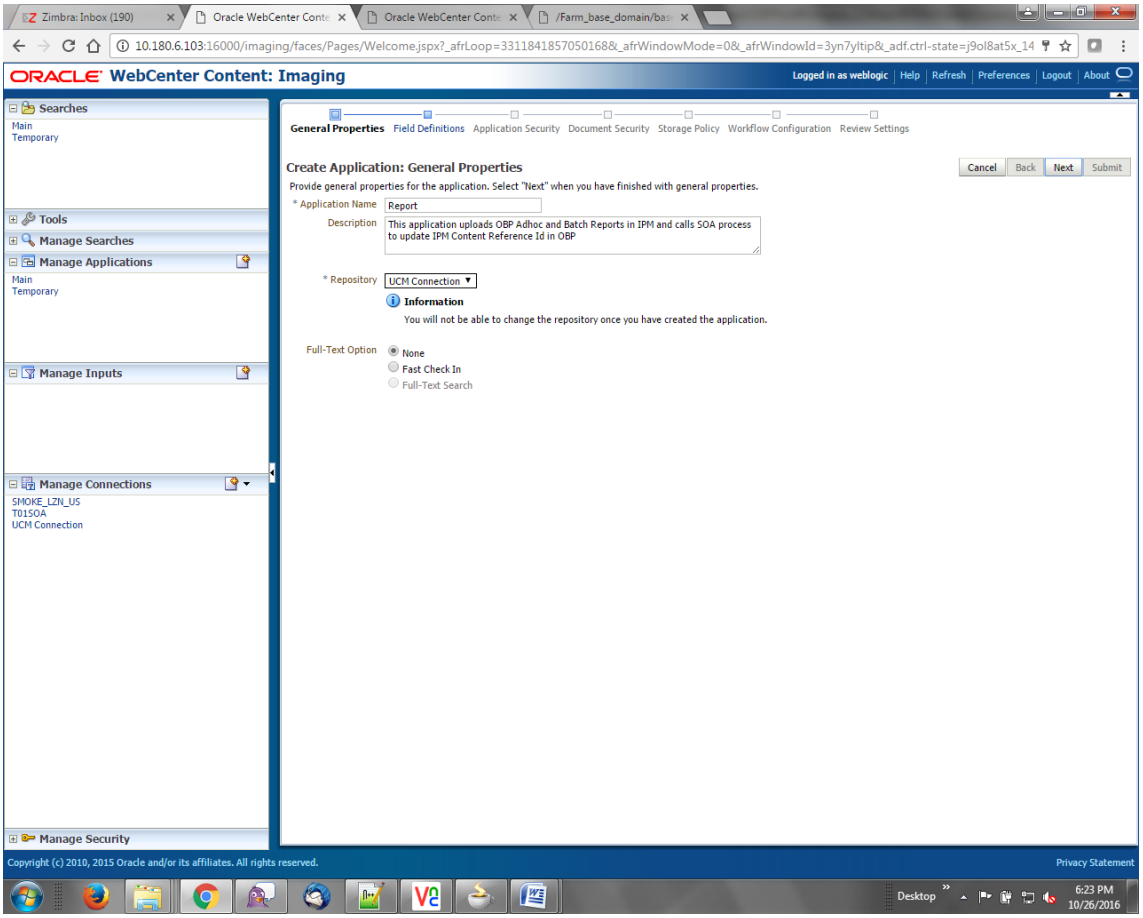
Figure 7–74 IUTSOA: Review Settings



7.3.5 Manage Application Configuration

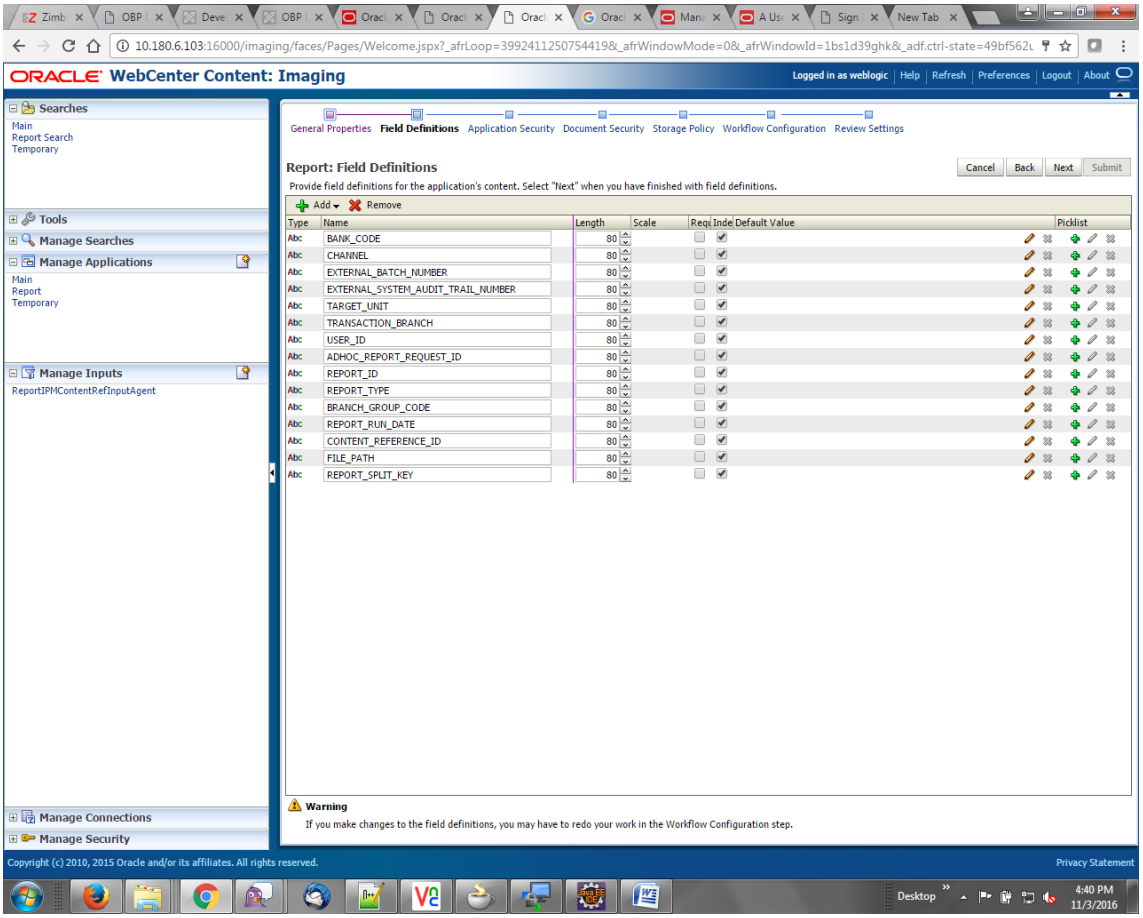
1. Navigate to the Manage Applications section.
2. Select Create New Application option. The Create Application: General Properties page appears.

Figure 7–75 Create Application: General Properties



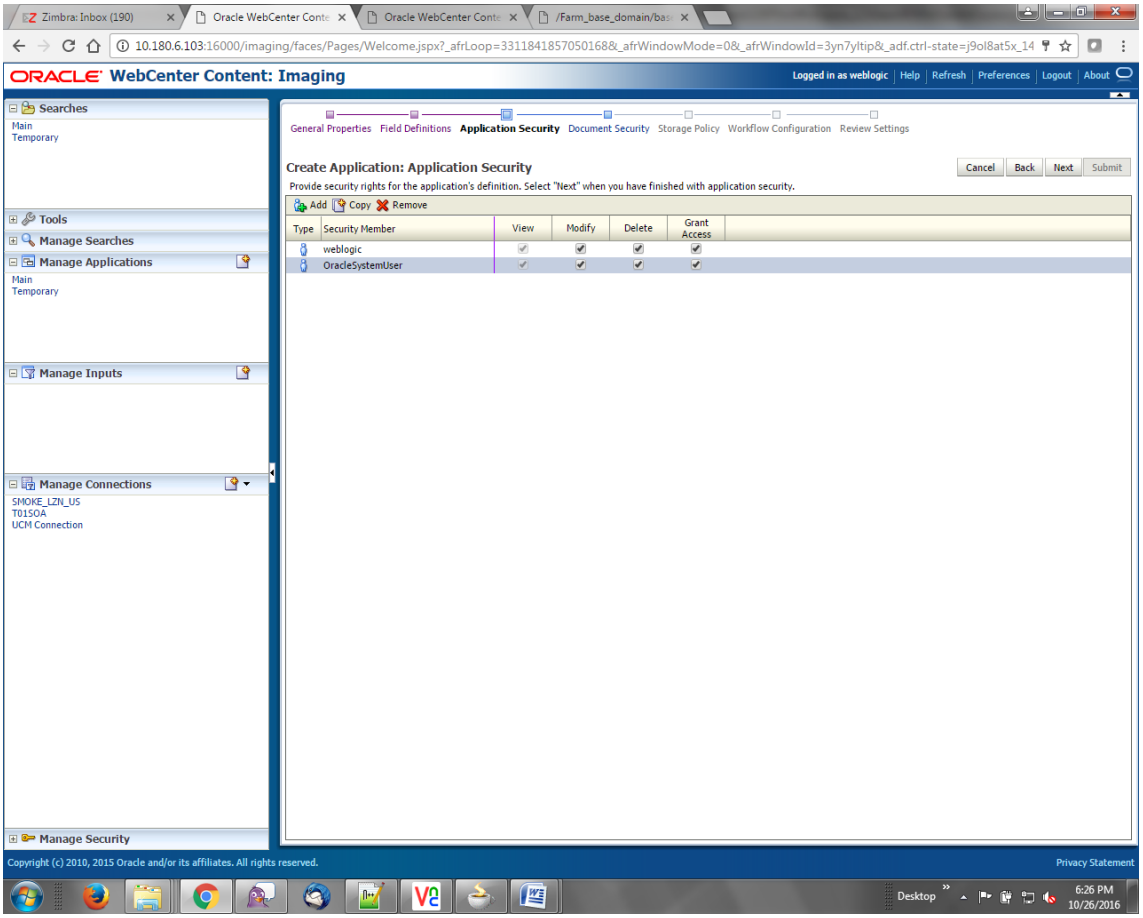
3. Enter the general properties for the application and click **Next.** The Report: Field Definitions page appears.

Figure 7–76 Report: Field Definitions



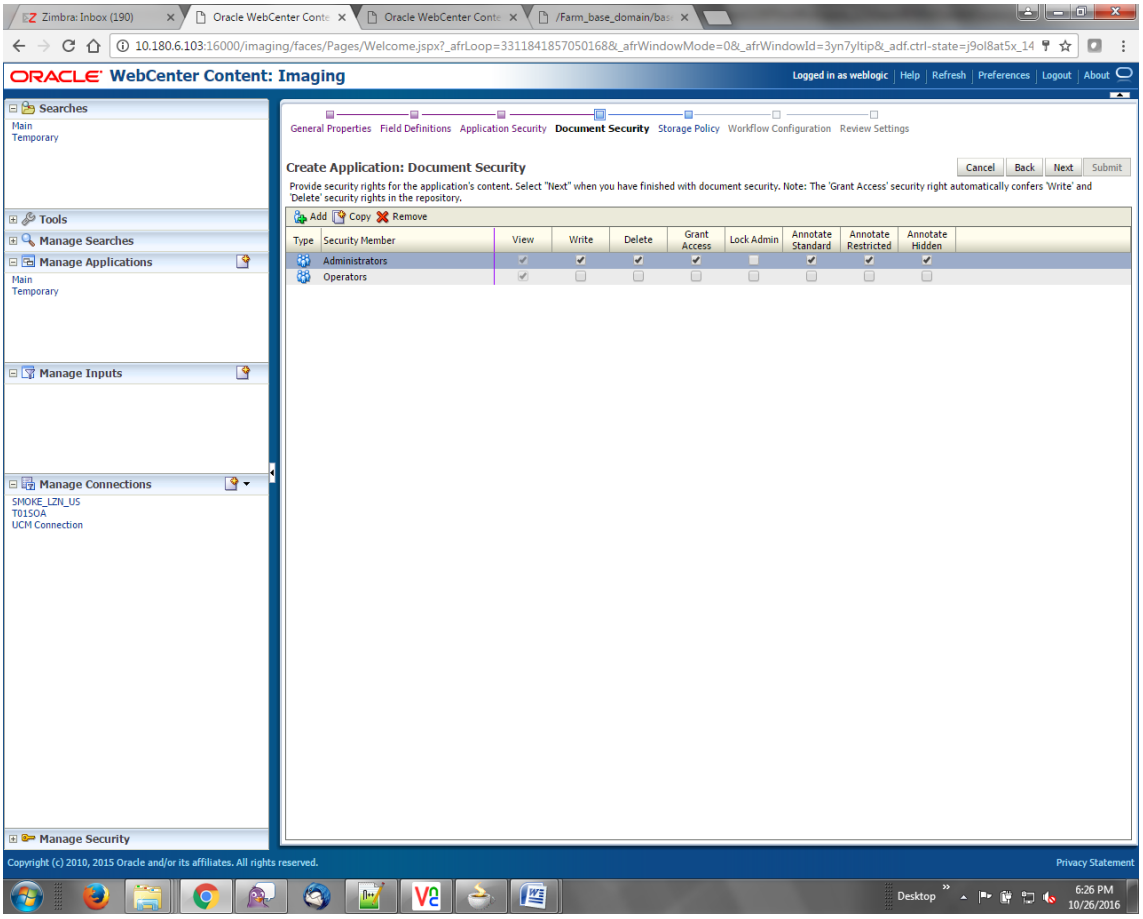
4. Enter the field definition details and click **Next.** The Create Application: Applications Security page appears.

Figure 7–77 Create Application: Applications Security



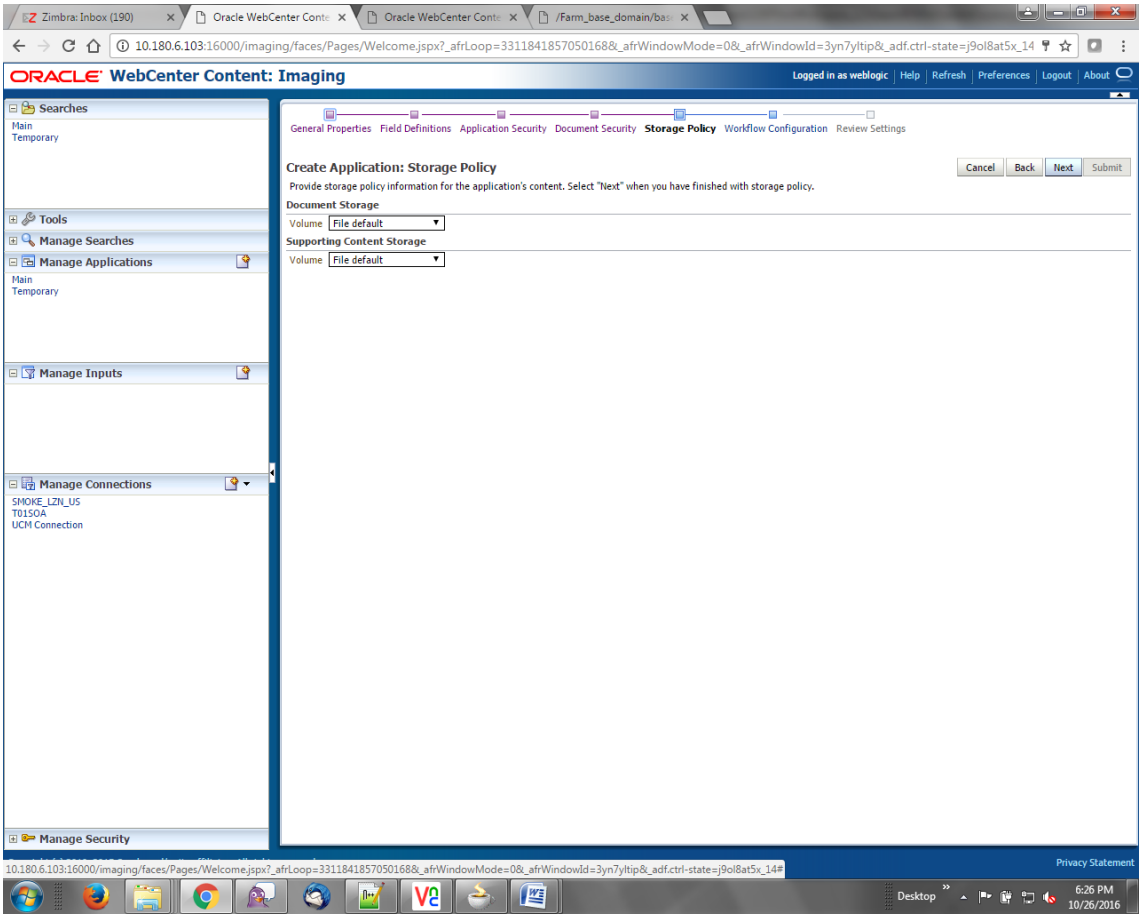
5. In the Application Security section, select the access rights for users and click **Next.** The Create Application: Document Security page appears.

Figure 7–78 Create Application: Document Security



6. In the Document Security section, select the access rights for users and click **Next.** The Create Application: Storage Policy page appears.

Figure 7–79 Create Application: Storage Policy



7. In Storage Policy section, select the **File Default** option in the Document Storage and Supporting Content Storage fields.
8. Click **Next.** The Report: Workflow Configuration page appears.
9. Enter the Workflow Configuration details in the Server Properties, Component Properties and Payload Properties sections as shown.

