Oracle® Banking Enterprise Default Management

US Localization Installation Guide - Silent Installation

Release 2.11.0.0.0

F36758-01

December 2020

ORACLE®

Oracle Banking Enterprise Default Management US Localization Installation Guide - Silent Installation, Release 2.11.0.0.0

F36758-01

Contents

List of Figures

List of Tables

Preface

The Oracle Banking Enterprise Default Management US Localization Installation Guide - Silent Installation contains information on silent installation and configuration of Oracle Banking Enterprise Default Management 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 Enterprise Default Management 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 and Oracle OID.

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 Enterprise Default Management and the installation guide. It also mentions the assumptions, limitations and exclusions that this document has been based upon.

Chapter 2 Pre-Installation Configuration

This chapter describes the pre-configuration activities that are to be completed successfully for proper installation and functioning of Oracle Banking Enterprise Default Management.

Chapter 3 OBEDM US Localization Host Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Enterprise Default Management US Localization Host Media Pack.

Chapter 4 OBEDM US Localization Presentation Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Enterprise Default Management Presentation (UI) Media Pack.

Chapter 5 Standalone Database Setup

This chapter explains the steps involved in Oracle Banking Enterprise Default Management database which are primarily concerned with importing an existing database dump of the QA database.

Chapter 6 OBEDM and IPM Integration

This chapter explains the steps involved in the integration of Oracle Banking Enterprise Default Management and Oracle Imaging and Process Management (IPM).

Chapter 7 Monitoring Servers Using Oracle Enterprise Manager

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

Chapter 8 Post Installation Verification

This chapter explains the steps required to verify the installation of Oracle Banking Enterprise Default Management.

Chapter 9 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 Enterprise Default Management.

Chapter 10 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Enterprise Default Management.

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 Enterprise Default Management and Oracle Documaker, see the installation and configuration guides a t 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 Enterprise Default Management Security Guide.
- For the complete list of licensed products and the third-party licenses included with the license, see the Oracle Banking Enterprise Default Management Licensing Guide.
- For information related to setting up a bank or a branch, and other operational and administrative functions, see the Oracle Banking Enterprise Default Management Administrator Guide.
- For information related to customization and extension, see the Oracle Banking Enterprise Default Management Extensibility Guides for HOST and UI.
- For information on the functionality and features, see the respective Oracle Banking Enterprise Default Management Functional Overview document.
- For recommendations of secure usage of extensible components, see the Oracle Banking Enterprise Default Management 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
DB or db	Oracle Database
HOST	Middleware Host Tier
IPM	Imaging and Process Management
OBEDM	Oracle Banking Enterprise Default Management
OEL	Oracle Enterprise Linux
OEM	Oracle Enterprise Manager
OID	Oracle Internet Directory
OIM	Oracle Identity Manager
RCU	Repository Creation Utility
sh	Unix Shell file
SVN	Source Code Version Repository
UI	User Interface, that is Presentation Tier
WLS	WebLogic Server

1 Getting Started

This chapter presents an overview of Oracle Banking Enterprise Default Management and the installation guide. It also mentions the assumptions, limitations and exclusions that this document has been based upon.

1.1 About Oracle Banking Enterprise Default Management

Oracle Banking Enterprise Default Management (OBEDM) is a web-based innovative solution designed to assist financial institutions with managing the repayment of their consumer lending portfolios. The solution enables financial institutions in identification of delinquent accounts, accurate tracking and monitoring of delinquent accounts as well as charged-off accounts with high standards of efficiency. OBEDM consists of two modules - Collections and Recovery. The Collections solution covers the delinquent life cycle of consumer loans and overdraft accounts, starting from the identification of the symptoms of delinquency to actually tracking delinquency and impairment. It creates strategies in a befitting manner to achieve time and cost efficiency in collection activities. The Recovery solution covers the life cycle of a charged-off account and manages the account for tracking interest levied, expenses incurred, and payments received throughout the life cycle of charged-off account. This inherits all the capabilities of Collections solution.

1.2 About This Document

This document guides you through the installation of the Oracle Banking Enterprise Default Management along with US 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)
- 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 OBEDM 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 OBEDM 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 OBEDM 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 Configuration

This chapter describes the pre-configuration activities that are to be completed successfully for proper installation and functioning of Oracle Banking Enterprise Default Management.

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 Enterprise Default Management 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 Enterprise Default Management 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 7.5 64 bit	OBEDM Oracle Database
2	4	32	200	OEL 7.5 64 bit	OBEDM ADF UI Presentation Server
3	4	32	200	OEL 7.5 64 bit	OBEDM 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

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 Enterprise Default Management 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	OBEDM UI Presentation	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_231)

Sr. No.	Components	Zone	Software
			Oracle Linux 7.5 64-bit
2	OBEDM HOST	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Oracle Database 19c Enterprise Edition Release 19.8 Java Version jdk1.8.0_xx (jdk1.8.0_231) Oracle Linux 7.5 64-bit
3	OID	Security	Oracle Internet Directory 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_231) Oracle Linux 7.5 64-bit
4	IPM	Document	Oracle WebCenter - Content 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_231) Oracle Linux 7.5 64-bit
5	OIM	Security	Oracle Identity Manager 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_231) Oracle Linux 7.5 64-bit
6	OAM	Security	Oracle Access Manager 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_231) Oracle Linux 7.5 64-bit
7	OEM	Management	Oracle Enterprise Manager 13.2.0.0.0 As per certification matrix of Oracle Enterprise Manager 13.2.0.0.0
8	EM Agent Installation	Management	Push from OEM Console
9	OBEDM Database	Database	Oracle Database 19c Enterprise Edition Release 19.8 Oracle Linux 7.5 64-bit
10	HTTP Server	Web Server	Oracle HTTP Server 12.2.1.4.0

The following are some notes related to the software.

Table 2–3 Notes

Serial Number	Description
1	OBEDM release has been certified with OEL version 7.5 during the release cycle. It is strongly recommended to use the versions on which the release is certified.
2	The OBEDM installer will not abort the installation if this component is not present. It can be installed later.

Serial Number	Description
	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.
3	OIM_OUTBOUND_USERNAME and OIM_OUTBOUND_PASSWORD The OBEDM 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.
4	Oracle Access Manager can be installed later.
5	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.
6	It is mandatory for machine nodes on which OBEDM UI and Host Media pack installation is planned, to install the Java Cryptography Extensions Unlimited Strength Jurisdiction Policy Files, to enable additional encryption strengths.
7	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 below link: https://www.oracle.com/technetwork/java/javase/downloads/jce-all-download-5170447.html Copy "local_policy.jar" and "US_export_policy.jar" from inside this zip file in the path mentioned below. JAVA_HOME/jre/lib/security/
8	It is mandatory that the team installing OBEDM reads and understands the system requirements and specifications for the fusion middleware specified in the following link: https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-B648EA24-ABB4-42CA-B8F2-4B535D5EC8DB The url details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.4.0) products. Changes necessary at a system level for the fusion middleware should be made prior to executing OBEDM 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/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-F800C79F-A8CA-4A80-A4E9-97BC8E264889

2.2 Installation Checklist

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

https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-67E44706-637A-4695-9925-E48936C8F461

The link details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.4.0) products.

Changes necessary at a system level for the fusion middleware should be made prior to executing OBEDM 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.

2.2.1 Updating installobp***.properties

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

Table 2–4 Values for updating installobp.properties - For HOST***

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	OID_FARM_AND_POLICY_SEEDING_FLAG	Flag for policy seeding	Y	
4	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
5	SECURITY_ENABLED	Flag for security enable	Y	
6	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	
7	LOCAL_DISPLAY_VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
8	DOMAIN_NAME	Weblogic Domain name	host_domain or ui_domain	Can give any

Sr. No	Name	Description	Example Value	Value
				logical name
9	XD_COMPONENT_NAME	XD Component value	batchhost	This will be always batchhost
10	LOCALIZATION_TYPE	Type of localization	US	Depends on localization type
11	DOMAIN_DIRECTORY_LOCATION	Location where DOMAIN_NAME folder will be created	/scratch/app/product/fmw/user_projects/domains	
12	WEBLOGIC_USERNAME	Username for weblogic domain	weblogic	
13	WEBLOGIC_PASSWORD	Password for weblogic domain	weblogic1	
14	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.110 (Do not use localhost)	
15	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
16	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen port	7002	
17	MANAGED_SERVER_LISTEN_ADDRESS	Managed server listen address	10.180.84.110	
18	MANAGED_SERVER_LISTEN_PORT	Managed server listen port	8001	
19	MANAGED_SERVER_SSL_LISTEN_PORT	SSL listen port for managed server	8002	
20	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
21	OID_IP	I/P address of the OID server.	10.180.84.113	
22	OID_PORT	Port of the OID process instance.	3060	
23	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn= orcladmin	
24	OID_ADMIN_PWD	Refers to the	welcome1	