Figure 7–80 Report: Workflow Configuration - Server Properties

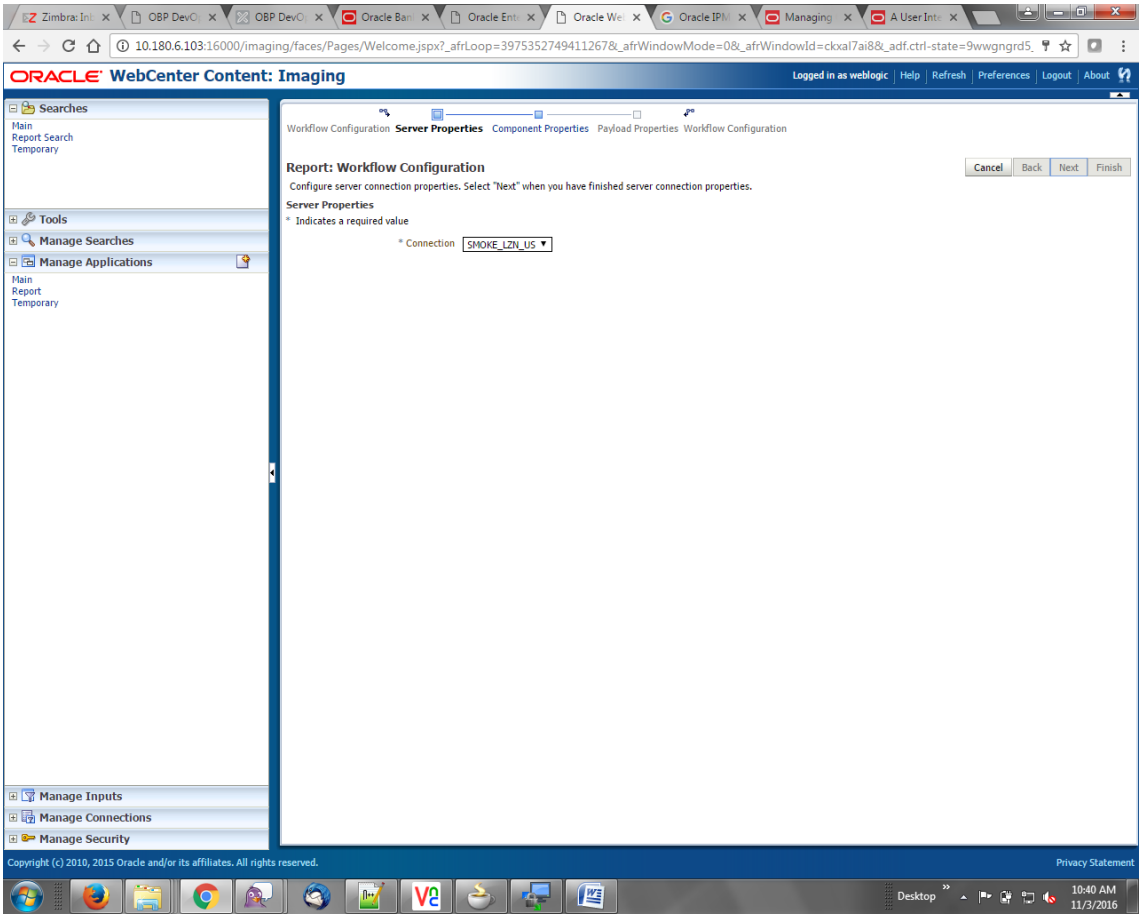


Figure 7–81 Report: Workflow Configuration - Component Properties

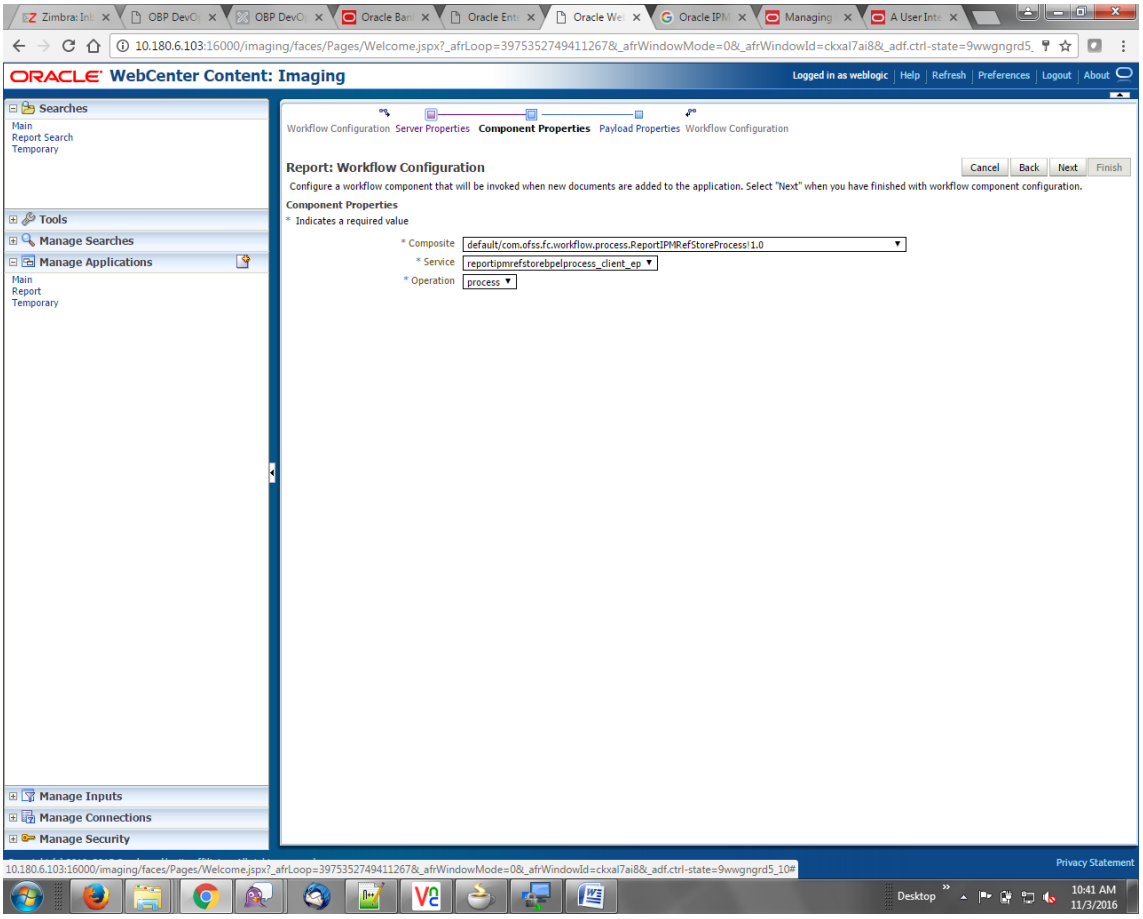
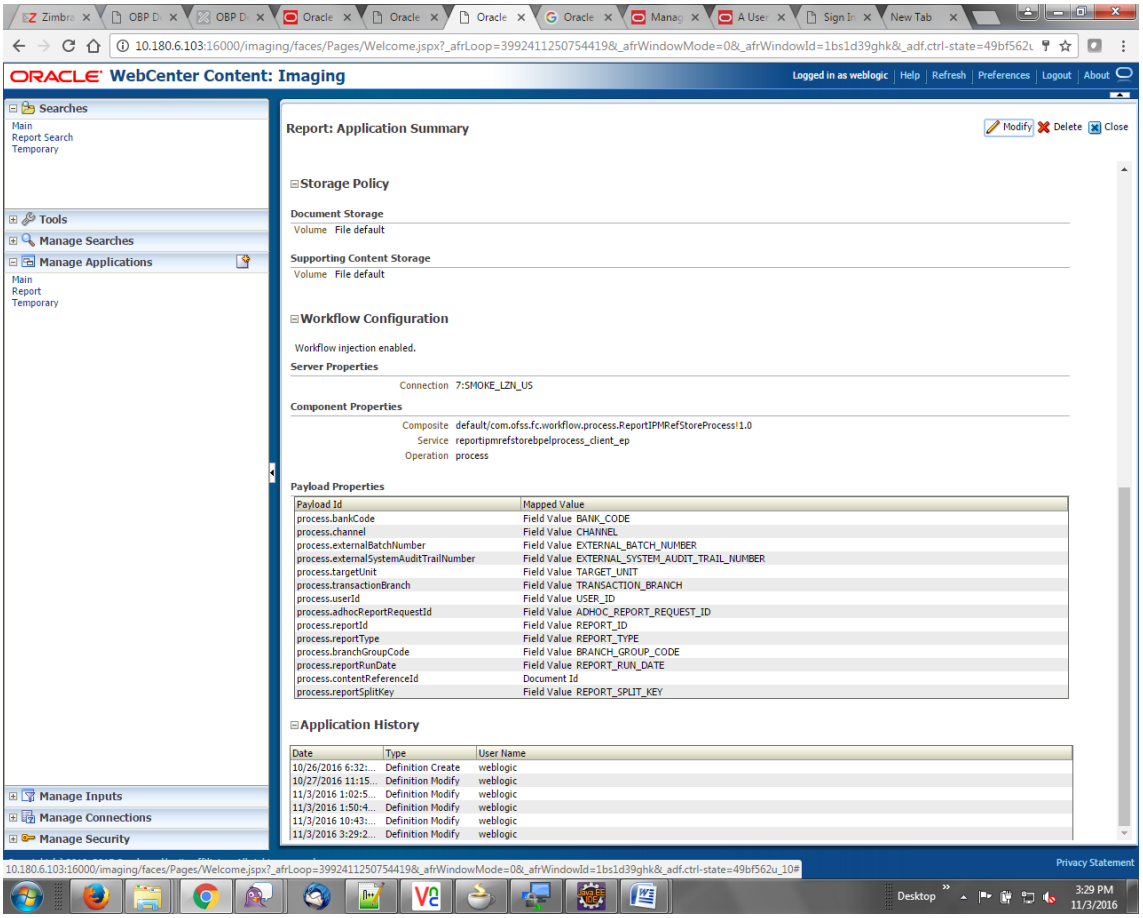
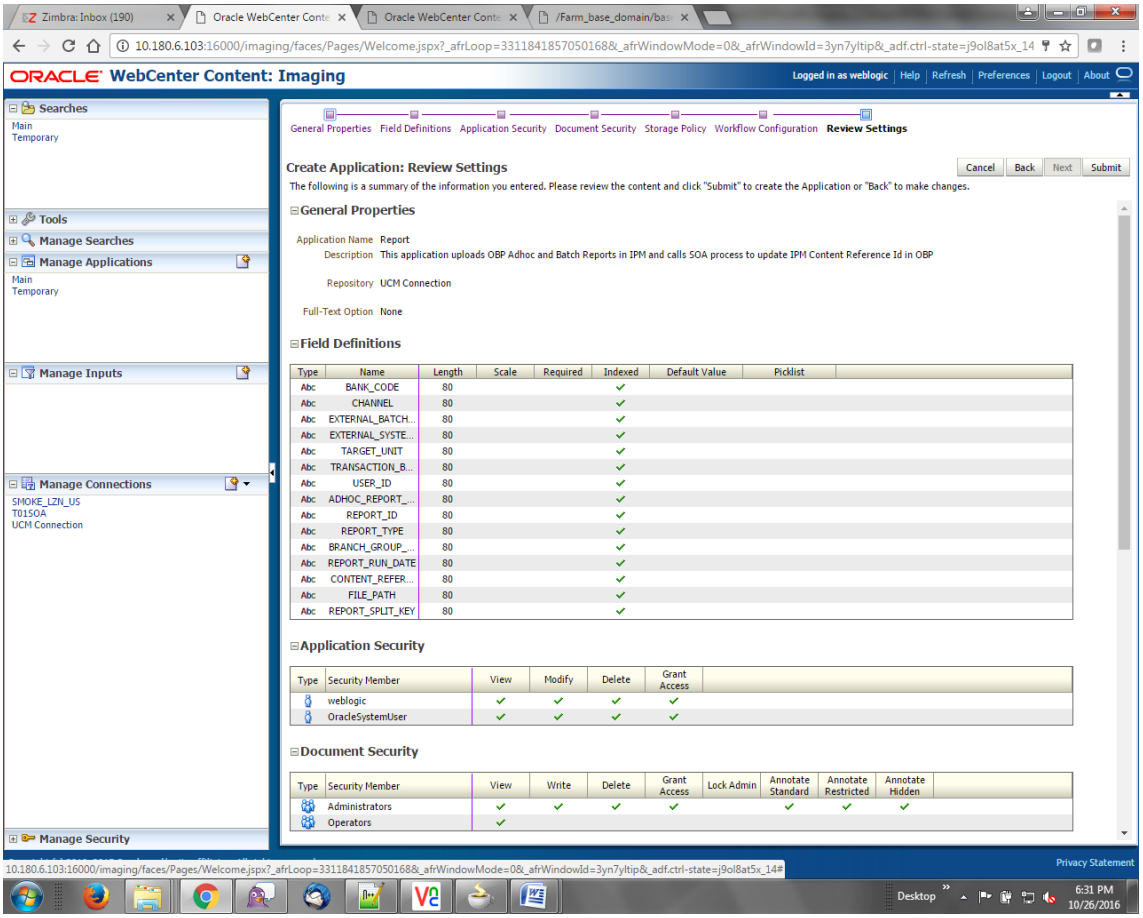


Figure 7–82 Report: Application Summary



10. Review the summary and click **Submit.**

Figure 7–83 Create Application: Review Settings

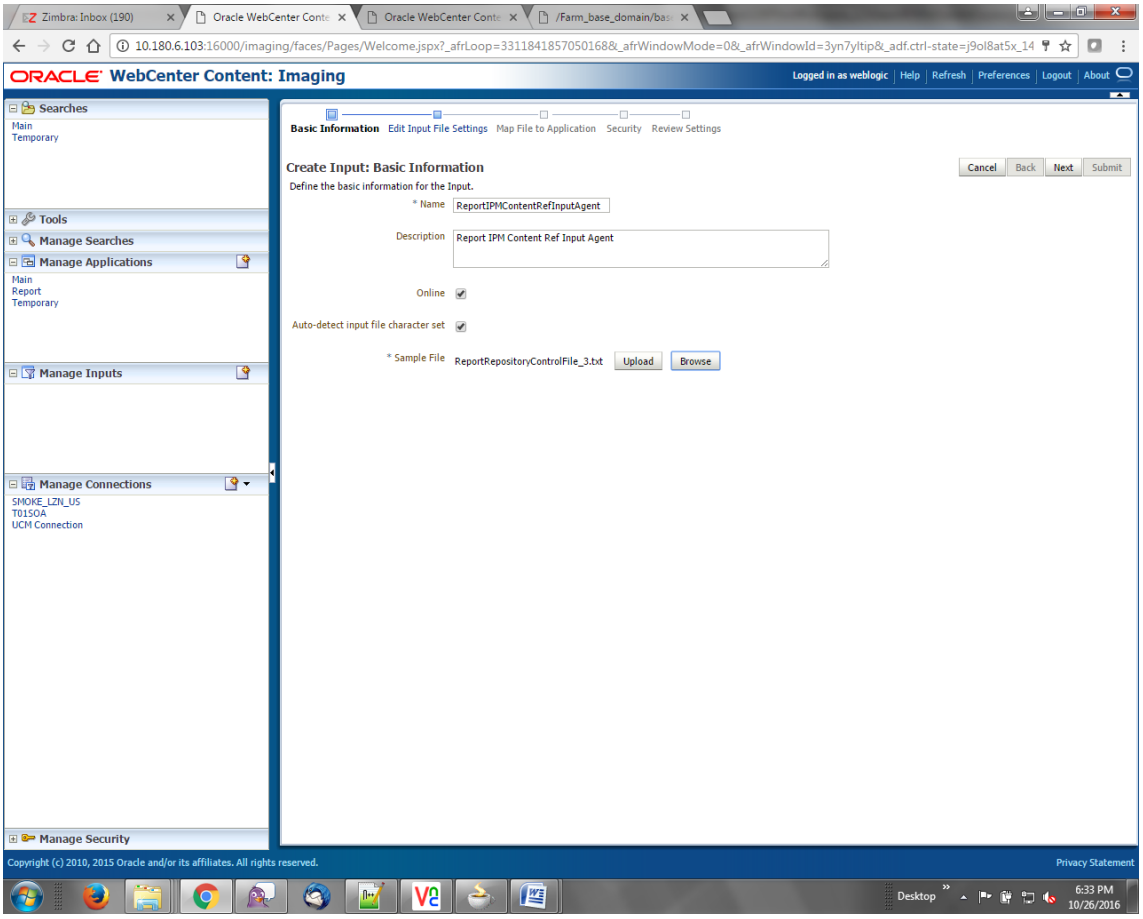


7.3.6 Manage Inputs for Input Agents

To manage workflow configuration:

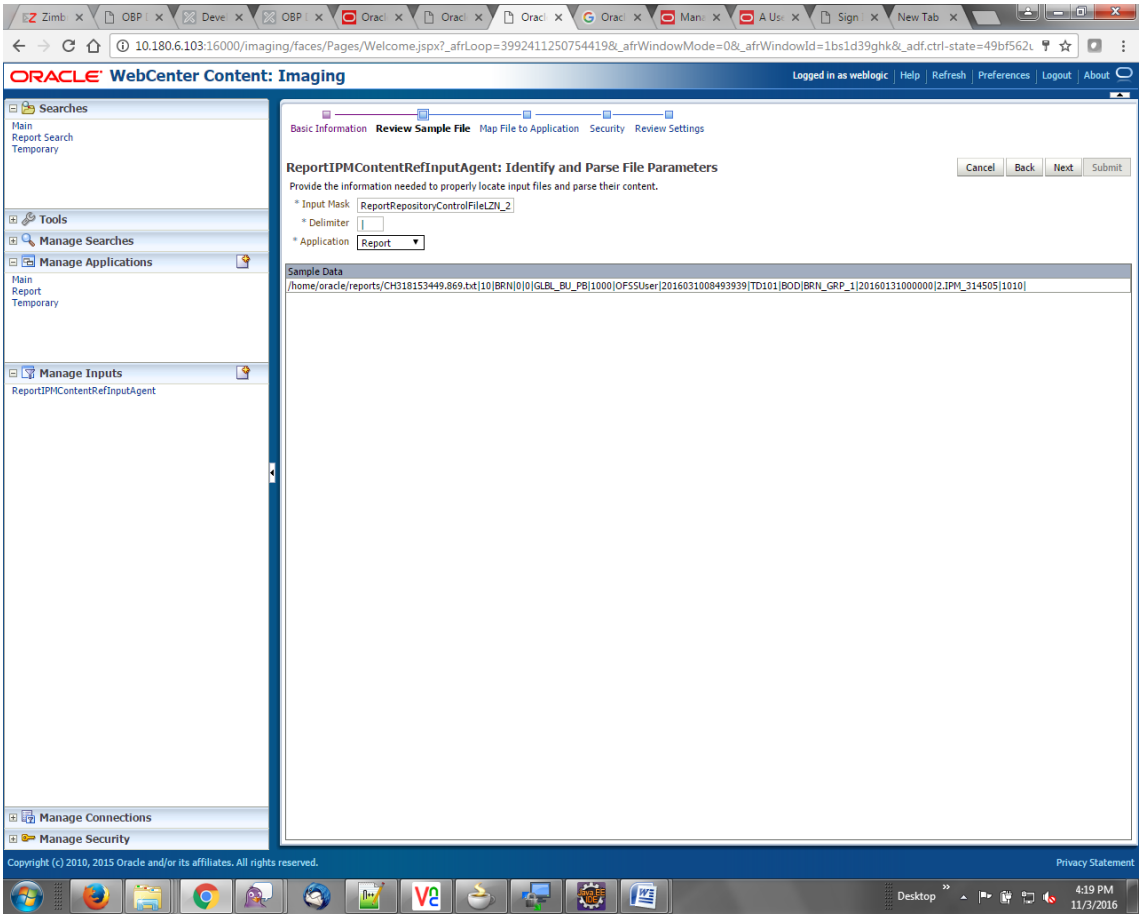
1. Log in to Image Processing Management (IPM).
2. Navigate to Manage Inputs section.

Figure 7–84 Manage Inputs



3. Define an input agent by entering a Name. For example, bulkUploadInput.
4. Define Input Mask as ReportRepositoryControlFileLZN*.txt.

Figure 7–85 Input Agent Details: Input Mask



5. Upload the sample file.

   For example, name the sample file as ReportRepositoryControlFile.txt and add the following content to the sample file.

   ```
   /home/oracle/reports/CH318153449.869.txt|10|BRN|0|0|GLBL_BU_
   PB|1000|OFSSUser|2016031008493939|TD101|BOD|BRN_GRP_
   1|20160131000000|2.IPM_314505|1010|
   ```

6. In the **Input Mask** field, enter the value which should be the same as the name given in table.

   flx_fw_config_all_b

   select prop_value from flx_fw_config_all_b where category_id = reports and prop_id=REPORT_UPLOAD_FILE_NAME_PREFIX;

   appended with name given in table flx_fw_config_var_b

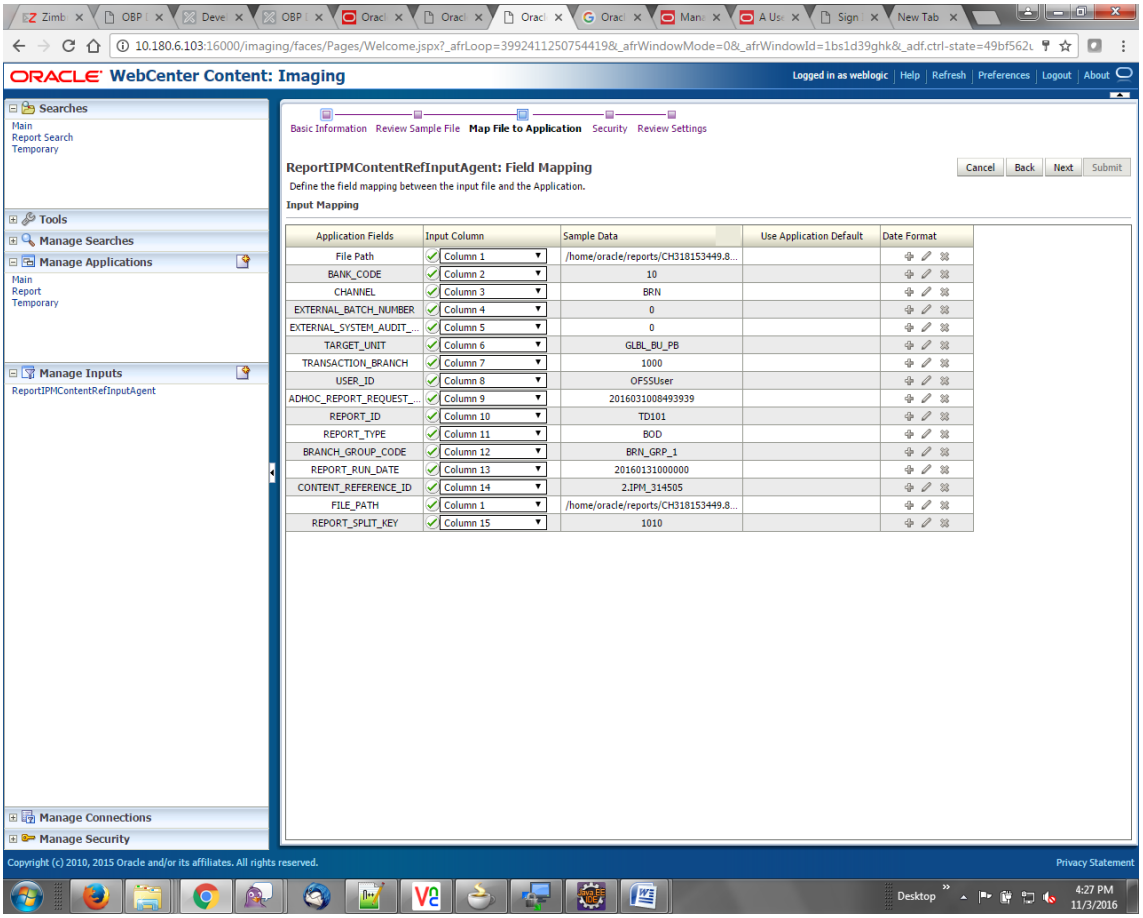
   select prop_value from flx_fw_config_var_b where prop_id = env.name;

Note

Input Mask name should have a * (asterisk character) to enable the process to read all the files whose prefix is same as the input mask value.

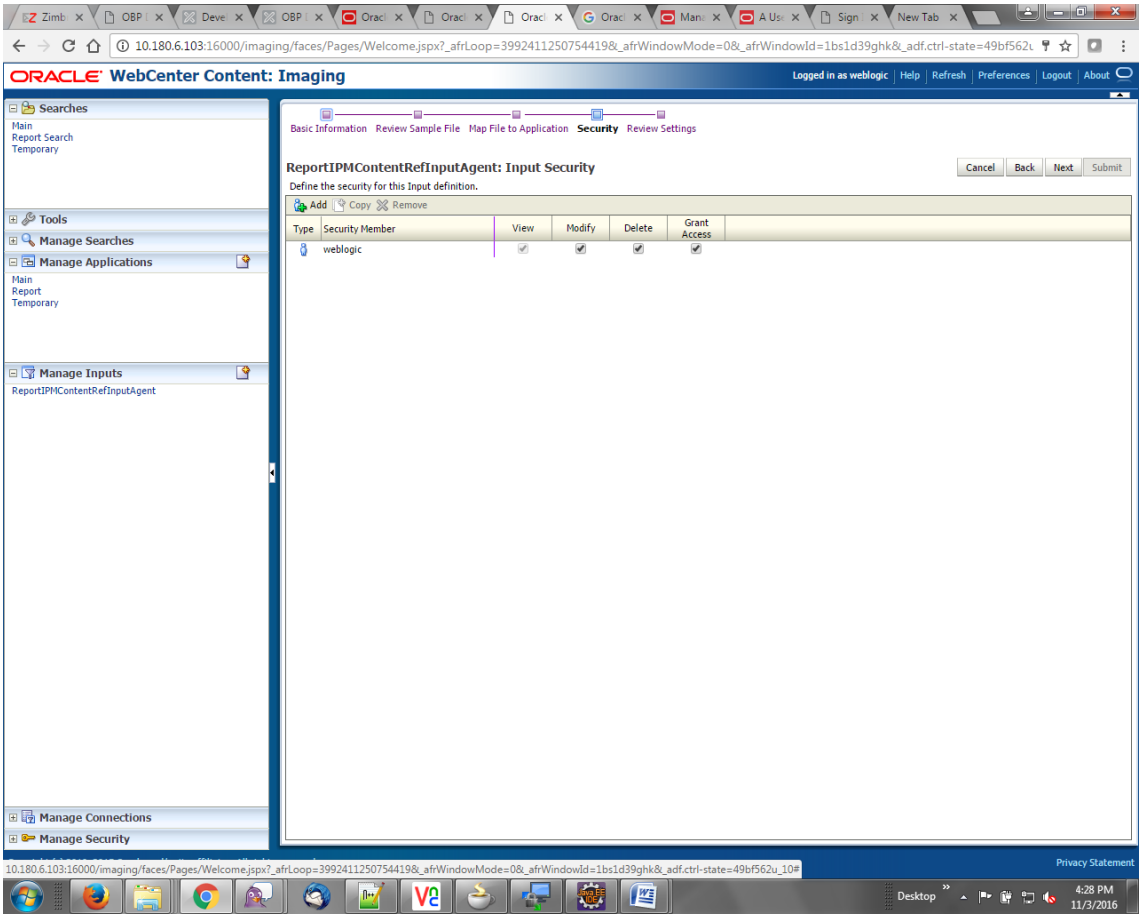
7. In the **Delimeter** field, enter the delimiter value as | (vertical bar character).
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 7–86 Input Agent Details: Field Mapping



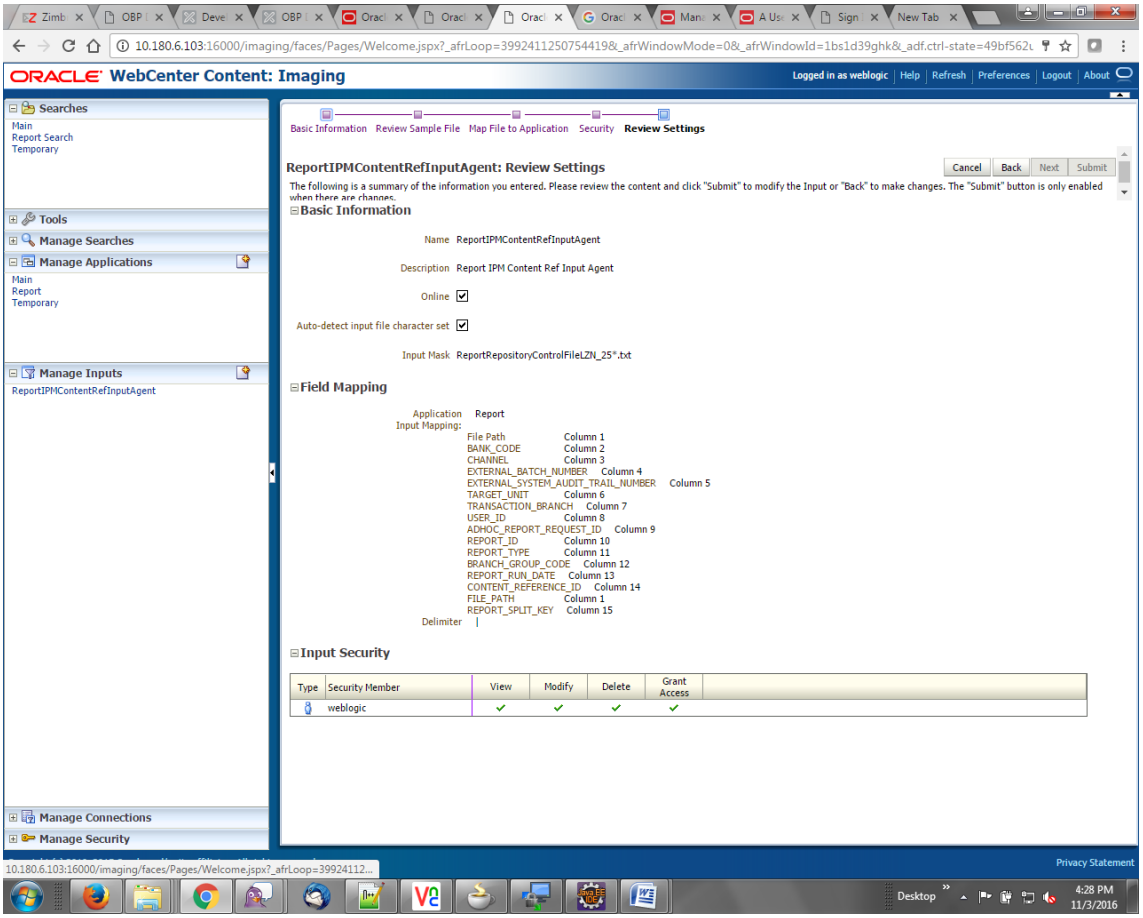
9. Select the access rights for user in the Security section and click **Next.**

Figure 7–87 Input Agent Details: Security



The Input Summary appears. The Input agent must have the settings similar to those shown in the following figure.

Figure 7–88 Input Agent Details: Review Settings



Note

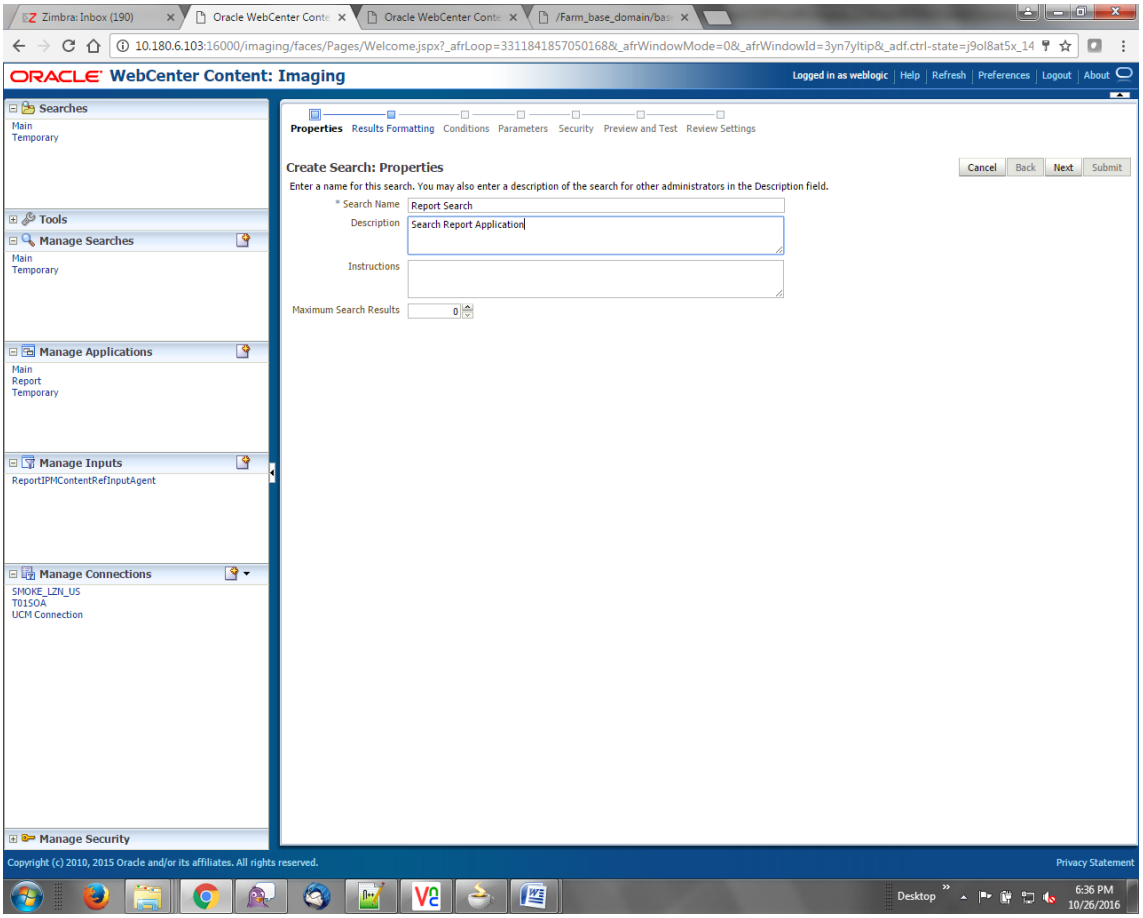
Do not forget to toggle online, else the input agent will not pick up any file for processing.