Sr. No	Name	Description	Example Value	Value
		password of admin user of the OID		
25	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
26	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	ou=obp,cn=Users,dc=in,dc=oracle,dc=com	
27	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	
28	HOST_CLUSTER_NAME	Refers to HOST cluster name	obphost_cluster1	Can give any logical name
29	HOST_SERVER_NAME	Refers to HOST server name	obphost_server1	Can give any logical name
30	HOST_JAVA_HOME	Refers to the home directory of java installation of the host machine. The version of java installed should be 1.8.0 or above. This is used to execute the OBP security policy seeding utility at the end of the installation.	/scratch/app/product/jdk1.8.0_231	
31	OUI_JAVA_HOME	Refers to the home directory of java installation. The version of java installed should be 1.8.101 . This is used for OBP patching.	/scratch/app/product/jdk1.8.0_231	

Sr. No	Name	Description	Example Value	Value
32	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
33	HOST_IP	I/P address of the server on which the OBP host or middleware layer should be installed.	10.180.84.110(Always use i/p , don't use localhost)	
34	HOST_TARGET	Refers to a location on the Host server where the installable can be transferred. The user id used for installation of OBP should have read, write and execute privileges on this directory.	/scratch/install/target	
35	HOST_MW_HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
36	UI_ADMIN_ SERVER_LISTEN_ ADDRESS	Listen address of UI Admin server	10.180.84.111	
37	UI_ADMIN_ SERVER_LISTEN_ PORT	Listen port of UI Admin server	7001	
38	UI_MANAGED_ SERVER_LISTEN_ ADDRESS	Listen address of UI managed server	10.180.84.111	
39	UI_MANAGED_ SERVER_LISTEN_ PORT	Listen port of UI managed server	8001	
40	UI_MANAGED_ SERVER_SSL_ LISTEN_PORT	Listen ssl port of UI managed server	8002	
41	UI_IP	I/P address of the server on which the OBP presentation or UI layer should be installed.	10.180.84.111	
42	UI_UNIX_USER	Linux login user id used to install the OBP UI solution.	ofssobp	

Sr. No	Name	Description	Example Value	Value
43	UI_DOMAIN_HOME	Refers to the domain name to be used for the weblogic domain of the OBP Presentation server	/scratch/app/ product /fmw/user_ projects /domains /ui_domain	
44	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
45	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
46	IPM_SERVER_IP	IP of Oracle Image and Processing Server for OBP Content Management	10.180.84.114	
47	IPM_SERVER_ PORT	Port of Oracle Image and Processing Server for OBP Content Management	16000	
48	IPM_MW_HOME	Oracle weblogic Home directory on IPM server	/scratch/app/product/fmw	
49	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ECM1	
50	OBP_HOST_DB_ USER	OBP Host database user/schema	OBEDMUS211	
51	OBP_HOST_DB_ PASSWORD	OBP Host database password	welcome1	
52	OBP_HOST_DB_IP	OBP Host database i/p address	10.180.84.113	
53	OBP_HOST_DB_ PORT	OBP Host database port	1521	
54	OBP_HOST_DB_ SERVICE_NAME	OBP Host database service name	P84113A	
55	ONS_NODE	i/p address of ONS service	10.180.84.113	
56	ONS_PORT	Listen port of ONS service	6200	
57	OPSS_HOST_ SCHEMA_USER	HOST OPSS Host schema user	COLLMW_OPSS	

Sr. No	Name	Description	Example Value	Value
58	OPSS_HOST_ AUDIT_DBDS	HOST OPSS Audit schema name	COLLMW_IAU_APPEND	
59	OPSS_HOST_ AUDIT_VIEWDS	HOST OPSS Audit View schema name	COLLMW_IAU_VIEWER	
60	OPSS_HOST_ SCHEMA_ PASSWORD	OPSS Host schema password	welcome1	
61	OPSS_HOST_DB_ IP	OPSS Host DB IP	10.180.84.113	
62	OPSS_HOST_DB_ PORT	OPSS Host DB Port	1521	
63	OPSS_HOST_DB_ SERVICE_NAME	OPSS Host database service name	P84113A	
64	LOCAL_ DATASOURCE	STB datasource schema name	COLLMW_STB	
65	WLS_RUNTIME_ SCHEMA_USER	WLS runtime datasource schema name	COLLMW_WLS_RUNTIME	
66	MDS_HOST_DB_ USER	MDS schema user to be used by UI and Host domain	COLLMW_MDS	
67	MDS_HOST_DB_ PASSWORD	MDS schema Password of MDS schema user to be used by UI and Host domain	welcome1	
68	MDS_HOST_DB_IP	MDS DB IP address of MDS schema user to be used by UI and Host domain	10.180.84.113	
69	MDS_HOST_DB_ PORT	MDS db port of MDS schema user to be used by UI and Host domain	1521	
70	MDS_HOST_DB_ SERVICE_NAME	MDS db service name of MDS schema user to be used by UI and Host domain	P84113A	
71	HOST_ADMIN_ JVM_PARAMS	Host domain admin JVM startup parameters	-Xms1024m -Xmx4096m	
72	HOST_MANAGED_	Host domain	Xms8g -Xmx8g -XX:NewSize=2048m	

Sr. No	Name	Description	Example Value	Value
	JVM_PARAMS	managed JVM startup parameters	-XX:MaxNewSize=4096m -XX:+UseParNewGC -XX: +CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75	
73	KEYSTORE_ PASSWORD	Password for generating certificate	welcome1	
74	IPM_OUTBOUND_ USERNAME	IPM Username created in connector	weblogic	
75	IPM_OUTBOUND_ PASSWORD	Password for the IPM user in connector	weblogic1	
76	BIP_OUTBOUND_ USERNAME	BIP Username created in connector	weblogic	
77	BIP_OUTBOUND_ PASSWORD	Password for the BIP user in connector	weblogic1	
78	ODI_OUTBOUND_ USERNAME	ODI Username created in connector	weblogic	
79	ODI_OUTBOUND_ PASSWORD	Password for the ODI user in connector	weblogic1	
80	OIM_OUTBOUND_ USERNAME	OIM Username created in connector	weblogic	
81	OIM_OUTBOUND_ PASSWORD	Password for the OIM user in connector	weblogic1	
82	WCM_ OUTBOUND_ USERNAME	WCM Username created in connector	weblogic	
83	WCM_ OUTBOUND_ PASSWORD	Password for the WCM user in connector	weblogic1	
84	OFFLINE_ CHANNEL_ OUTBOUND_ USERNAME	Offline Username created in connector	offlineuser	

Sr. No	Name	Description	Example Value	Value
85	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password for the Offline user in connector	welcome1	
86	SAML_ISSUER_ OUTBOUND_ USERNAME	SAML ISSUER Username created in connector	weblogic	
87	SAML_ISSUER_ OUTBOUND_ PASSWORD	Password for the SAML ISSUER user in connector	weblogic1	
88	BPEL_ ENCRYPTION_ OUTBOUND_ USERNAME	BPEL_ ENCRYPTION Username created in connector	weblogic	
89	BPEL_ ENCRYPTION_ OUTBOUND_ PASSWORD	Password for the BPEL_ ENCRYPTION user in connector	weblogic1	
90	FTP_IPM_ OUTBOUND_ USERNAME	FTP IPM Username created in connector	weblogic	
91	FTP_IPM_ OUTBOUND_ PASSWORD	Password for the FTP IPM user in connector	weblogic1	
92	FTP_BIP_ OUTBOUND_ USERNAME	FTP BIP Username created in connector	weblogic	
93	FTP_BIP_ OUTBOUND_ PASSWORD	Password for the FTP BIP user in connector	weblogic1	
94	BIP_USR_ OUTBOUND_ USERNAME	BIP Username created in connector	weblogic	
95	BIP_USR_ OUTBOUND_ PASSWORD	Password for the BIP user in connector	weblogic1	
96	SOA_PURGING_ OUTBOUND_ USERNAME	SOA Username created in connector	weblogic	
97	SOA_PURGING_ OUTBOUND_ PASSWORD	Password for the SOA user in connector	weblogic1	
98	SOA_OUTBOUND_ USERNAME	SOA Username created in connector	weblogic	

Sr. No	Name	Description	Example Value	Value
99	SOA_OUTBOUND_PASSWORD	Password for the SOA user in connector	weblogic1	
100	ATMUSER_OUTBOUND_USERNAME	ATM Username created in connector	ATMUser	
101	ATMUSER_OUTBOUND_PASSWORD	Password for the ATM user in connector	welcome1	
102	POSUSER_OUTBOUND_USERNAME	POS Username created in connector	POSUser	
103	POSUSER_OUTBOUND_PASSWORD	Password for the POS user in connector	welcome1	
104	DMSHOST_OUTBOUND_USERNAME	DMS HOST Username created in connector	weblogic	
105	DMSHOST_OUTBOUND_PASSWORD	Password for the DMS HOST user in connector	weblogic1	
106	DMSUI_OUTBOUND_USERNAME	DMS UI Username created in connector	weblogic	
107	DMSUI_OUTBOUND_PASSWORD	Password for the DMS UI user in connector	weblogic1	
108	OCH_OUTBOUND_USERNAME	OCH Username created in connector	weblogic	
109	OCH_OUTBOUND_PASSWORD	Password for the OCH user in connector	weblogic1	
110	WS_MFT_OUTBOUND_USERNAME	WS_MFT Username created in connector	weblogic	
111	WS_MFT_OUTBOUND_PASSWORD	Password for the WS_MFT user in connector	weblogic1	
112	OP_OUTBOUND_USERNAME	OP Username created in connector	weblogic	
113	OP_OUTBOUND_PASSWORD	Password for the OP user in	weblogic1	

Sr. No	Name	Description	Example Value	Value
		connector		
114	ICS_OUTBOUND_USERNAME	Username for ICS connector	weblogic	
115	ICS_OUTBOUND_PASSWORD	Password for ICS connector	Weblogic1	
116	OBDX_OUTBOUND_USERNAME	Username for OBDX connector	1518675030085dean.white@test.com	
117	OBDX_OUTBOUND_PASSWORD	Password for OBDX connector	Welcome@1	
118	CARD_USERNAME	Username of Card connector	orakey	
119	CARD_PASSWORD	Password of Card connector	welcome1	
120	RULE_USERNAME	Username of Rule connector	orakey	
121	RULE_PASSWORD	Password of Rule connector	welcome1	
122	BAM_USERNAME	Username of BAM connector	weblogic	
123	BAM_PASSWORD	Password of BAM connector	weblogic1	
124	COMMON_OUTBOUND_USERNAME	Username for common connector	Weblogic1	
125	COMMON_OUTBOUND_PASSWORD	Password for common connector	Weblogic1	
126	PM_OUTBOUND_USERNAME	Username for PM connector	weblogic	
127	PM_OUTBOUND_PASSWORD	Password for PM connector	weblogic1	
128	LENDING_OUTBOUND_USERNAME	Username for lending connector	weblogic	
129	LENDING_OUTBOUND_PASSWORD	Password for lending connector	weblogic1	
130	DEPOSITS_OUTBOUND_USERNAME	Username for deposits connector	weblogic	

Sr. No	Name	Description	Example Value	Value
131	DEPOSITS_OUTBOUND_PASSWORD	Password for deposits connector	weblogic1	
132	FW_OUTBOUND_USERNAME	Username for FW connector	weblogic	
133	FW_OUTBOUND_PASSWORD	Password for fw connector	weblogic1	
134	COLLECTION_OUTBOUND_USERNAME	Username for collection connector	weblogic	
135	COLLECTION_OUTBOUND_PASSWORD	Password for collection Connector	weblogic1	
136	OR_OUTBOUND_USERNAME	Username for OR connector	weblogic	
137	OR_OUTBOUND_PASSWORD	Password for OR connector	weblogic1	
138	PARTY_OUTBOUND_USERNAME	Username for Party connector	weblogic	
139	PARTY_OUTBOUND_PASSWORD	Password for Party connector	weblogic1	
140	PRODPROC_OUTBOUND_USERNAME	Username for PRODPROC connector	weblogic	
141	PRODPROC_OUTBOUND_PASSWORD	Password for PRODPROC connector	weblogic1	
142	RECOVERY_OUTBOUND_USERNAME	Username for Recovery connector	weblogic	
143	RECOVERY_OUTBOUND_PASSWORD	Password for Recovery connector	weblogic1	
144	PRICING_OUTBOUND_USERNAME	Username for Pricing connector	weblogic	
145	PRICING_OUTBOUND_PASSWORD	Password for Pricing connector	weblogic1	
146	LCM_OUTBOUND_USERNAME	Username for LCM connector	weblogic	

Sr. No	Name	Description	Example Value	Value
147	LCM_OUTBOUND_PASSWORD	Password for LCM connector	weblogic1	
148	MDM_OUTBOUND_USERNAME	Username for MDM connector	weblogic	
149	MDM_OUTBOUND_PASSWORD	Password for MDM connector	weblogic1	
150	COMMUNICATIONS_OUTBOUND_USERNAME	Username for COMMUNICATIONS connector	weblogic	
151	COMMUNICATIONS_OUTBOUND_PASSWORD	Password for COMMUNICATIONS connector	weblogic1	
152	APPCAPTURE_OUTBOUND_USERNAME	Username for APPCAPTURE connector	weblogic	
153	APPCAPTURE_OUTBOUND_PASSWORD	Password for APPCAPTURE connector	weblogic1	
154	EDN_OUTBOUND_USERNAME	Username for EDN connector	weblogic	
155	EDN_OUTBOUND_PASSWORD	Password for EDN connector	weblogic1	
156	EJBSUBJECT_USERNAME	Username for EJBSUBJECT connector	weblogic	
157	EJBSUBJECT_PASSWORD	Password for EJBSUBJECT connector	weblogic1	
158	USER_TIMEZONE	Time zone entry	+5:30	
159	HOST_SSL_PASSWORD	Password for configuring SSL in HOST domain	welcome1	
160	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	
161	OAAM_SERVER_PORT	OAAM server Port for 2FA.	14000	

Sr. No	Name	Description	Example Value	Value
		OAAM_SERVER_ PORT refers to the port of OAAM Server (default server name as oaam_server_ server1)		
162	OIM_SERVER_IP	Oracle Identity Manager IP	oim-ofss.com	
163	OIM_SERVER_ PORT	Oracle Identity Manager Port	16000	
164	OFSAA_SERVER_ IP	OFSAA Server IP	ofsaa-ofss.com	
165	OFSAA_SERVER_ PORT	OFSAA Server Port	17000	
166	DOCUMAKER_ SERVER_IP	i/p address of Documaker server	documaker-ofss.com	
167	DOCUMAKER_ SERVER_PORT	Listen port of Documaker server	15000	
168	BAM_SERVER_ NAME	Bam sever listen address	bam-ofss.com	
169	BAM_SERVER_ PORT	BAM managed server port	9003	
170	ODI_SERVER_ NAME	ODI server listen address	odi-ofss.com	
171	ODI_SERVER_ PORT	ODI server listen port	8001	

Table 2–5 Values for updating installobp.properties - For UI***

Sr. No	Name	Description	Example Value	Value
1	SILENT_INSTALL	Flag for executing installer remotely	Y	
2	SECURITY_ ENABLED	Flag for security enable	Y	
3	IPM_INSTALLED	Flag for if IPM is installed	Y	
4	LOCAL_IP	I/P address of the local machine which could be a windows machine on which software like	10.180.84.111	

Sr. No	Name	Description	Example Value	Value
		XManager is installed for rendering UI of a utility executing on a remote Linux server.		
5	LOCAL_DISPLAY_ VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
6	DOMAIN_NAME	Weblogic Domain name	Host_domain or ui_domain or base_ domain	
7	XD_COMPONENT_ NAME	XD Component value	obpui	This will be always obpui
8	LOCALIZATION_ TYPE	Type of localization	US	Depends on localization type
9	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
10	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
11	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
12	LOCAL_ DATASOURCE	Username of LOCAL_ DATASOURCE	COLLUI_STB	
13	WLS_RUNTIME_ SCHEMA_USER	Username of WLS Runtime schema	COLLUI_WLS_RUNTIME	
14	OPSS_UI_ SCHEMA_USER	OPSS UI schema name	COLLUI_OPSS	
15	OPSS_UI_ SCHEMA_ PASSWORD	OPSS UI schema password	Welcome1	
16	OPSS_UI_DB_IP	OPSS UI DB IP	10.180.84.113	
17	OPSS_UI_DB_ PORT	OPSS UI DB PORT	1521	
18	OPSS_UI_DB_ SERVICE_NAME	OPSS UI DB SERIVICE NAME	P84113A	
19	MDS_SCHEMA_ USER	MDS schema name	COLLUI _MDS	
20	MDS_SCHEMA_ PASSWORD	Password of MDS schema	welcome1	