7.3.7 Manage Searches

To manage searches:

1. Click Manage Searches option and enter the search name with description.

Figure 7–89 Create Search: Properties



2. Select the source application along with its field details.

Figure 7–90 Create Search: Results Formatting

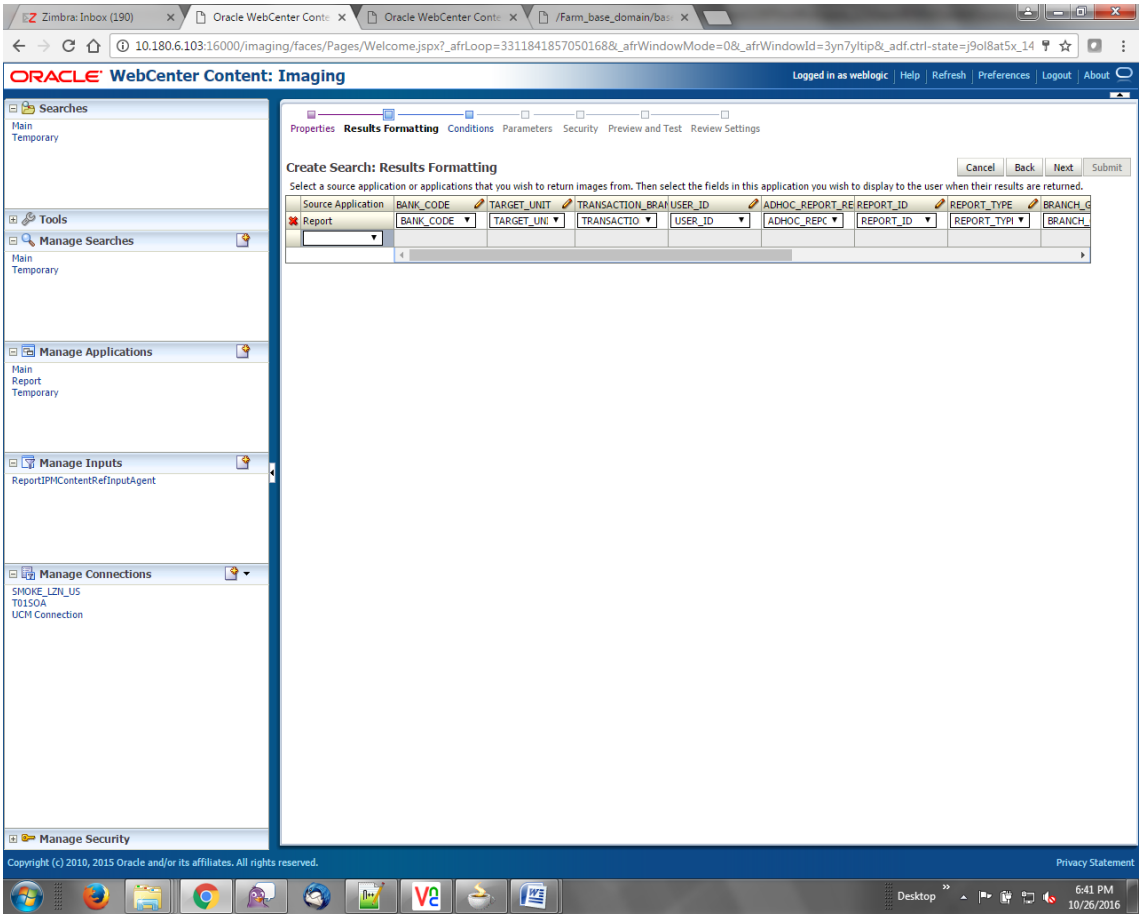


Figure 7–91 Create Search: Conditions

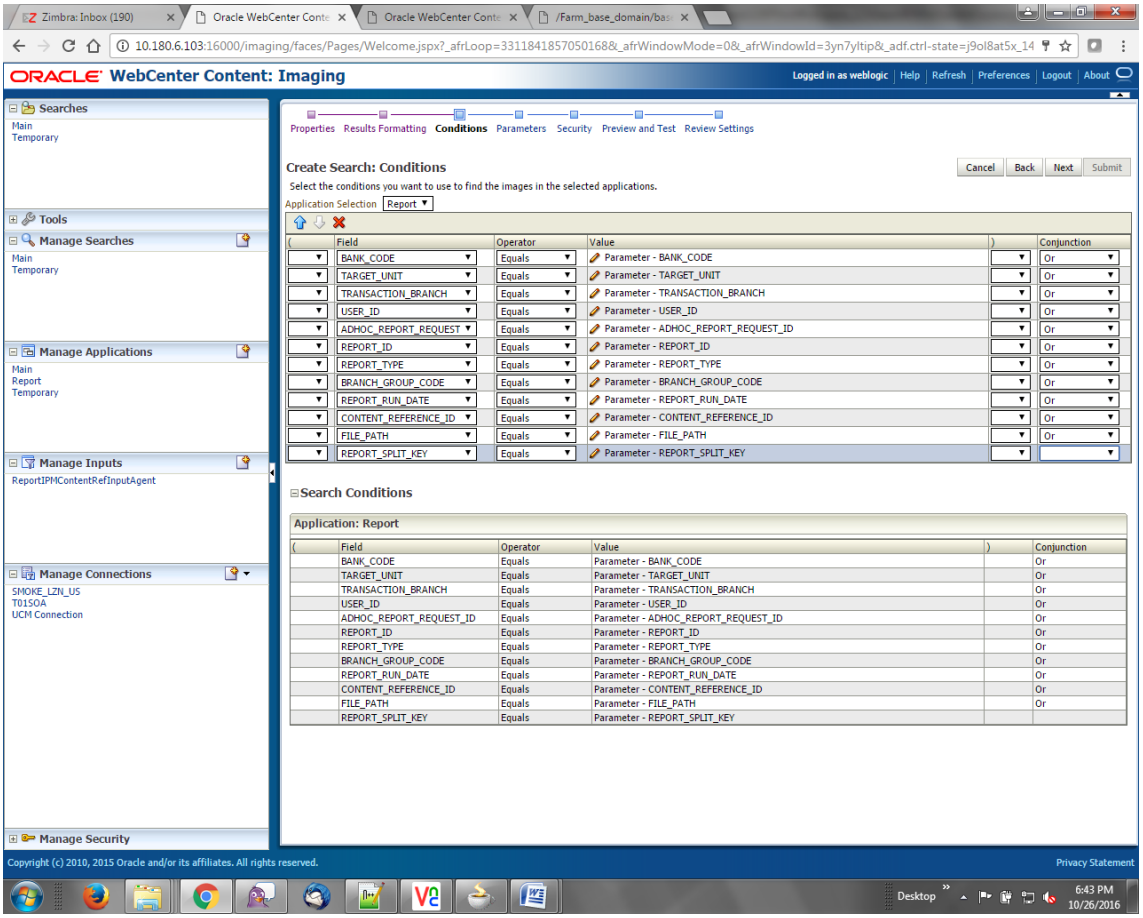
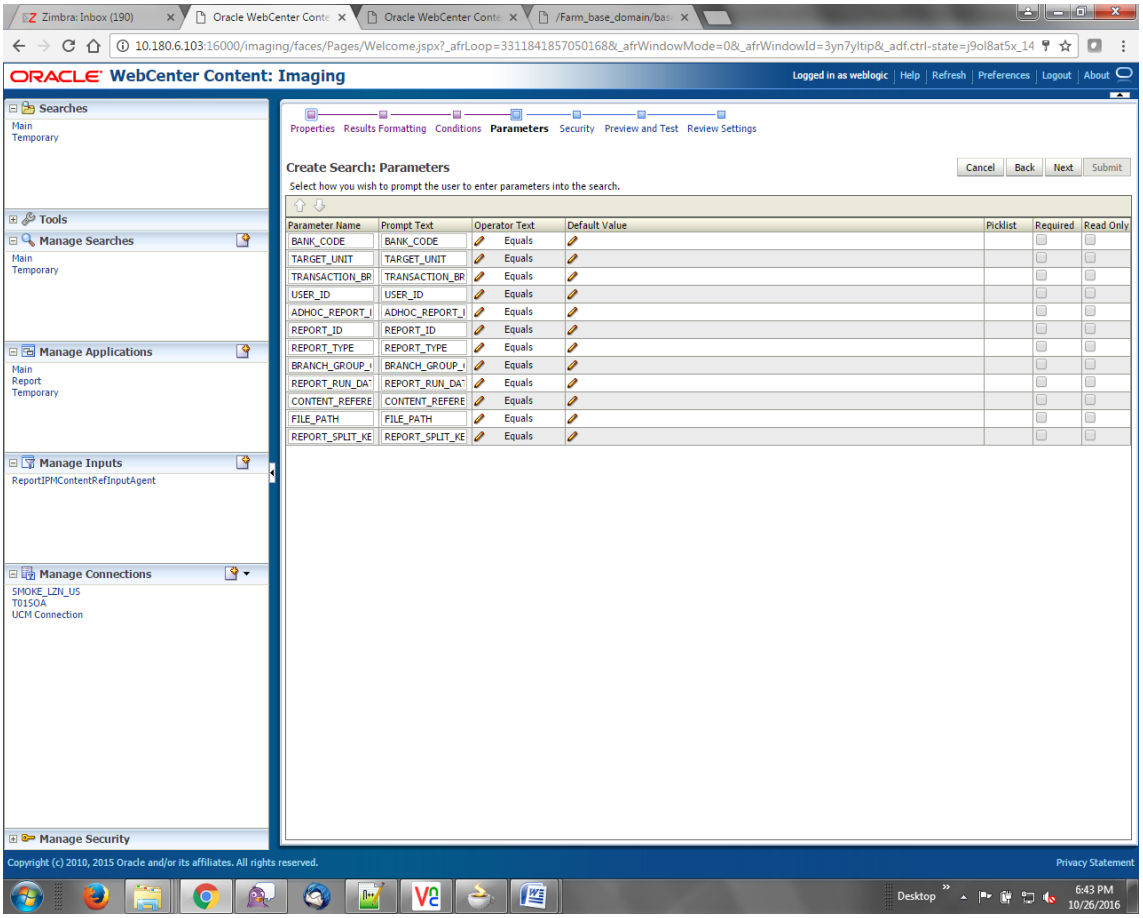
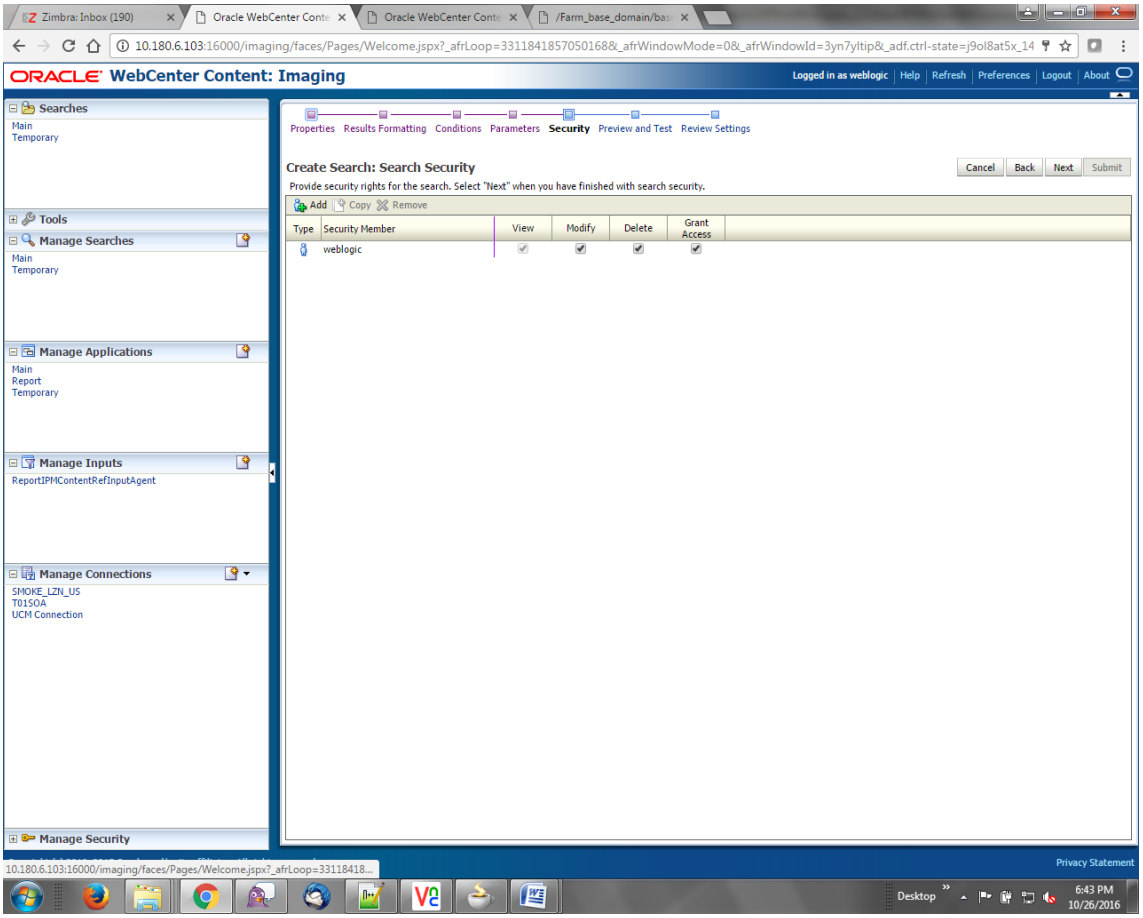


Figure 7–92 Create Search: Parameters



3. Select the access rights for users in security configuration.

Figure 7–93 Create Search: Security



4. Review the summary and click **Submit.**

Figure 7–94 Create Search: Preview and Test

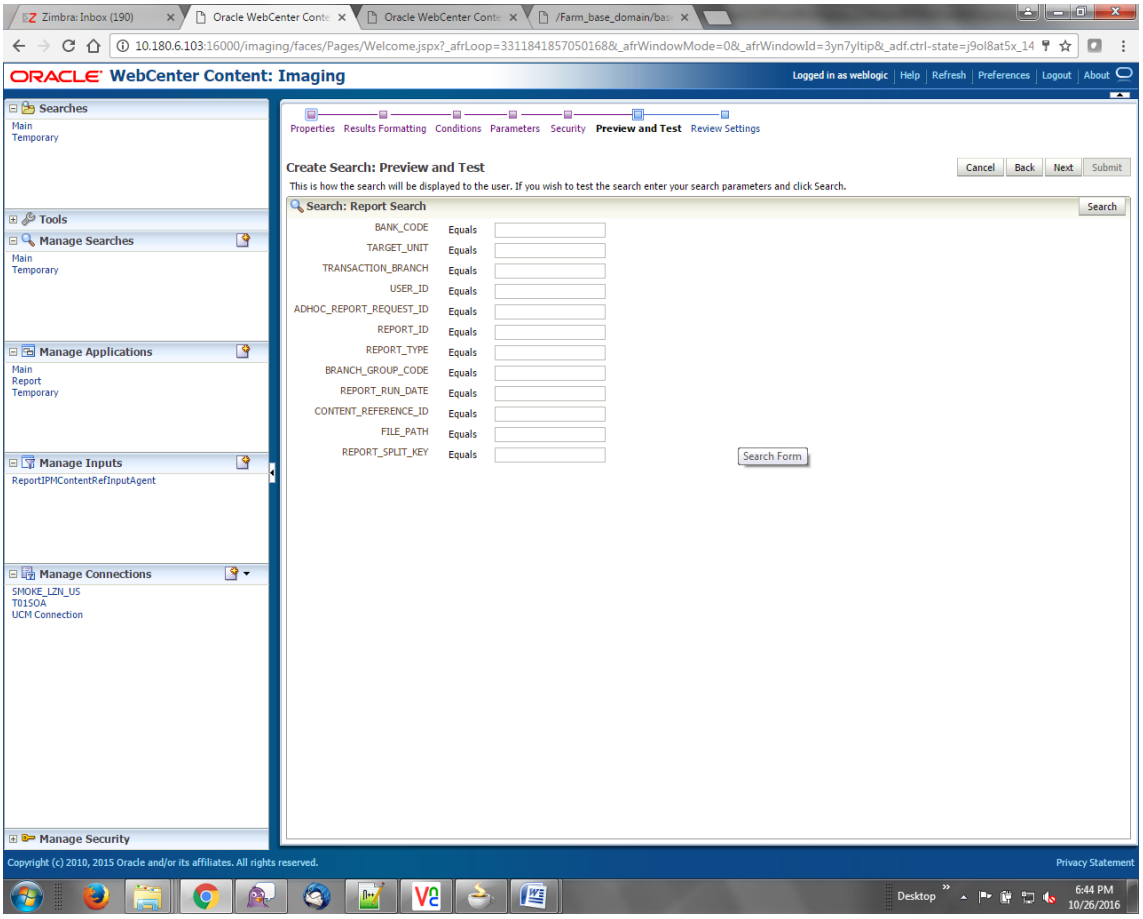
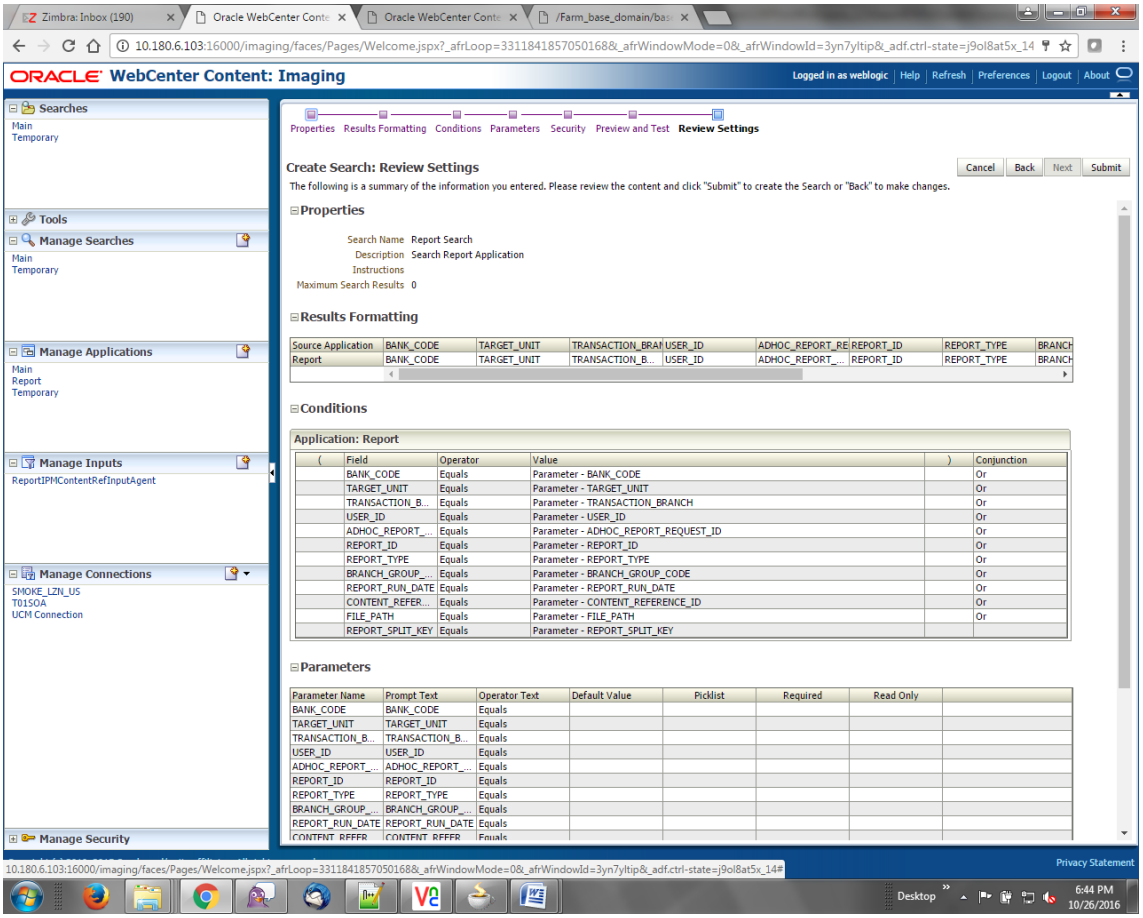