Sr. No	Name	Description	Example Value	Value
21	MDS_DB_IP	MDS DB IP	10.180.84.113	
22	MDS_DB_PORT	MDS DB PORT	1521	
23	MDS_DB_ SERVICE_NAME	MDS DB SERVIVE NAME	P84113A	
24	OPSS_HOST_ SCHEMA_USER	HOST OPSS Schema name	COLLMW _OPSS	
25	OPSS_HOST_ AUDIT_DBDS	HOST OPSS AUDIT schema name	COLLMW_IAU_APPEND	
26	OPSS_HOST_ AUDIT_VIEWDS	HOST OPSS AUDIT VIEWDB Schema name	COLLMW_IAU_VIEWER	
27	OPSS_HOST_ SCHEMA_ PASSWORD	HOST OPSS password for above three OPSS schema	welcome1	
28	OPSS_HOST_DB_ IP	Service name of UI OPSS DB	10.180.84.113	
29	OPSS_HOST_DB_ PORT	HOST OPSS DB PORT	1521	
30	OPSS_HOST_DB_ SERVICE_NAME	HOST OPSS DB SERVICE NAME	P84113A	
31	HOST_SCHEMA_ USER	OBP Host Database username	OBEDMUS211	
32	HOST_SCHEMA_ PASSWORD	OBP Host Database password	welcome1	
33	HOST_DB_IP	OBP Host Database i/p address	10.180.84.113	
34	HOST_DB_PORT	OBP Host Database listen port	1521	
35	HOST_DB_ SERVICE_NAME	OBP Host Database service name	P84113A	
36	ONS_NODE	i/p address of ONS service	10.180.84.113	
37	ONS_PORT	Listen port of ONS service	6200	
38	ADMIN_SERVER_ LISTEN_ADDRESS	Admin server listen address	10.180.84.111	
39	ADMIN_SERVER_ LISTEN_PORT	Admin server listen port	7001	
40	ADMIN_SERVER_ SSL_LISTEN_	Admin server SSL listen port	7002	

Sr. No	Name	Description	Example Value	Value
	PORT			
41	MANAGED_ SERVER_LISTEN_ ADDRESS	Managed server listen address	10.180.84.111	
42	MANAGED_ SERVER_LISTEN_ PORT	Managed server listen port	8001	
43	MANAGED_ SERVER_SSL_ LISTEN_PORT	Managed server SSL listen port	8002	
44	LDAP_PROVIDER	Refers to LDAP Provider. Value will be OID or OVD.	OID	
45	OID_IP	I/P address of the OID server	10.180.84.113	
46	OID_PORT	Port of the OID process instance.	3060	
47	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn=orcladmin	
48	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
49	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
50	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	cn=Users,dc=in,dc=oracle,dc=com	
51	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	
52	UI_IP	I/P address of the server on which the OBP presentation or UI layer should be	10.180.84.111	

Sr. No	Name	Description	Example Value	Value
		installed.		
53	UI_CLUSTER_ NAME	Name of UI Managed Cluster	obpui_cluster1	
54	UI_SERVER_ NAME	Name of UI Managed Server	obpui_server1	
55	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 OBP should have read, write and execute privileges on this directory.	/scratch/install/target	
56	UI_MW_HOME	Refers to the middleware home of the weblogic installation on the UI server.	/scratch/app/product/fmw	
57	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 OBP security policies policy seeding utility at the end of the installation.	/scratch/app/product/jdk1.8.0_231	
58	OUI_JAVA_HOME	Refers to the home directory of java installation. The version of java installed should be 1.8.0 . This is used for OBP patching.	/scratch/app/product/jdk1.8.0_231	
59	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
60	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
61	IPM_UNIX_USER	Linux login user id of IPM server	ofssobp	
62	IPM_SERVER_IP	i/p address of IPM	10.180.84.114	

Sr. No	Name	Description	Example Value	Value
		server		
63	IPM_SERVER_ PORT	Listen port of IPM server	16000	
64	IPM_MW_HOME	Oracle Weblogic Home directory on IPM server	/scratch/app/product/fmw	
65	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ ECM1	
66	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	
67	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	
68	OIM_SERVER_IP	Oracle Identity Manager i/p address	oim-ofss.com	
69	OIM_SERVER_ PORT	Oracle Identity Manager Listen Port	16000	
70	OFSAA_SERVER_ IP	OFSAA Server i/p address	ofsaa-ofss.com	
71	OFSAA_SERVER_ PORT	OFSAA Server listen port	17000	
72	UI_ADMIN_JVM_ PARAMS	UI domain admin JVM startup parameters	-Xms2048m -Xmx4096m	
73	UI_MANAGED_ JVM_PARAMS	UI domain managed JVM startup parameters	-Djbo.ampoo l.doampooling=false -Xms6g -Xmx6g -XX:NewSize=512m -XX:MaxNewSize =2048m -XX:+UseParNewGC -XX:+CMSParallel RemarkEnabled -XX:+UseConcMark SweepGC -XX:CMSInitiating Occupancy Fraction=75 -Djbo.load.com ponents.lazily=true	

Sr. No	Name	Description	Example Value	Value
74	HOST_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of HOST admin server	10.180.84.110	
75	HOST_ADMIN_SERVER_LISTEN_PORT	Listen port of HOST admin server	7001	
76	HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of host managed server	10.180.84.110	
77	HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of host managed server	8001	
78	KEYSTORE_PASSWORD	Password for generating certificate	welcome1	
79	UI_SSL_PASSWORD	Password for configuring SSL in UI domain	welcome1	
80	UCM_READ_FROM_URL	Flag for getting UCM URL from properties file. These values are used by the Webcenter Portal application for internet banking. 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	true/false	
81	UCM_IP	UCM_IP the IP address of the UCM WebLogic managed server.	ofss.ucm.com	
82	UCM_PORT	Port of UCM.	4444	
83	OFFLINE_	Offline username created in connector	offlineuser	

Sr. No	Name	Description	Example Value	Value
	CHANNEL_ OUTBOUND_ USERNAME			
84	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password for the Offlineuser user in connector	welcome1	
85	CARD_ USERNAME	Username of Card connector.	orakey	
86	CARD_ PASSWORD	Password of Card connector.	welcome1	
87	RULE_USERNAME	Username of Rule connector	orakey	
88	RULE_ PASSWORD	Password of Rule connector	welcome1	
89	USER_TIMEZONE	Time zone entry	+5:30	
90	REMOTE_ EXECUTION	Flag for executing installer remotely	Y	
91	IPM_USERNAME	Username of IPM connector	weblogic	
92	IPM_PASSWORD	Password of IPM connector	weblogic1	
93	FTP_IPM_ USERNAME	Username of FTP_IPM connector	ofssobp	
94	FTP_IPM_ PASSWORD	Password of FTP_IPM connector	ofssobp123	
95	FTP_IPM_BATCH_ USERNAME	Username of FTP_ IPM_BATCH	ofssobp	
96	FTP_IPM_BATCH_ PASSWORD	Password of FTP_ IPM_BATCH	ofssobp123	
97	HOST_UNIX_ USER	Linux login user id for HOST server	ofssobp	
98	HOST_MW_HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
99	HOST_DOMAIN_ NAME	Refers to the middleware Host domain name.	host_domain	

2.2.2 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 Oracle Banking Enterprise Default Management 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.	
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 OBEDM Oracle DB server	10.180.90.30	
6.	Port of the OBEDM Oracle DB instance	1521	
7.	OBEDM DB Service Name	OBEDMDB	
8.	OBEDM 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 OBEDM 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 OBEDM 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	Decide on the password to be used and note it. This is required for the	

Sr. No.	Name	Description and Example	Value
	trust between the OBEDM UI and Host.	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 OBEDM 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 the OBEDM Host 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	
17.	Password for the key generated to establish trust between the OBEDM 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.	

2.3 OID Schema Setup – Custom OBEDM Schema

This section describes the OID Schema setup which is a pre-installation configuration required for Oracle Banking Enterprise Default Management setup.

2.3.1 Prerequisite – OID setup

It is assumed that OID 12.2.1.3.0 is installed with ODSM and configured. We can thereafter proceed to the next step of setting up the OBEDM policy store. OID works better when installed on OEL. See Section 2.1.2 Software Environment for version information of the software products.

2.3.2 Verify the OID installation

This section describes the procedure to verify the OID installation.