Figure 7–95 Create Search: Review Settings



7.3.8 Additional Steps

1. Update user and bankcode as follows:

   update flx_fw_config_all_b set prop_value= ofssuser where prop_id='userId' and category_id like contentmanager%;

2. In the flx_fw_config_all_b table, the values for PROP_ID should be the same as mentioned for path in IPM server.

Table 7–2 PROP ID Values

PROP_ID	PROP_VALUE
FTPSERVER.DMSFILEPATH=/scratch/ofssobp/testinputagent/inputdir1/	Path in IPM config
FTPSERVER.REPORTPATH=/scratch/reports/	Path where files will be FTP
FTPSERVER.HOST	IPM IP
BULK_UPLOAD_FILE_NAME_PREFIX	Input Mask name

PROP_ID	PROP_VALUE
	given in 1.5 Manage Inputs for Input Agents section.

3. FTP service on IPM server should be running and FTP user should be created on host user connectors.
4. For resolving the SSLHandshake between IPM and SOA server:
    a. Save the SOA Server Certificate. SOA certificate needs to be saved in Base64 (.cer) format for import to IPM server.
    b. Import the SOA server certificate on IPM server with following command.

        Copy certificate at the following path on IPM server.

        path:/scratch/app/product/oracle_jrockit_jdk1.6.0_37_R28.2.5_4.1.0/jre/lib/security

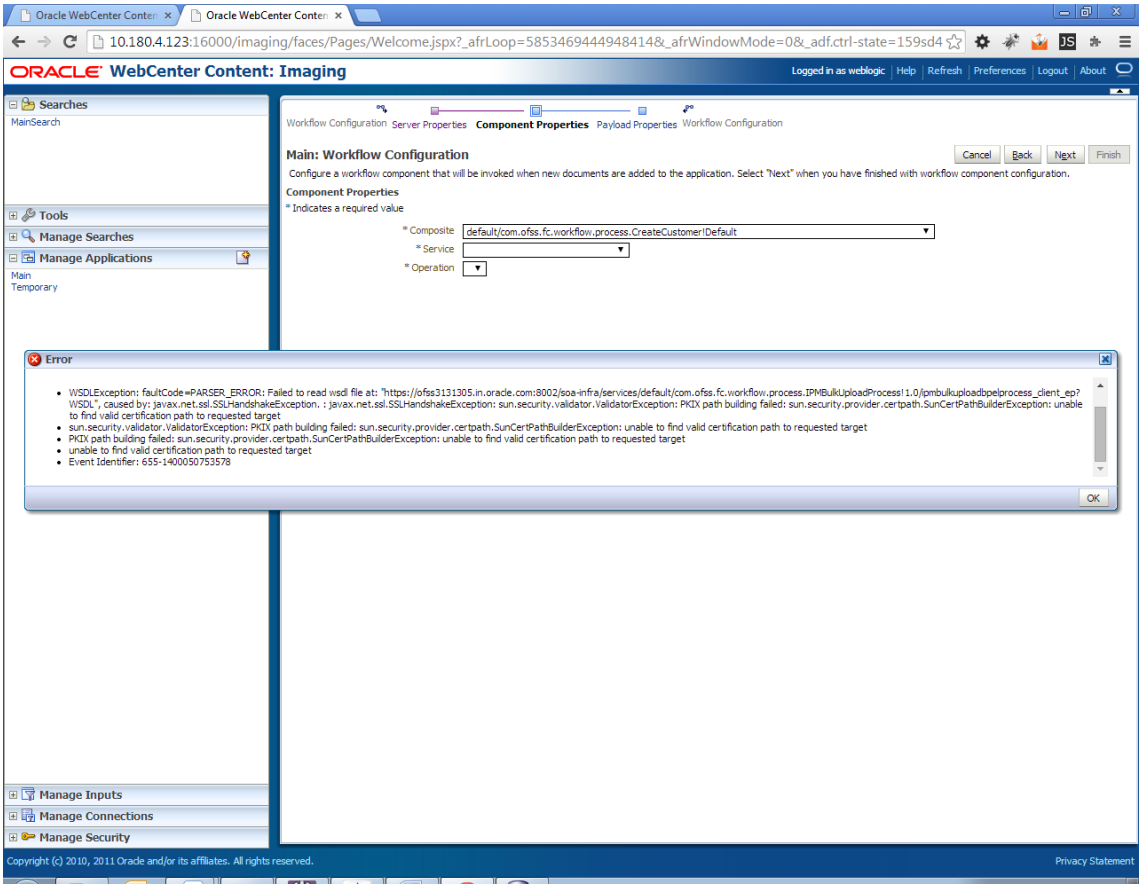
        keytool -import -noprompt -trustcacerts -alias UI_SSL_trustself -file SOACert.cer -keystore cacerts -storepass changeit
    c. Security policy for ReportIPMRefStoreProcess can been removed (if required).

        Security for called method

        com.ofss.fc.app.report.ReportGenerationApplicationService.updateAdhocReportContentRefId (SessionContext, ReportRequestDTO) needs to be removed (for Development environment).

        com.ofss.fc.app.report.ReportGenerationApplicationService.updateBatchReportContentRefId (SessionContext, BatchRequestDTO) needs to be removed (for Development environment).
        com.ofss.fc.app.report.ReportGenerationApplicationService.updateSplitReportContentRefId (SessionContext, ReportSplitDetailDTO) needs to be removed (for Development environment).

Figure 7–96 Component Properties



8 BIP Datasource Creation

This chapter explains the steps required for Business Intelligence Publisher (BIP) datasource creation.

8.1 BIP Datasource Creation

To use BIP, it is required to create datasource in BIP server. This can be done after Host pre-install. The data source must point to the same db schema as given in BIP_DATASOURCE_NAME in installobphost.properties.

Follow the below mentioned steps to create the datasource:

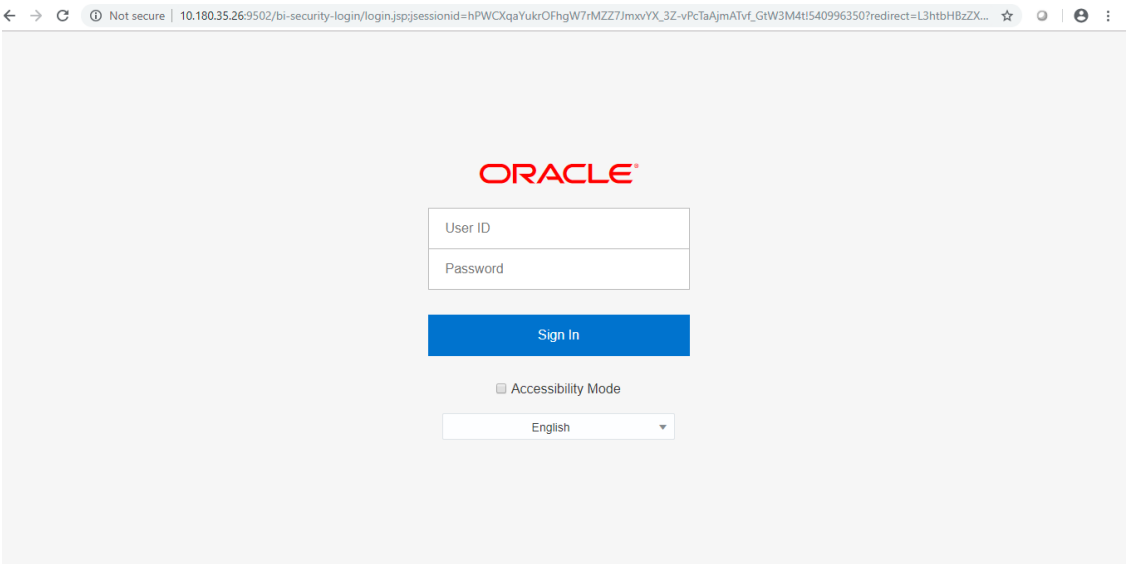
1. Open a browser and navigate to:

   <BIP_SERVER_IP>:<BIP_SERVER_PORT>/xmlpserver

2. Log in using the following credentials:

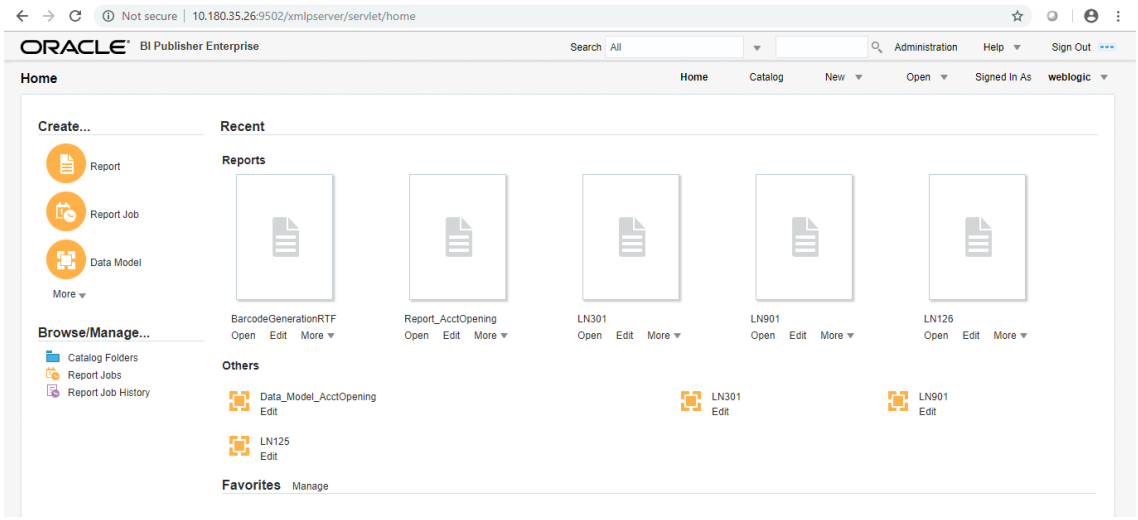
   - Username: <BIP_SERVER_USER>
   - Passowrd: <BIP_SERVER_PSWD>

Figure 8–1 BIP Server Console Login



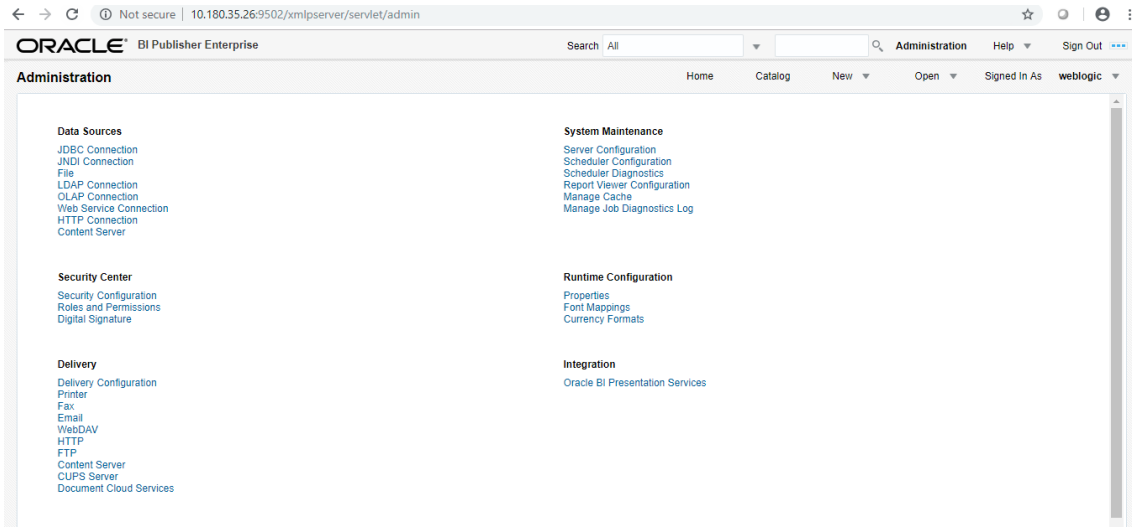
3. After logging in, click **Administration**.

Figure 8–2 BIP Administration



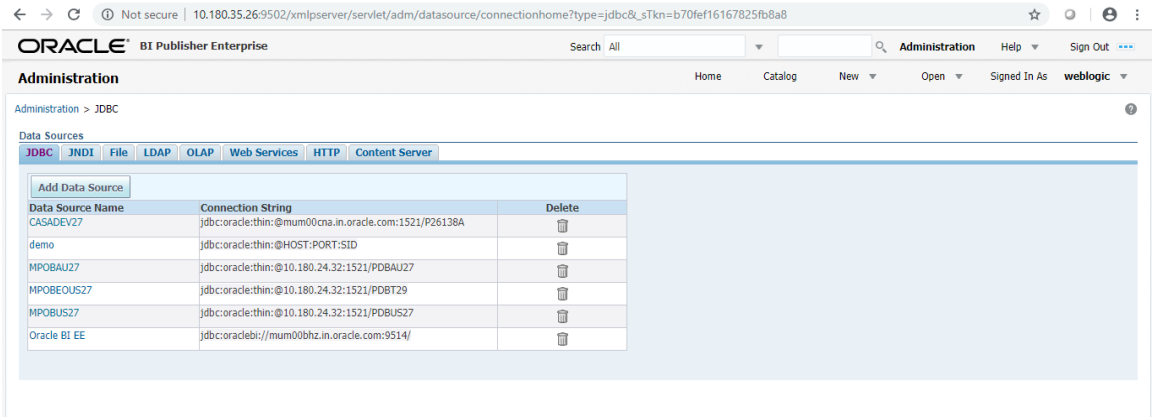
4. Click **JDBC Connection** under **Data Sources**.

Figure 8–3 BIP JDBC Connection



5. Click the **Add Data Source** button.

Figure 8–4 BIP - Add Data Source



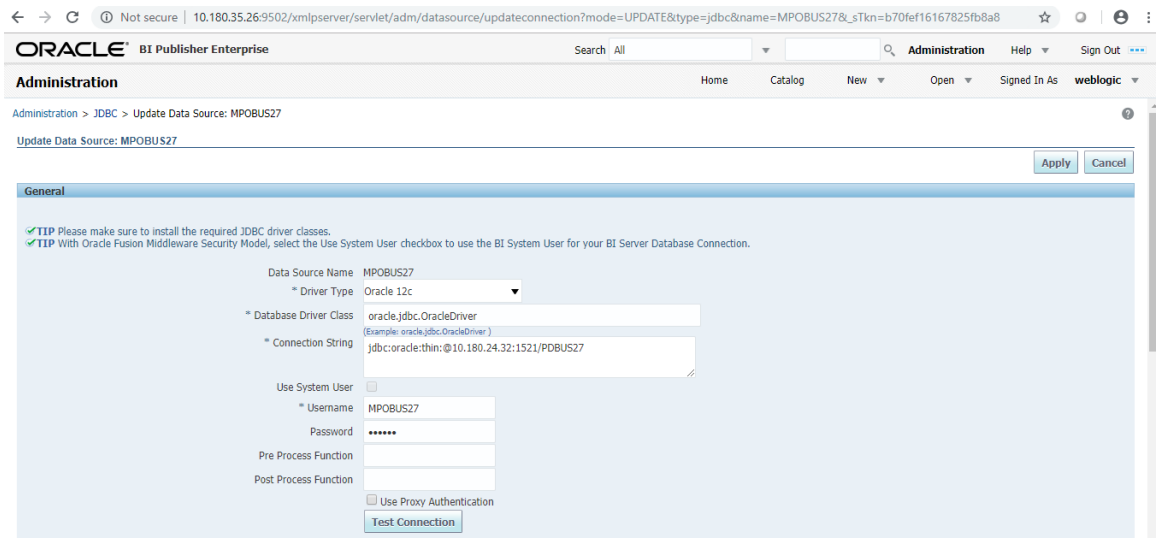
6. Fill up the following fields:

Table 8–1 Data Source Details

Field Name	Description
Data Source Name	Any name can be given here
Driver Type	Oracle 11g
Database Driver Class	oracle.jdbc.OracleDriver
Connection String	jdbc:oracle:thin:@<OBP_HOST_DB_IP>:<OBP_HOST_DB_PORT>:<OBP_HOST_DB_SERVICE_NAME>
Username	<BIP_DATASOURCE_NAME>
Password	<OBP_HOST_DB_PASSWORD>

7. Click **Ok**.

Figure 8–5 BIP Data Source Created



9 ODI Configuration

This chapter details steps involved in the configuration of ODI. Before configuring ODI, you need to install the required ODI version mentioned in Section 1.1.2.1 Certification Details.