2.3.2.1 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
```

To start the OID, use startComponent script and pass the component name as a parameter. Before starting OID, make sure Admin Server and NodeManager are up and running.

2.3.2.2 OPSS/OID Performance Tuning

The following changes are required in OID before initiating OBEDM 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
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;

Sr. No.	DB Property Name	Suggested Value for Tuning	Alter Command
			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_ 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 OBEDM-UI, OBEDM-Host, OBEDM-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

Property	Description
	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
```

2.3.2.3 Import OBEDM 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 OBEDM.

If OIM is not part of the ecosystem and an initial sanity test of the OBEDM 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 ’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
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
   ```

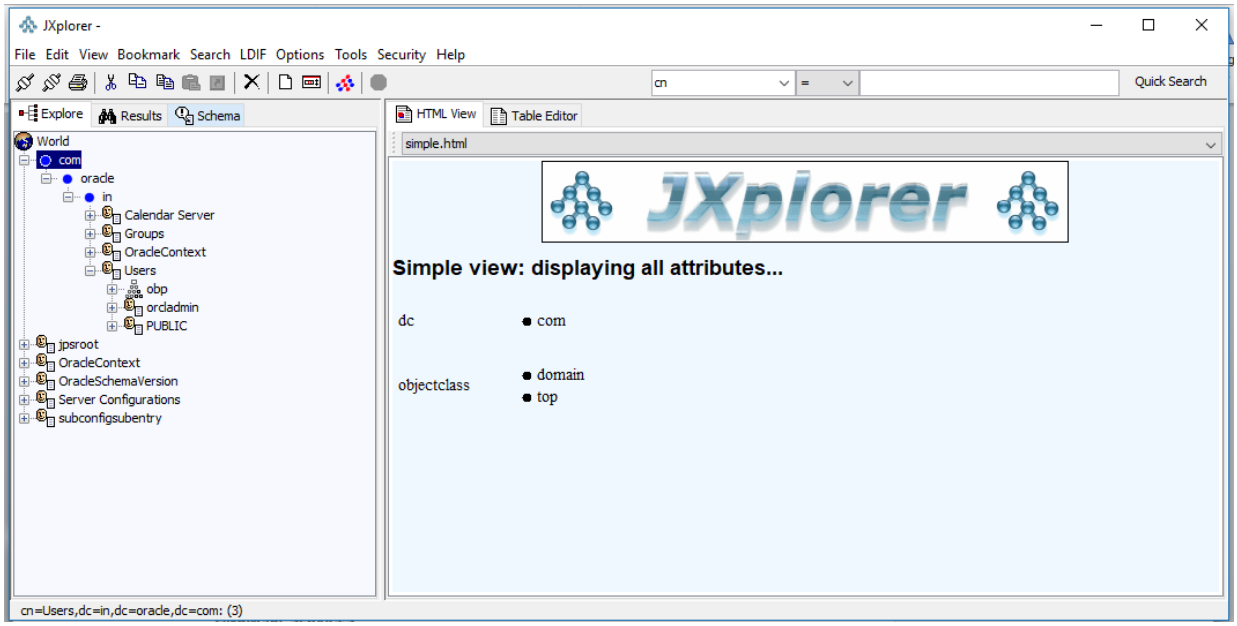
   ldapadd Administrators.ldif

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

2.3.2.4 Verify the import using ODSM or JXplorer

The import of Oracle Banking Enterprise Default Management specific LDIF files can be verified using JXplorer.

Figure 2–1 JXplorer



3 OBEDM US Localization Host Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Enterprise Default Management US Localization Host Media pack. The subsequent section refers to the variable names specified in Section 2.2 Installation Checklist.

3.1 Installation and Configuration Procedure

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

3.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBEDM 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 'obpus-host.zip'. Below files will be extracted:

- A zip file 'obpinstall-host.zip'
- The installation script 'installobphost.sh'
- The install configuration property file 'installobphost.properties'
- A zip file 'em_monitor.zip' that is used for monitoring (For more information, see Chapter 1 Monitoring Servers Using Oracle Enterprise Manager).