You can configure ODI using odi.tar.gz. ODI configuration zip is present inside the ob-utils zip/Insights.zip.

9.1 Configuration Procedure

Following are the steps required for ODI configuration using ob-utils zip/Insights.zip:

1. Create master and work repository using RCU. At the end of RCU run, master and work repository is created in one schema.
2. Create a staging area to copy all the scenarios from ob-utils.zip\Insights.zip\odi.tar.gz\odi.tar.
3. Set ODI Level Configurations as mentioned in Section 1 Analytics Configuration.
4. Create data source for master and work repository with schema and DB details based on step 1.
    - odiMasterRepository for Master Repository having JNDI name: jdbc/odiMasterRepository.
    - odiWorkRepository for Work Repository having JNDI name: jdbc/odiWorkRepository.
5. Create three more data sources in the ODI domain.
    - odiOCSA for CSA DB having JNDI name: jdbc/odiOracleCsa
    - odIUploadOBP for OBP DB having JNDI name: jdbc/odIUploadOBP
    - odiOBP for source DB having JNDI name: jdbc/odiOBP
6. Deploy agent from staging area in ODI domain.
7. Create one data source to access reporting db (jdbc/FCBDataSourceODI) with the name OBP_HOST_ODI_XA in host domain where batch will run.
8. Make the entry for WSDL_URL in odi.properties file in host domain where batch will run.

    Example: WSDL_URL =

    http: //<ODIDOMAINSERVER>:8080/oracle12diagent/OdiInvoke?WSDL

10 Monitoring Servers Using Oracle Enterprise Manager

This chapter lists the steps required to monitor servers using Oracle Enterprise Manager (OEM).

The OBDLOCS servers can be monitored using Oracle Enterprise Manager. 'em_monitor.zip' is available inside 'ob-utils' for this purpose. The procedure is as follows:

1. Extract the 'ob-utils' to get 'em_monitor.zip'.
2. Extract 'em_monitor.zip'. It contains 'obp_em_view_script' folder.

   For monitoring the OBDLOCS Servers, follow the procedures given in Oracle Banking Deposits and Lines of Credit Servicing Management Pack Setup Guide.

11 Post Installation Verification

This chapter lists the steps required to verify the Oracle Banking Deposits and Lines of Credit Servicing solution installation.

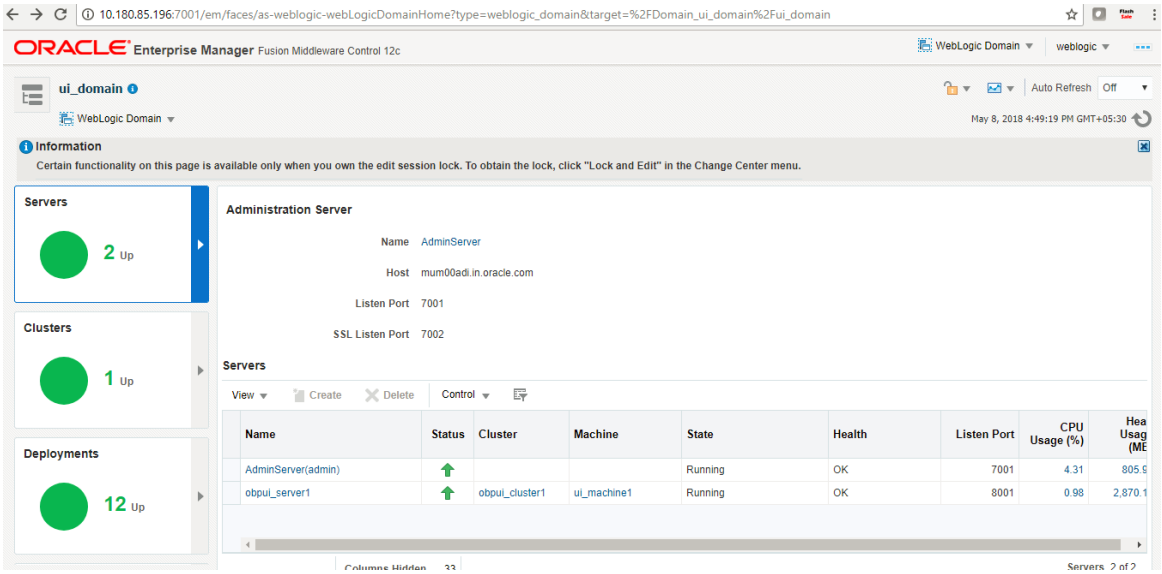
11.1 UI Domain Verification

To verify the UI domain installation:

1. Start the UI domain Admin and Managed servers.
2. In the WebLogic console (<UI_IP>:<UI_ADMIN_PORT>/console), navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following OBDLOCS libraries and applications is *Active*.
    - Shared Libraries
        - ob.app.client.coll
        - ob.app.client.communications
        - ob.app.client.cz
        - ob.app.client.deposit
        - ob.app.client.fw
        - ob.app.client.indirectlending
        - ob.app.client.lcm
        - ob.app.client.lending
        - ob.app.client.or
        - ob.app.client.party
        - ob.app.client.pm
        - ob.app.client.pricing
        - ob.app.client.sh
        - ob.ui.coll
        - ob.ui.communications
        - ob.ui.cz
        - ob.ui.deposit
        - ob.ui.fusion
        - ob.ui.lcm
        - ob.ui.indirectlending
        - ob.ui.lending
        - ob.ui.or

        - ob.ui.party
        - ob.ui.pm
        - ob.ui.pricing
        - ob.ui.sh
        - ob.ui.tp
        - ob.ui.tp.cz
    - Ears
        - com.ofss.fc.app.monitoring
        - com.ofss.fc.app.ui.connector
        - com.ofss.fc.ui.view.obcm
        - com.ofss.fc.ui.view
        - com.ofss.fc.ui.view.admin
        - com.ofss.fc.ui.view.admin.dashboard
        - com.ofss.fc.ui.view.developer
        - com.ofss.fc.ui.view.mds
        - com.ofss.fc.ui.view.obecasa
        - com.ofss.fc.ui.view.obepm
        - com.ofss.fc.ui.view.qa
4. In EM console (<UI_IP>:<UI_ADMIN_PORT>/em), check the status of:
    - Cluster
    - Managed Servers
    - Applications

Figure 11–1 UI EM Console Status Check

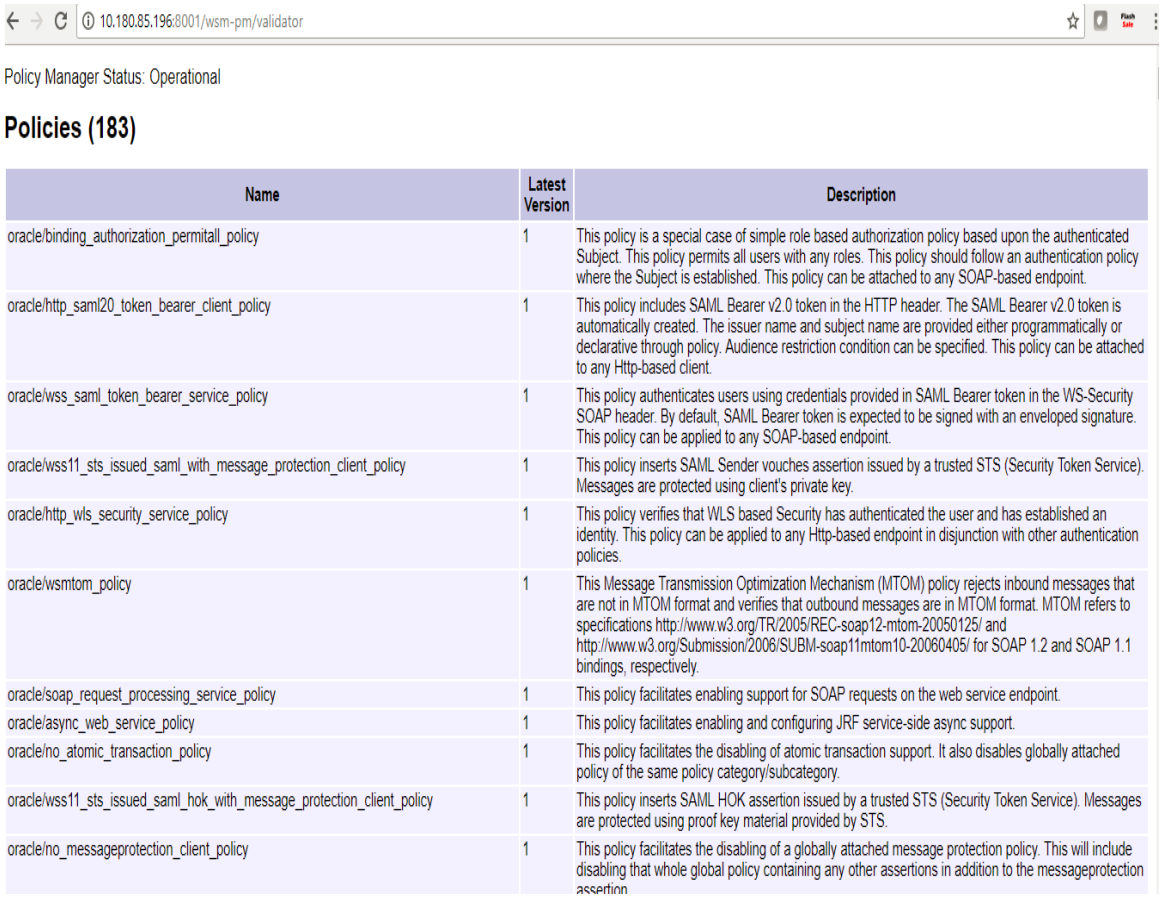


5. In (<UI_IP>:<UI_ADMIN_PORT>/wsm-pm/validator) and (<UI_IP>:<UI_MANAGED_PORT>/ wsm-pm/validator) screens, all policies must appear.

Figure 11–2 UI Admin wsm-pm Validator

		configuration. A SAML token, included in the SOAP message, is used in SAML-based authentication with sender vouches confirmation. These credentials are provided either programmatically or through the security configuration. This policy performs dynamic identity switching by propagating a different identity than the one based on authenticated Subject. This policy can be attached to any SOAP-based client.
oracle/wss_saml20_token_over_ssl_service_policy	1	This policy authenticates users using credentials provided in SAML V2.0 token in the WS-Security SOAP header. The credentials in the SAML V2.0 token are authenticated against a SAML V2.0 login module. The policy verifies that the transport protocol provides SSL message protection. This policy can be applied to any SOAP-based endpoint.
oracle/wss11_username_token_with_message_protection_wssc_client_policy	1	This policy provides message-level protection and authentication for outbound SOAP requests in accordance with the WS-Security 1.1 standard. Messages are protected using WS-Security's Basic 128 suite of symmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption. The keystore on the client side is configured either on a per-request basis or through the security configuration. Credentials are included in the WS-Security UsernameToken header of outbound SOAP request messages. Only plain text mechanism is supported. Credentials are provided either programmatically through the current Java Authentication and Authorization Service (JAAS) subject or by a reference in the policy to the configured credential store. This policy has secure conversation enabled. This policy can be attached to any SOAP-based client.
oracle/wss11_x509_token_with_message_protection_wssc_client_policy	1	This policy provides message-level protection and certificate-based authentication for outbound SOAP requests in accordance with the WS-Security 1.1 standard. Messages are protected using WS-Security's Basic 128 suite of symmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption. The keystore on the client side is configured either on a per-request basis or through the security configuration. Credentials are included in the WS-Security binary security token of the SOAP message. These credentials are provider either programmatically or through the security configuration. This policy has secure conversation enabled.
oracle/wss_saml_token_over_ssl_service_policy	1	This policy authenticates users using credentials provided in SAML tokens in the WS-Security SOAP header. The credentials in the SAML token are authenticated against a SAML login module. The policy verifies that the transport protocol provides SSL message protection. This policy can be applied to any SOAP-based endpoint.
oracle/wss11_saml_or_username_token_with_message_protection_service_policy	1	This policy authenticates users using credentials provided in SAML token or Username token or SAML token with confirmation method 'Bearer' in the WS-Security SOAP header or using credentials in the HTTP header against the configured identity store. Messages are protected either over transport layer using HTTPS or message level protection using WS-Security 1.1 standard . Message level protection(integrity, confidentiality) is done using WS-Security's Basic 128 suite of symmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption.This policy can be attached to any SOAP based endpoint or any HTTP based endpoint

Figure 11–3 UI managed wsm-pm validator



11.2 Host Domain Verification

To verify the Host domain installation:

1. Start the Host domain Admin and Managed servers.
2. Navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following Oracle Banking Platform libraries and applications is *Active*. Following are the details of all XD components libraries and ears:

   batchhost Server deployments

   - Shared libraries
     - ob.app.client.coll
     - ob.app.client.communications
     - ob.app.client.cz
     - ob.app.client.deposit
     - ob.app.client.fw

- ob.app.client.indirectlending
- ob.app.client.lcm
- ob.app.client.lending
- ob.app.client.or
- ob.app.client.party
- ob.app.client.pm
- ob.app.client.pricing
- ob.app.client.sh
- ob.app.host.communications
- ob.app.host.cz
- ob.app.host.fw
- ob.app.host.lcm
- ob.app.host.deposits
- ob.app.host.party
- ob.app.host.pm
- ob.app.host.pricing
- ob.app.host.sh
- ob.app.host.tp
- ob.app.host.tp.cz
- ob.app.integration

- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging
  - com.ofss.fc.middleware
  - com.ofss.fc.module.rest.ops
  - com.ofss.fc.reports.communications
  - com.ofss.fc.webservices

OBPR Server deployments

- Shared libraries
  - ob.app.client.coll
  - ob.app.client.communications
  - ob.app.client.cz

- ob.app.client.deposit
- ob.app.client.fw
- ob.app.client.lcm
- ob.app.client.lending
- ob.app.client.or
- ob.app.client.party
- ob.app.client.pm
- ob.app.client.pricing
- ob.app.client.sh
- ob.app.host.cz
- ob.app.host.fw
- ob.app.host.pricing
- ob.app.host.tp
- ob.app.host.tp.cz

- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging.pricing
  - com.ofss.fc.middleware.pricing
  - com.ofss.fc.webservices.pricing

OBEPM Server deployments

- Shared libraries
  - ob.app.client.communications
  - ob.app.client.cz
  - ob.app.client.fw
  - ob.app.client.lcm
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.sh
  - ob.app.host.communications
  - ob.app.host.cz
  - ob.app.host.fw

- ob.app.host.pm
- ob.app.host.sh
- ob.app.host.tp
- ob.app.host.tp.cz

- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging.pm
  - com.ofss.fc.middleware.pm
  - com.ofss.fc.webservices.pm

OBDLOCS Server deployments

- Shared libraries
  - ob.app.client.coll
  - ob.app.client.communications
  - ob.app.client.cz
  - ob.app.client.deposit
  - ob.app.client.fw
  - ob.app.client.lcm
  - ob.app.client.lending
  - ob.app.client.or
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.indirectlending
  - ob.app.client.sh
  - ob.app.host.indirectlending
  - ob.app.host.cz
  - ob.app.host.fw
  - ob.app.host.deposits
  - ob.app.host.sh
  - ob.app.host.tp
  - ob.app.host.tp.cz
  - ob.app.integration

- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging.deposits
  - com.ofss.fc.middleware.deposits
  - com.ofss.fc.webservices.deposits

OBPM Server deployments

- Shared libraries
  - ob.app.client.coll
  - ob.app.client.communications
  - ob.app.client.cz
  - ob.app.client.deposit
  - ob.app.client.fw
  - ob.app.client.indirectlending
  - ob.app.client.lcm
  - ob.app.client.lending
  - ob.app.client.or
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.sh
  - ob.app.host.cz
  - ob.app.host.fw
  - ob.app.host.party
  - ob.app.host.sh
  - ob.app.host.tp
  - ob.app.host.tp.cz
  - ob.app.integration
- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging.party

- com.ofss.fc.middleware.party
- com.ofss.fc.webservices.party

OBCCM Server deployments

- Shared libraries
  - ob.app.client.coll
  - ob.app.client.communications
  - ob.app.client.cz
  - ob.app.client.deposit
  - ob.app.client.fw
  - ob.app.client.lcm
  - ob.app.client.indirectlending
  - ob.app.client.lending
  - ob.app.client.or
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.sh
  - ob.app.host.coll
  - ob.app.host.communications
  - ob.app.host.cz
  - ob.app.host.fw
  - ob.app.host.lcm
  - ob.app.host.sh
  - ob.app.host.tp
  - ob.app.host.tp.cz
- Ears
  - com.ofss.fc.app.connector
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.messaging.lcm
  - com.ofss.fc.middleware.lcm
  - com.ofss.fc.webservices.lcm

JMS Modules

JMS Modules for all XD host servers.