Step 3 Printing Checklists

Take a printout of the installation checklist mentioned in Section 2.2 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 OBEDM US Localization Host Media Pack installation.

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.

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 5.1 Pre-Installation Steps and Section 5.2 OBEDM 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.

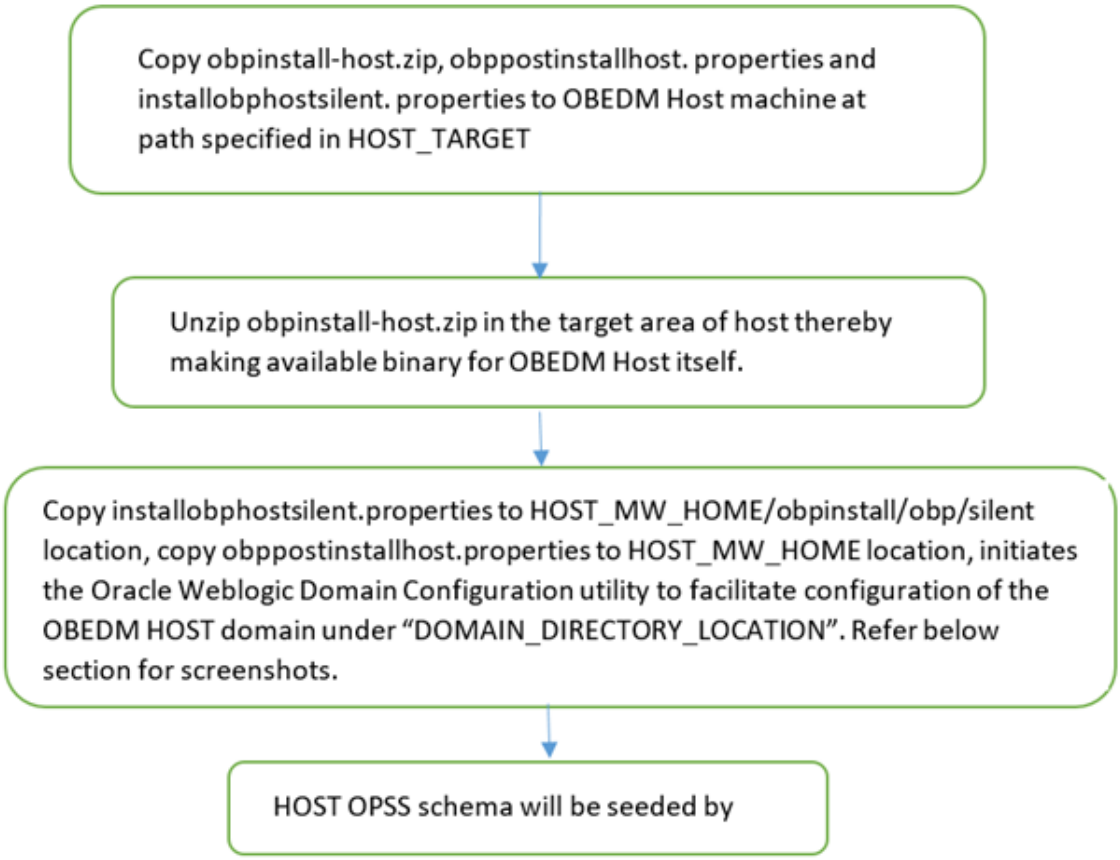
  For example, if HOST_DB_SCHEMA_PREFIX is DEV, then OBP_HOST_DB_USER should be DEV_OBP.
- OID_DOMAIN_NAME in installobphost.properties should match with the OID_DOMAIN_NAME given in installobpui.properties. Any other domain with the same name must not exist in OID. The domain in OID will be created in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

3.1.3 Installation Steps

This section lists the installation steps required for the OBEDM 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 3–1 Steps in installobphost.sh script



A sample output is given here.

Figure 3–2 Verification of Properties

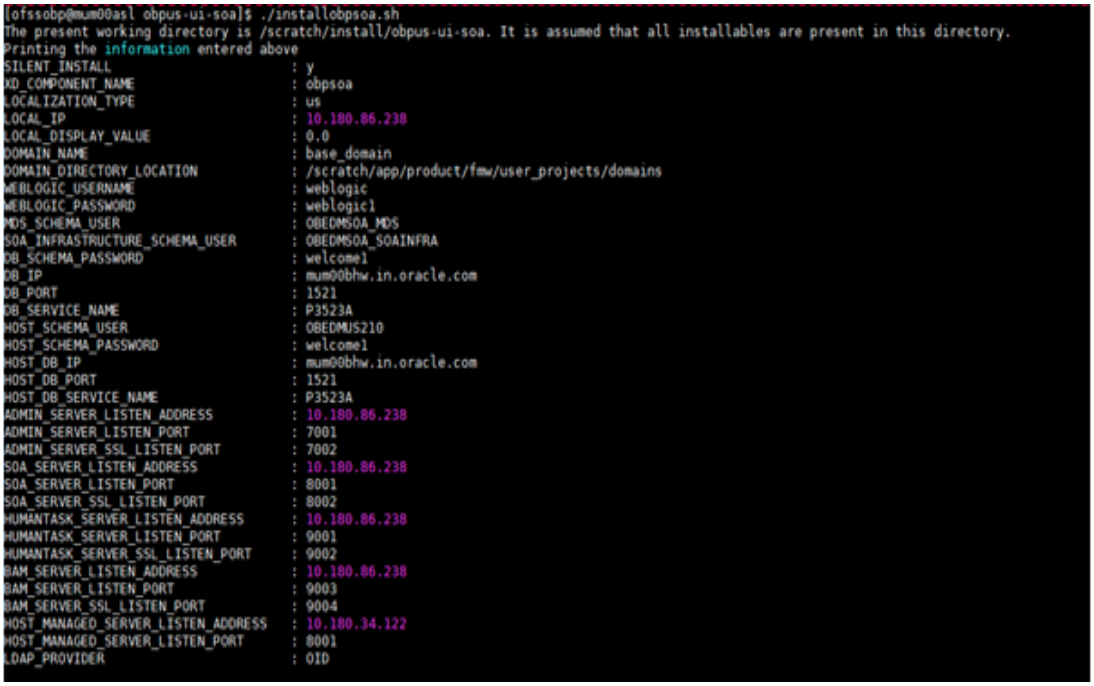


Figure 3–3 Verification of Properties (contd)

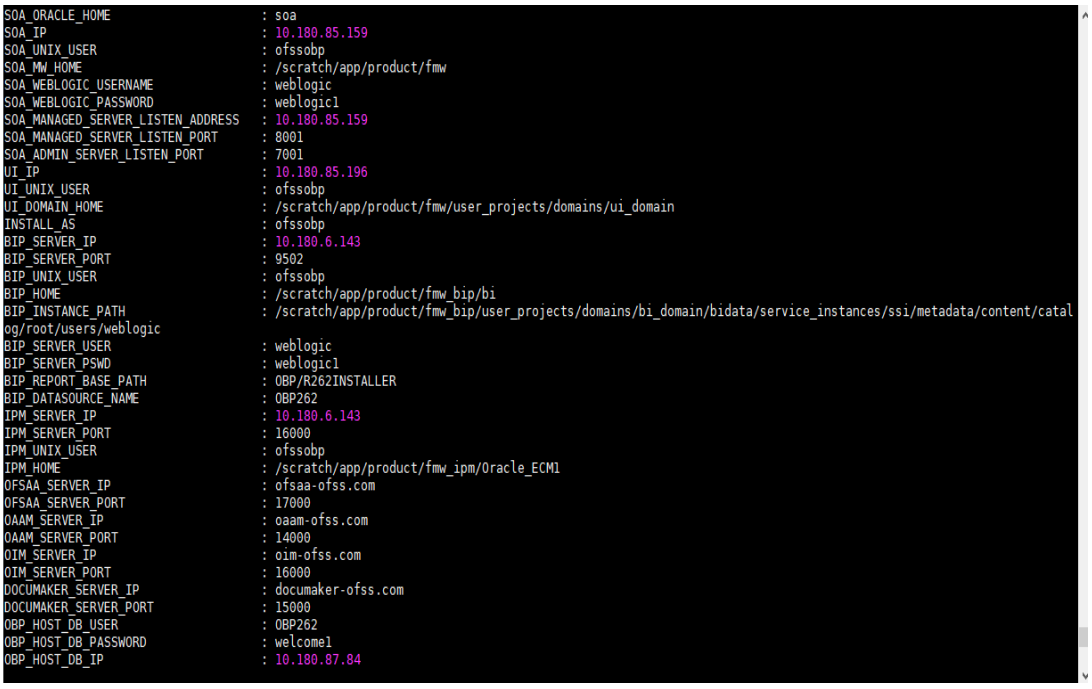


Figure 3–4 Verification of Properties (contd)

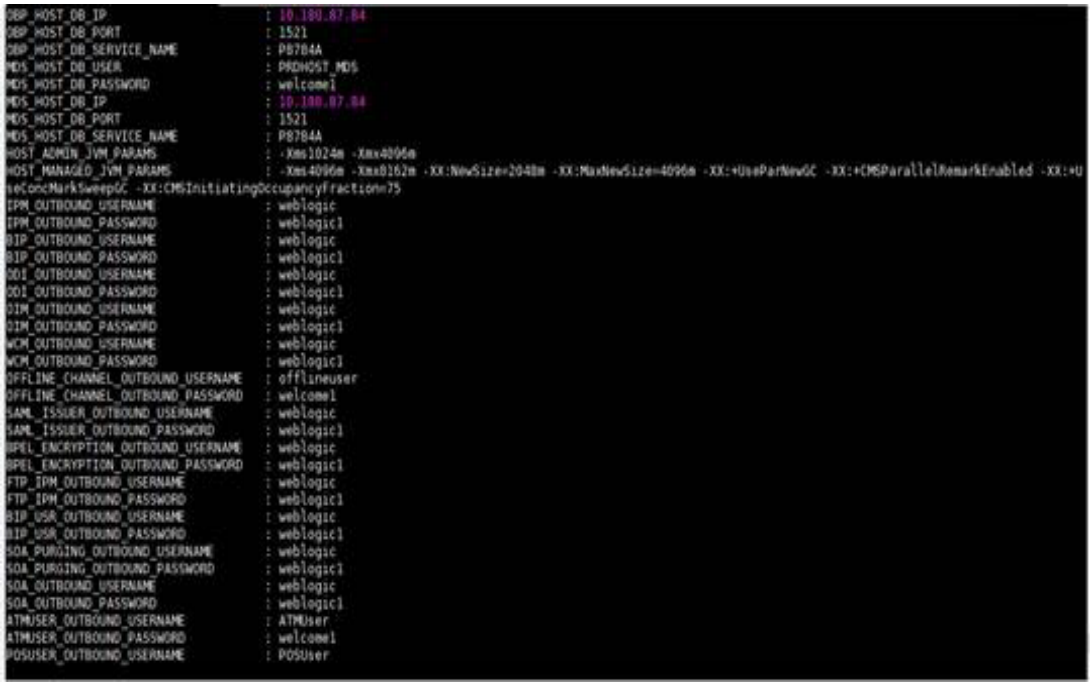
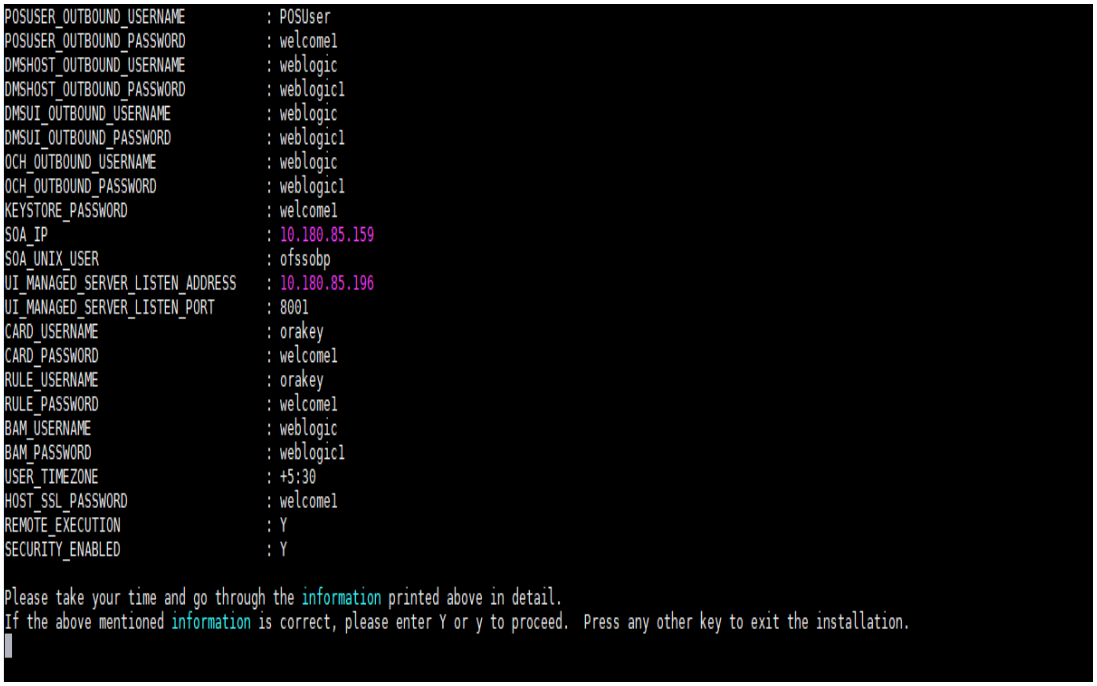


Figure 3–5 Verification of Properties (contd)



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 3–6 Confirmation and Copying of Installables to Target Machine

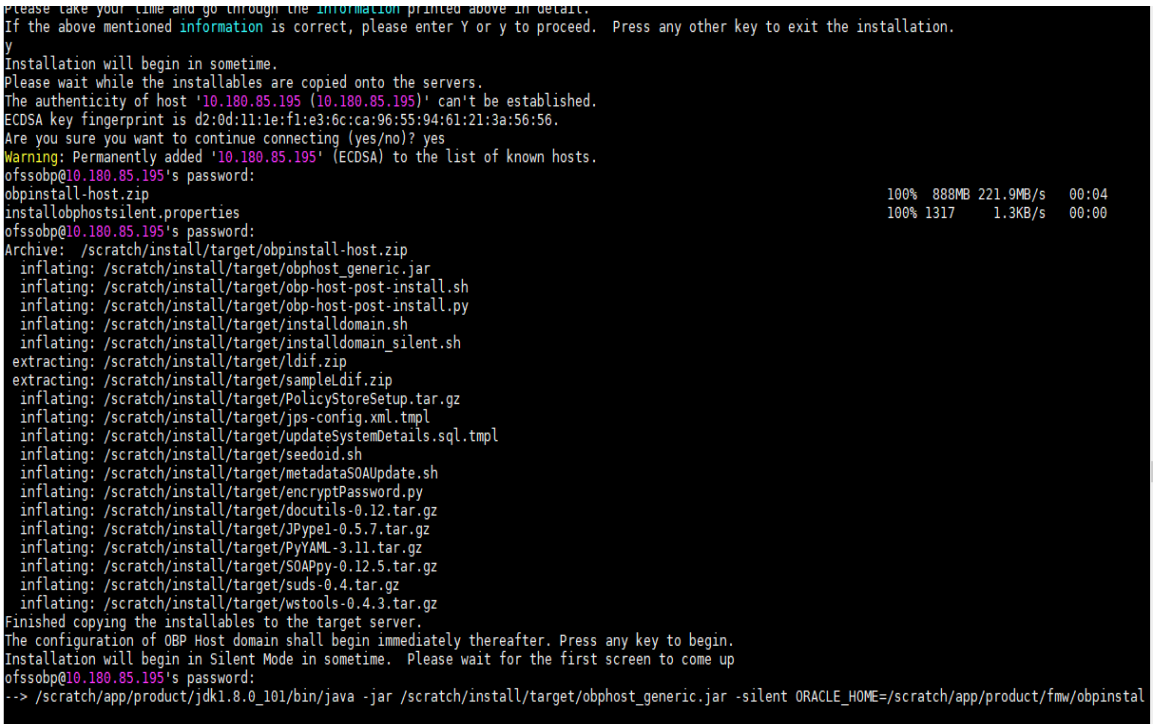


Figure 3–7 Confirmation and Copying of Installables to Target Machine (contd)

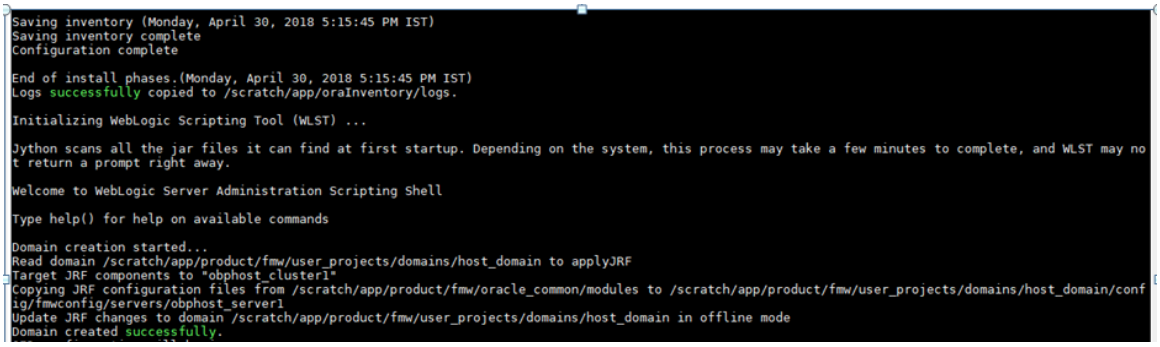
```
Installation will begin in Silent Mode in sometime.  Please wait for the first screen to come up
ofssobp@10.180.85.195's password:
--> /scratch/app/product/jdk1.8.0_101/bin/java -jar /scratch/install/target/obphost_generic.jar -silent ORACLE_HOME=/scratch/app/product/fmw/obpinstal
l INVENTORY_LOCATION=/scratch/app/oraInventory
Launcher log file is /tmp/OraInstall2018-05-03_02-55-30PM/launcher2018-05-03_02-55-30PM.log.
Extracting files......
Starting Oracle Universal Installer

Checking if CPU speed is above 300 MHz.   Actual 2693.527 MHz    Passed
Checking swap space: must be greater than 512 MB.   Actual 16057324 MB    Passed
Checking if this platform requires a 64-bit JVM.   Actual 64    Passed (64-bit not required)
Checking temp space: must be greater than 300 MB.   Actual 30062 MB    Passed


Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2018-05-03_02-55-30PM
.....................................................................................
Installation Summary


Disk Space : Required 827 MB, Available 295,999 MB
Feature Sets to Install:
        OBP Host Server FeatureSet 2.6.2.0.0
        Next Generation Install Core 13.2.0.0.0
        OPatch 13.2.0.0.0
.....................................................................................
You can find the log of this install session at:
 /tmp/OraInstall2018-05-03_02-55-30PM/install2018-05-03_02-55-30PM.log

Loading products list. Please wait.
.................. 1%
.................. 40%

Loading products. Please wait.
.................. 44%
.................. 47%
.................. 50%
.................. 53%
.................. 56%
```

Figure 3–8 Confirmation and Copying of Installables to Target Machine (contd)

```
.................. 56%
.................. 60%
.................. 63%
.................. 66%
.................. 70%
.................. 73%
.................. 76%
.................. 80%
.................. 83%
.................. 86%
.................. 90%
.................. 93%
.................. 96%
.................. 99%

............................................................  37% Done.
............................................................  75% Done.
..................................
Installation in progress (Thursday, May 3, 2018 2:55:53 PM IST)
                          98% Done.
Install successful

Linking in progress (Thursday, May 3, 2018 2:55:53 PM IST)
Link successful

Setup in progress (Thursday, May 3, 2018 2:55:53 PM IST)
Setup successful

Saving inventory (Thursday, May 3, 2018 2:55:53 PM IST)
Saving inventory complete
Configuration complete

End of install phases.(Thursday, May 3, 2018 2:55:54 PM IST)
Logs successfully copied to /scratch/app/oraInventory/logs.

Initializing WebLogic Scripting Tool (WLST) ...