JMS Modules (Filtered - More Columns Exist)

Click the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

New | Delete — Showing 1 to 17 of 17 Previous | Next

Name	Type
jmsAccountingModule	JMSSystemResource
jmsAnalyticsModule	JMSSystemResource
jmsAsyncAuditModule	JMSSystemResource
jmsBatchModule	JMSSystemResource
jmsCasaModule	JMSSystemResource
jmsCollateralModule	JMSSystemResource
jmsCollectionModule	JMSSystemResource
jmsDocumentOutboundModule	JMSSystemResource
jmsDomainPublishModule	JMSSystemResource
jmsODIModule	JMSSystemResource
jmsOriginationModule	JMSSystemResource
jmsPartyModule	JMSSystemResource
jmsPaymentModule	JMSSystemResource
jmsPricingAnalysisModule	JMSSystemResource
jmsReportModule	JMSSystemResource
jmsRuleModule	JMSSystemResource
jmsWorkflowModule	JMSSystemResource

New | Delete — Showing 1 to 17 of 17 Previous | Next

4. In (<HOST_IP>:<HOST_ADMIN_PORT>/wsm-pm/validator) and (<HOST_IP>:<HOST_MANAGED_PORT>/ wsm-pm/validator) screens, all policies must appear.

Figure 11–4 HOST admin wsm-pm validator

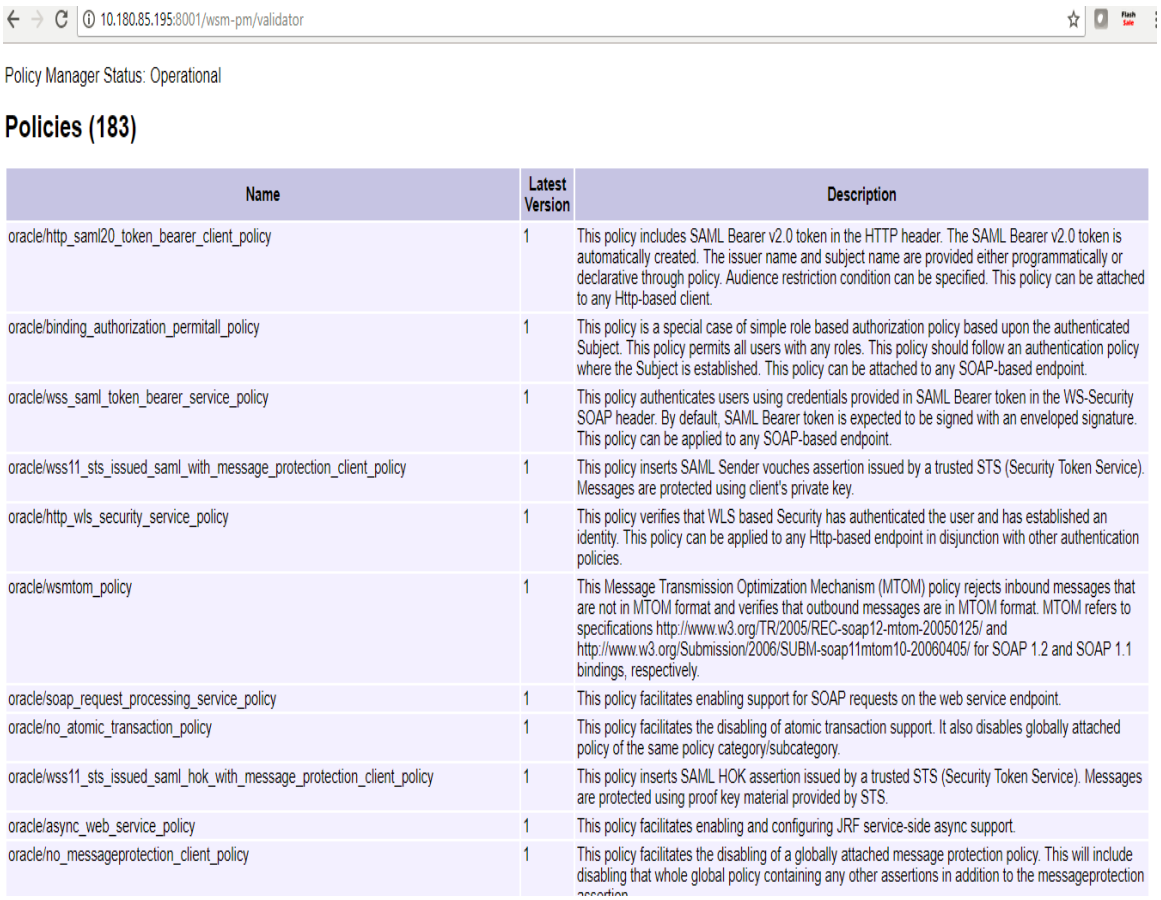
10.180.85.195:7001/wsm-pm/validator

Policy Manager Status: Operational

Policies (183)

Name	Latest Version	Description
oracle/http_saml20_token_bearer_client_policy	1	This policy includes SAML Bearer v2.0 token in the HTTP header. The SAML Bearer v2.0 token is automatically created. The issuer name and subject name are provided either programmatically or declarative through policy. Audience restriction condition can be specified. This policy can be attached to any Http-based client.
oracle/binding_authorization_permitall_policy	1	This policy is a special case of simple role based authorization policy based upon the authenticated Subject. This policy permits all users with any roles. This policy should follow an authentication policy where the Subject is established. This policy can be attached to any SOAP-based endpoint.
oracle/wss_saml_token_bearer_service_policy	1	This policy authenticates users using credentials provided in SAML Bearer token in the WS-Security SOAP header. By default, SAML Bearer token is expected to be signed with an enveloped signature. This policy can be applied to any SOAP-based endpoint.
oracle/wss11_sts_issued_saml_with_message_protection_client_policy	1	This policy inserts SAML Sender vouches assertion issued by a trusted STS (Security Token Service). Messages are protected using client's private key.
oracle/http_wls_security_service_policy	1	This policy verifies that WLS based Security has authenticated the user and has established an identity. This policy can be applied to any Http-based endpoint in disjunction with other authentication policies.
oracle/wsmtom_policy	1	This Message Transmission Optimization Mechanism (MTOM) policy rejects inbound messages that are not in MTOM format and verifies that outbound messages are in MTOM format. MTOM refers to specifications http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/ and http://www.w3.org/Submission/2006/SUBM-soap11mtom10-20060405/ for SOAP 1.2 and SOAP 1.1 bindings, respectively.
oracle/soap_request_processing_service_policy	1	This policy facilitates enabling support for SOAP requests on the web service endpoint.
oracle/no_atomic_transaction_policy	1	This policy facilitates the disabling of atomic transaction support. It also disables globally attached policy of the same policy category/subcategory.
oracle/wss11_sts_issued_saml_hok_with_message_protection_client_policy	1	This policy inserts SAML HOK assertion issued by a trusted STS (Security Token Service). Messages are protected using proof key material provided by STS.
oracle/async_web_service_policy	1	This policy facilitates enabling and configuring JRF service-side async support.
oracle/no_messageprotection_client_policy	1	This policy facilitates the disabling of a globally attached message protection policy. This will include disabling that whole global policy containing any other assertions in addition to the messageprotection

Figure 11–5 HOST managed wsm-pm validator



Additionally, the installer can verify the following:

- **JMS Resources and Security Credentials**
  - Verify the creation of JMS resources Using admin console.
  - Verify security credential mappings for resource adapter under obphost.
- **OID Integration**
  - Verify that the users and groups are created under **Security -->Myrealms --> Users And Groups**. This is one of the indicators of successful OID integration.
- **SMS Policy Seeding**
  - Verify from logs under ${HOST_FWM}/obpoidinstall/PolicyStoreSetup/logs to ensure policy seeding was complete.
  - EM and OWSM should also be verified in host as in UI.

11.3 SOA Domain Verification

To verify the SOA domain installation:

1. Start the SOA domain Admin and Managed servers (SOA and human task).
2. Navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following Oracle Banking Platform libraries and human task files with .ear extension is *Active*.
    - Shared Libraries
        - ob.app.client.coll
        - ob.app.client.communications
        - ob.app.client.cz
        - ob.app.client.deposit
        - ob.app.client.fw
        - ob.app.client.lcm
        - ob.app.client.lending
        - ob.app.client.or
        - ob.app.client.party
        - ob.app.client.pm
        - ob.app.client.pricing
        - ob.app.client.sh
        - ob.ui.coll
        - ob.ui.communications
        - ob.ui.cz
        - ob.ui.deposit
        - ob.ui.fusion
        - ob.ui.lcm
        - ob.ui.lending
        - ob.ui.or
        - ob.ui.party
        - ob.ui.pm
        - ob.ui.pricing
        - ob.ui.sh
        - ob.ui.tp
        - ob.ui.tp.cz
    - Ears
        - com.ofss.fc.app.ui.connector
        - com.ofss.fc.ui.view.mds

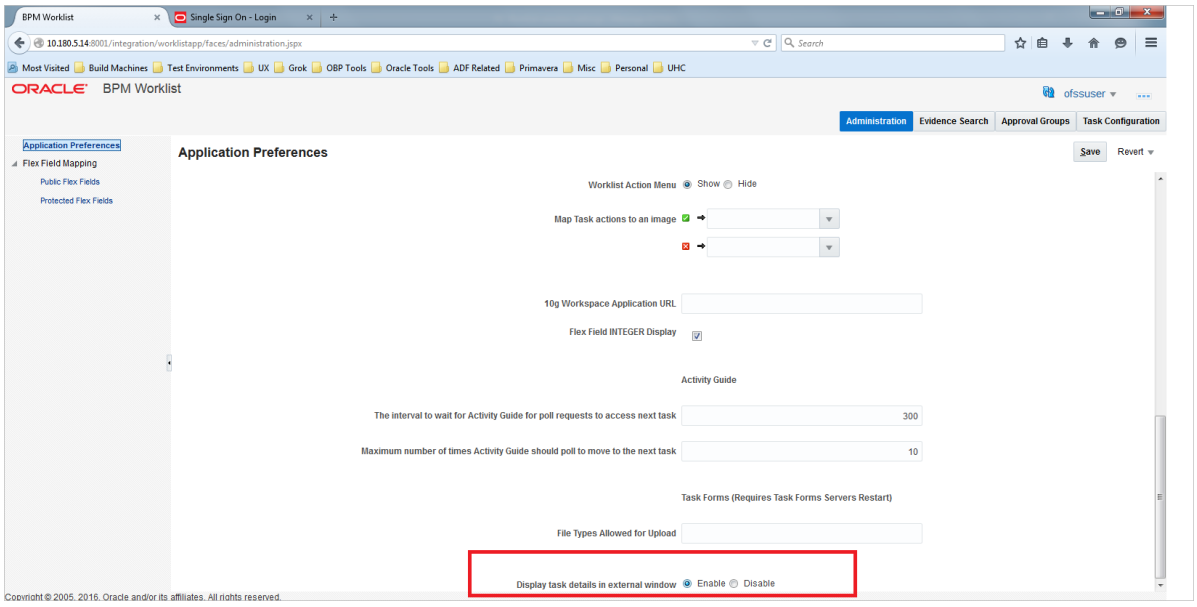
- com.ofss.fc.workflow.ui.batchexceptionrecovery
- com.ofss.fc.workflow.ui.brop
- com.ofss.fc.workflow.ui.CapturePartyFinancialsHumanTask
- com.ofss.fc.workflow.ui.common.approval
- com.ofss.fc.workflow.ui.FeeNegotiationApprovalTask
- com.ofss.fc.workflow.ui.hardshiprelief
- com.ofss.fc.workflow.ui.lcm.PerformManualAllocationUITask
- com.ofss.fc.workflow.ui.lcm.valuation
- com.ofss.fc.workflow.ui.dda
- com.ofss.fc.workflow.ui.PartyMerge

4. Also verify that the standard SOA application soa-infra is in *Active* state.

11.4 BPM Worklist Window Setting

For BPM Worklist window setting, the option **Display task details in external window** must be set to enable mode. This option is present in administration mode of BPM Worklist as shown in Figure 11–6.

Figure 11–6 BPM Worklist Window Settings



12 Errors and Remedies

This chapter provides information on troubleshooting to help diagnose and remedy some of the problems encountered during installation of the Oracle Banking Deposits and Lines of Credit Servicing.

12.1 OBDLOCS Domain Installation

In general, any environmental condition such as a network error that may lead to a halt in the installation is evident to you on the console itself. You can additionally inspect WLST logs created in logs directory under middleware for any anomalies.

While creating OBDLOCS SOA domain, ignore the following error:

Error: No domain or domain template has been read.

Error: No domain or domain template has been read.

Figure 12–1 SOA Domain Error

The domain is created successfully. Also note that for recreation of SOA, Host, and UI domain, a new set of RCUs is required, otherwise the pre-installation of respective component fails.

12.2 OBDLOCS Security Policy Seeding

For monitoring Oracle Banking Deposits and Lines of Credit Servicing application security policy seeding, you can check the logs generated in $HOST_FMW/obpoidinstall/PolicyStoreSetup/logs.

12.3 OBDLOCS Domain Post Installation

This section lists various log files that assist in troubleshooting domain post installation as follows:

obp-* logs

During post installation in order to monitor errors, if any, you can check the obp-* logs created in the OBDLOCS WebLogic domain. These logs contain adequate tracing information required to understand the current execution point of the script. This facilitates to determine the various configurations that were executed and those that need due action.

WebLogic Admin Server Logs and stderr file

The script does domain level configurations that require several automated reboots of admin server, which can be monitored by checking the WebLogic admin server logs and stderr file created under obp-domain-dir/servers/AdminServer/stderr.log.

For instance, consider a scenario of OBDLOCS Host installation in which once the post install script for OBDLOCS host has secured itself against a LDAP (OID/OVD) it proceeds to restart the OBDLOCS Host domain admin server to produce these changes. During this if due to a momentary network failure the host machine is unable to make a connection to LDAP then the admin server would fail to start. This will result in the post install script to abruptly abort throwing a subsequent script error (again which might not conclusive enough to point out the root cause). The 'obp-*' logs created in the OBDLOCS Host domain would indicate an incomplete attempt by post install script to start the admin server.

You can check the admin server logs (to find why the admin server could not start) which will ultimately yield out the actual reasons (in this case the reason being host machine was unable to connect to LDAP).

stderr log, WebLogic Domain Managed Server logs, OFSS logs

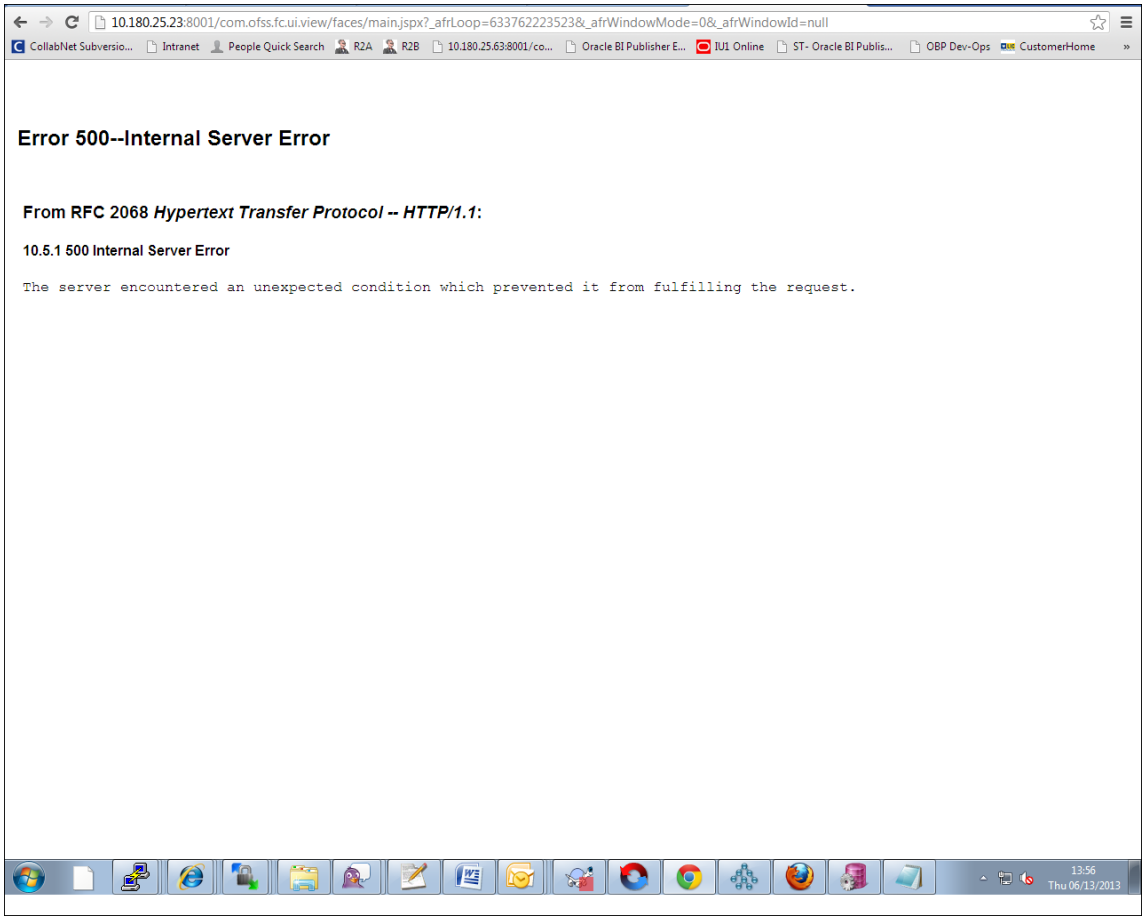
Once the post install script is completed successfully, you can start the domain servers and enter a dummy transaction to check the system correctness. If you face an error you can inspect the stderr log, the WebLogic domain managed server logs as well as the ofss logs under domain directory.

When you start the managed servers post installation, there may occur a lot of error printing in startup logs that you can ignore. However, ensure that the status of the applications deployed on the components is active and the server is in running mode. Even if there are errors during startup of the managed server, you can login to the application successfully.

12.4 Error on First Log in

In the first log in after installation, the following page may appear or blank page may appear:

Figure 12–2 Error on First Log In



In this case, remove the part of the url after '/main.jspx', and then hit the rest of the url (Example: https://10.180.25.23:8001/com.ofss.fc.ui.view/faces/main.jspx) again.

12.5 Log in Issues

If there is a problem during logging in the main page, you can check whether the home branch and business unit of the user in OID are the same with the Host DB table. Use the following query to verify it in database:

```
select * from flx_cs_branches_b;
select * from flx_me_business_unit_b;
```

If there is mismatch between the database and OID, make change in OID to match with the database.

12.6 SOA Setup in Cluster

This section explains the error that can be encountered in SOA setup in Cluster, and its resolution.

12.6.1 "COMPONENTTYPE": invalid identifier error

Due to one of the one-off patches for SOA applied during the OBDLOCS installation, in SOA cluster environment, the following error might be seen in SOA server logs.

```
Internal Exception: java.sql.SQLSyntaxErrorException: ORA-00904:
```

```
"COMPONENTTYPE": invalid identifier
```

Though this is not a fatal kind of exception, it can be resolved by adding one more column **componenttype** of size **10** with **char** type in **soainfra** schema for table **cluster_master**.

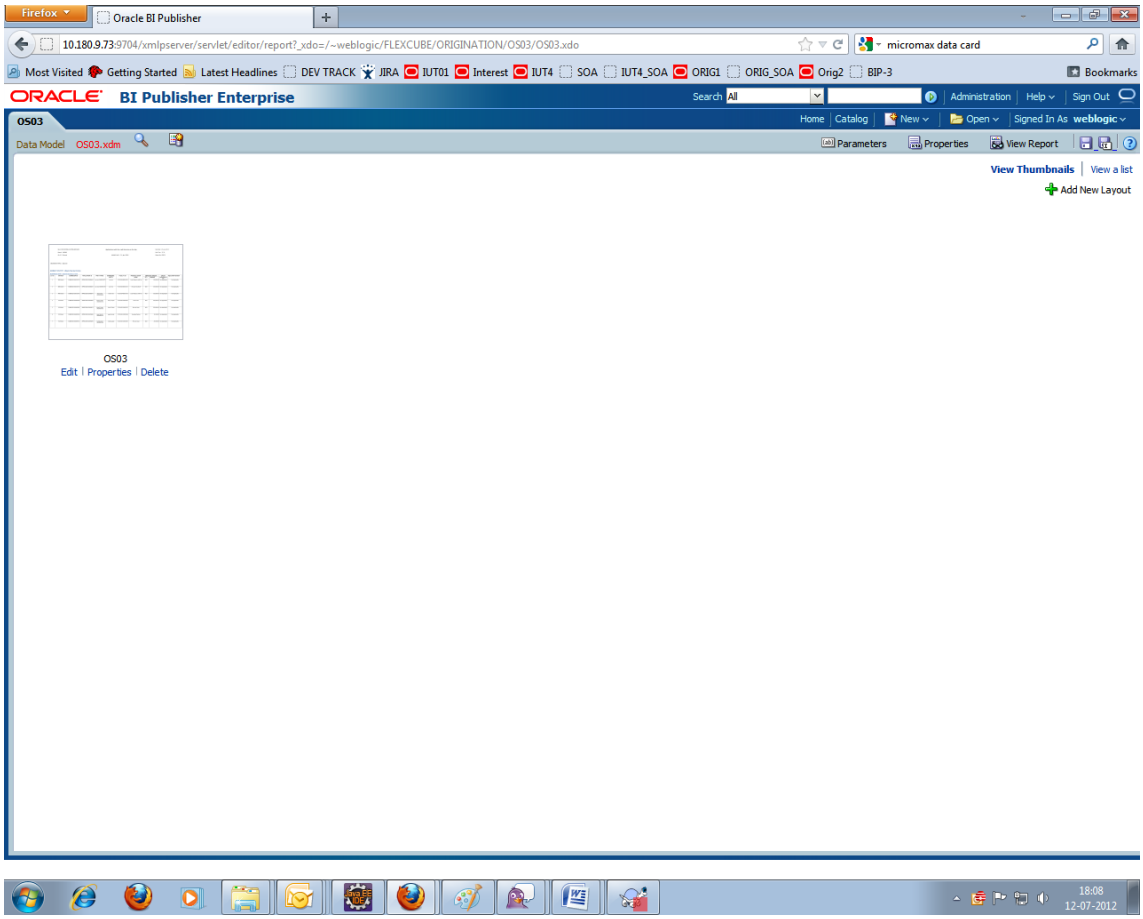
For example on Oracle database user needs to run the following command on soainfra schema:

```
alter table cluster_master add (componenttype varchar2(10));
```

12.7 BIP Report Data Model Linkage Problem after Host Post Installation Step

After editing a report, click the magnifying glass icon to select the data model associated with this report. (Here OS03.xdm in red indicates that the data model is not properly connected with the report or that the report is not able to find the model at the location that it is referring)

Figure 12–3 Selecting the Data model



Note

The above step is to be carried out in case the data model of a report has not correctly linked with a report, after reports are deployed in BIP server in Host Post Installation step.

12.8 BPM Worklist Task Issue

If the BPM Task (human task) is not working after installation and you get a backend error indicating access denied, then:

1. Add the following parameters in setStartupEnv.sh for obphumantask_server1.

   -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImp

   l -Djavax.xml.transform.TransformerFactory=com.sun.org.apache.xalan.internal.xsltc.trax.TransformerFactoryImpl

   -Djavax.xml.parsers.SAXParserFactory=com.sun.org.apache.xerces.internal.jaxp.SAXParserFactoryImpl

   And jps-config.xml

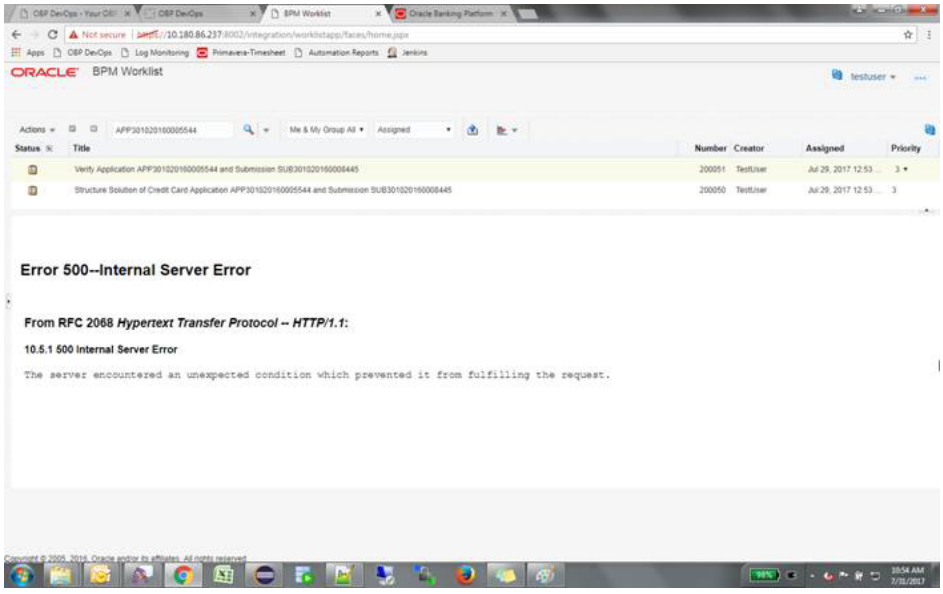
   <property name="trust.keystoreType" value="KSS"/>

   <property name="trust.keyStoreName" value="kss://opss/trustservice_ks"/>

   <property name="trust.trustStoreName" value="kss://opss/trustservice_ts"/>

2. Restart it.

Figure 12–4 BPM Worklist Task issue



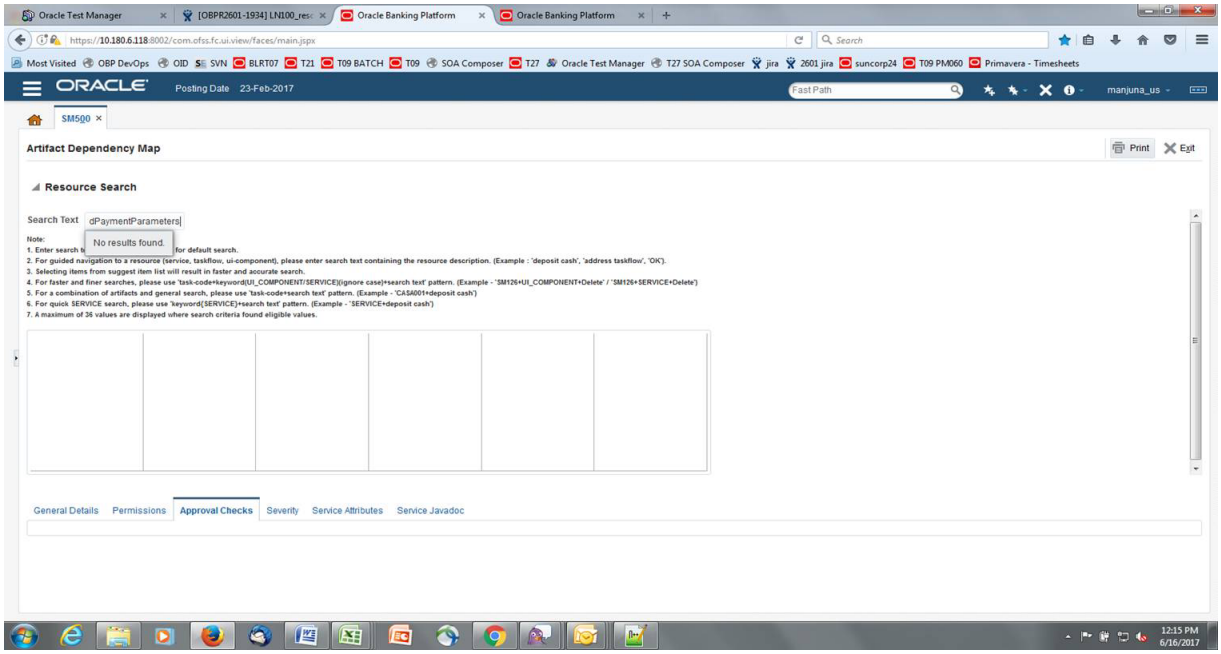
12.9 Artifacts Issue for SM500 page

If artifacts are not available for SM500, execute the load-artifacts.sh script present at the host installable path.

For example,

sh /scratch/install/ load-artifacts.sh

Figure 12–5 Artifacts Issue for SM500 page



12.10 ra/FCRJConnectorSOA connector issue

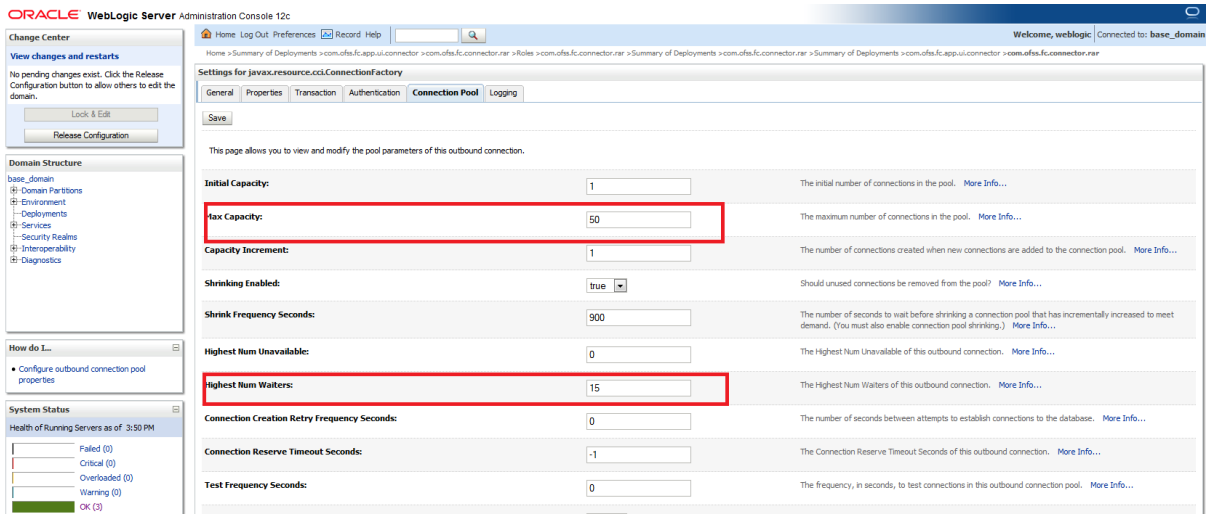
If below mentioned error is faced on Humantask server, configuration shown in the below figure has to be done to resolve issue.

Caused By: javax.resource.spi.ApplicationServerInternalException: Unable to get a connection for pool = "ra/FCRJConnectorSOA", weblogic.common.resourcepool.ResourceUnavailableException: No resources currently available in pool ra/FCRJConnectorSOA to allocate to applications. Either specify a time period to wait for resources to become available, or increase the size of the pool and retry.

at weblogic.connector.outbound.ConnectionManagerImpl.getConnectionInfo (ConnectionManagerImpl.java:458)

Set the Max Capacity size to 50 and Highest Num Waiters to 15 as shown in the below figure and redeploy the connector on Humantask server.

Figure 12–6 Settings for javax.resource.cci.ConnectionFactory page



12.11 Humantask Startup Issue

If Humantask server is not coming up in running mode after installation and if you face below mentioned error,

<Nov 21, 2017, 7:40:52,638 PM GMT+05:30> <Error> <Socket> <BEA-000403> <IOException occurred on socket: Socket[addr=/10.180.35.5,port=57761,localport=7001]

weblogic.socket.MaxMessageSizeExceededException: Incoming message of size: '10000080' bytes exceeds the configured maximum of: '10000000' bytes for protocol: 't3'.

weblogic.socket.MaxMessageSizeExceededException: Incoming message of size: '10000080' bytes exceeds the configured maximum of: '10000000' bytes for protocol: 't3'

at weblogic.socket.BaseAbstractMuxableSocket.incrementBufferOffset (BaseAbstractMuxableSocket.java:212)

at weblogic.socket.BaseAbstractMuxableSocket.incrementBufferOffset (BaseAbstractMuxableSocket.java:188)

at weblogic.rjvm.t3.MuxableSocketT3.incrementBufferOffset(MuxableSocketT3.java:675)

at weblogic.socket.SocketMuxer.readFromSocket(SocketMuxer.java:1004)

at weblogic.socket.NIOSocketMuxer.readFromSocket(NIOSocketMuxer.java:771)

Truncated. see log file for complete stacktrace

>

Update the setDomainEnv.sh configuration file by setting MaxMessageSize for server as,

EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Dweblogic.MaxMessageSize=50000000"

export EXTRA_JAVA_PROPERTIES

12.12 Collection Mocking

By default collection is enabled in enterprise application. For mocking collection, perform the following steps:

1. Execute the following SQL queries in application database:

   ```
   update flx_fw_config_all_b set prop_value='false' where prop_
   id='collection.bootstrap' and category_id='root';
   ```

   ```
   update flx_fw_config_all_b set prop_value='false' where prop_
   id='collection.webservice.bootstrap' and category_id='root';
   ```

2. Update the setDomainEnv.sh configuration file on HOST server with the following parameters:

   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -
   DAdapterFactories:INS_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:PARTY_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:LN_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:LCM_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:ACCOUNT_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:DDA_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:AC_COLLECTION_ADAPTER_MOCKED=true -
   DAdapterFactories:CS_COLLECTION_ADAPTER_MOCKED=true"
   export EXTRA_JAVA_PROPERTIES

3. Restart the HOST managed server.

12.13 DDA, Party and LOAN Mocking for OBDLOCS installer

For DDA, Party and LOAN Mocking, perform the following steps:

1. Update the setDomainEnv.sh configuration file on HOST server with the following parameters:

   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -
   DAdapterFactories:ACCOUNT_DDA_MOCKED=true -
   DAdapterFactories:ACCOUNT_LOAN_MOCKED=true -
   DAdapterFactories:PARTY_ENTITLEMENT_ADPT_MOCKED=true "
   export EXTRA_JAVA_PROPERTIES

2. Restart the HOST managed server.

13 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Deposits and Lines of Credit Servicing.

13.1 Manual Uninstall

Currently an installed OBDLOCS WebLogic domain can be uninstalled manually by removing following directories:

- Manually delete WebLogic domain (Middleware_Home/user_projects/domains) created from obpinstall template.
- Clean up middleware directory for any files or folders containing obp in their names (simply run rm –rf *obp* under middleware directory).
- For uninstalling any of the Oracle Banking Deposits and Lines of Credit Servicing related database schemas run the RCU utility and choose the **Drop** option.