Jython scans all the jar files it can find at first startup. Depending on the system, this process may take a few minutes to complete, and WLST may no
```

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 3–9 Domain Installation Confirmation



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

Figure 3–10 Untar the policyStoreSetup and Copy on destination location

Figure 3–11 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 3–12 Untar the policyStoreSetup and Copy on destination location (contd)

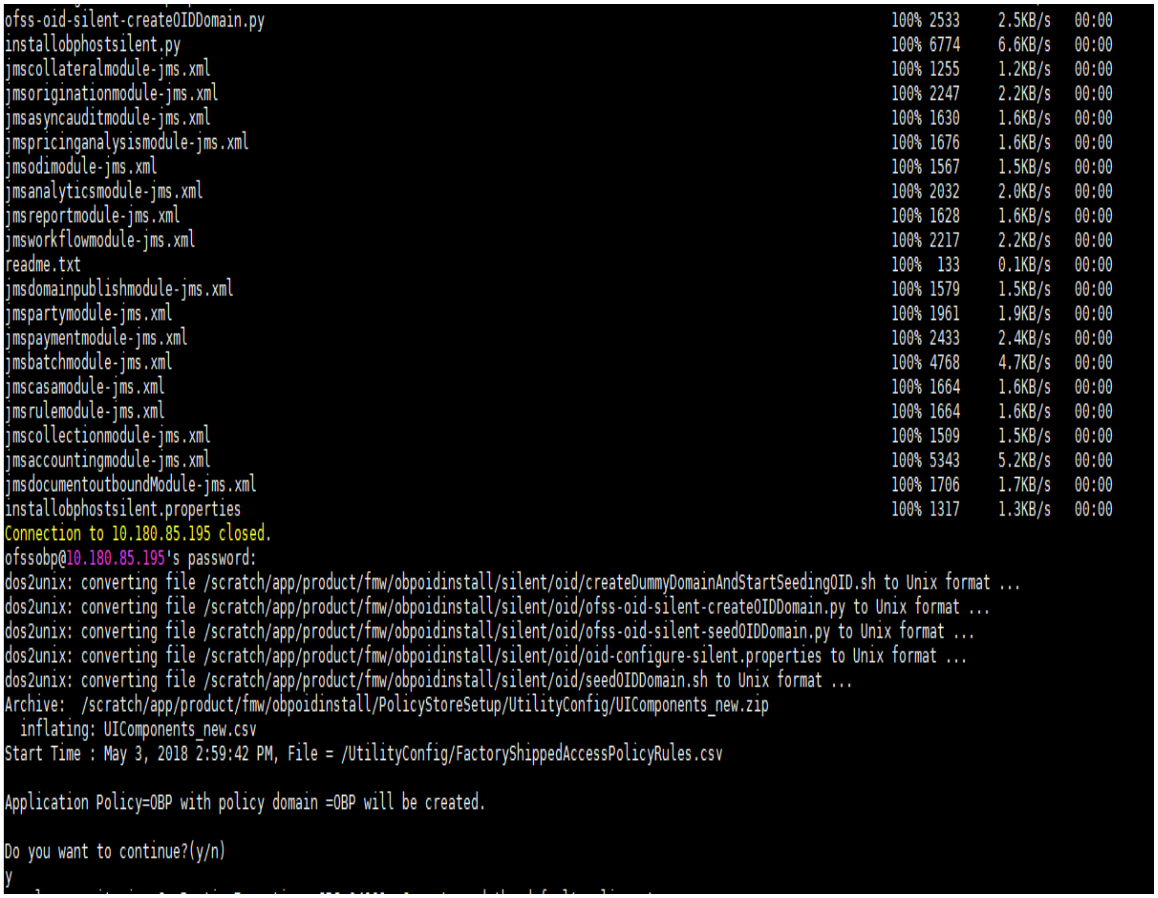
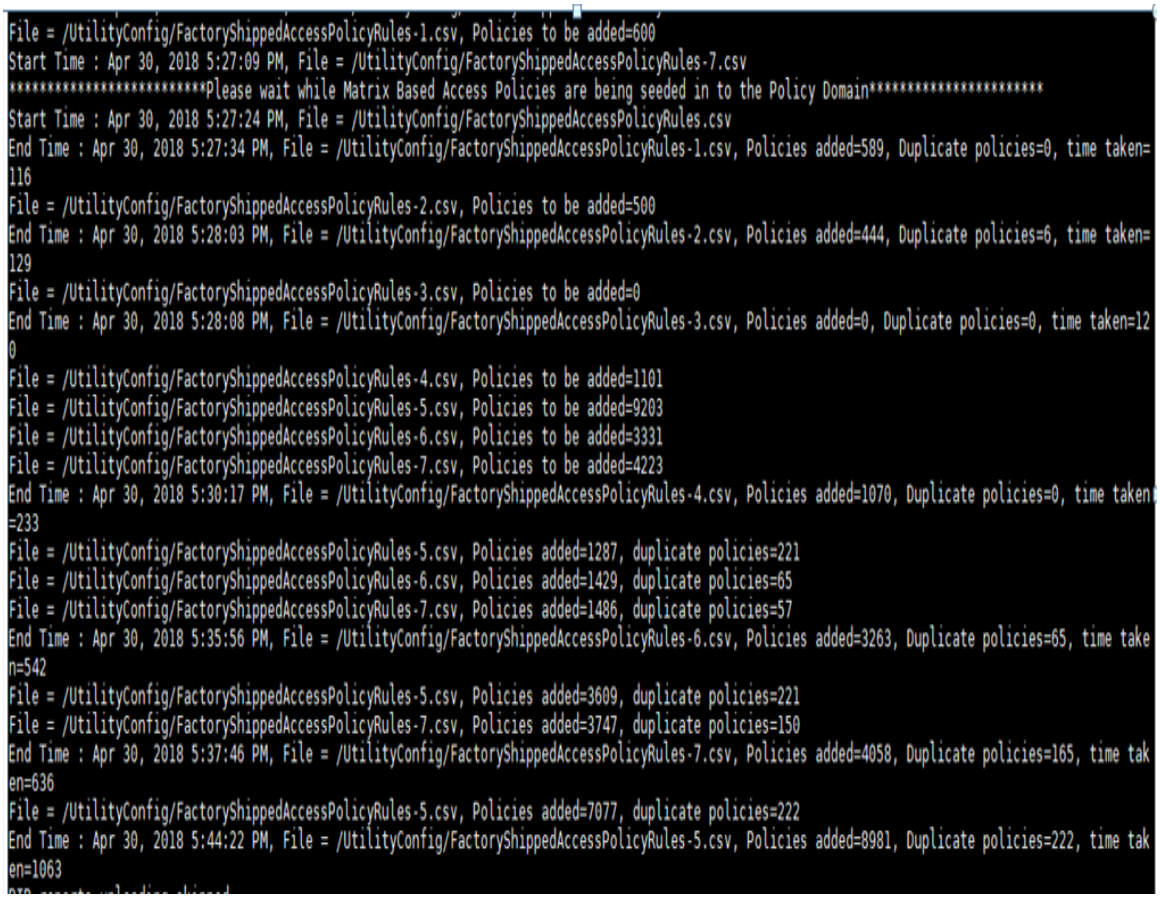


Figure 3–13 Policy Seeding

Figure 3–14 Policy Seeding (contd)



3.2 Post Installation Configuration

This section describes the post installation configuration procedure for OBEDM Host Media Pack. The procedure can be started after UI 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 5.3.3 HOST DB Schema Seeding and Section 5.3.4 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
  ```

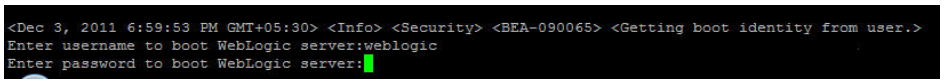
Post Installation Configuration

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/obphostdomai/bin
   ./startWebLogic.sh
   ```

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

   Figure 3–15 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 OBEDM config properties to point to the appropriate integration server
   - 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
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 3–16 Host Domain Post Installation Script Execution

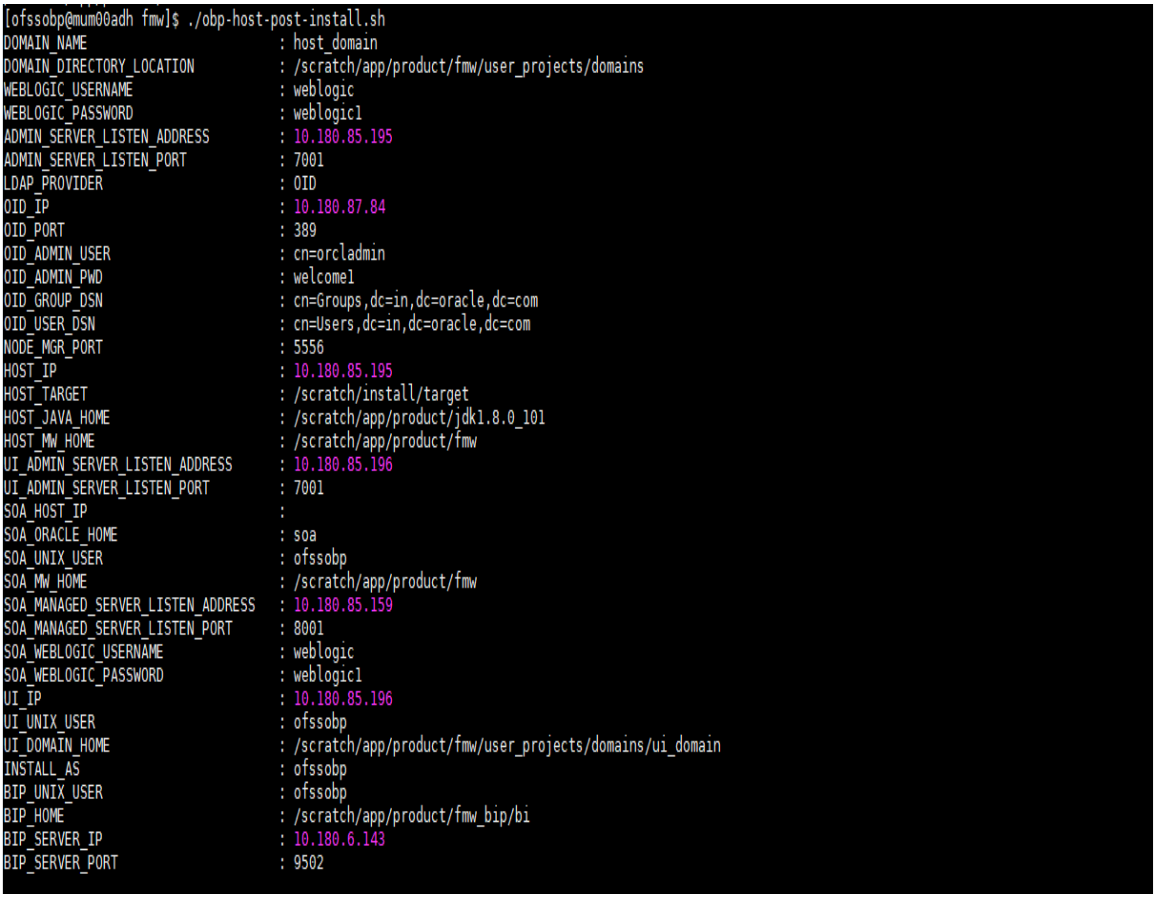


Figure 3–17 Host Domain Post Installation Script Execution (contd)

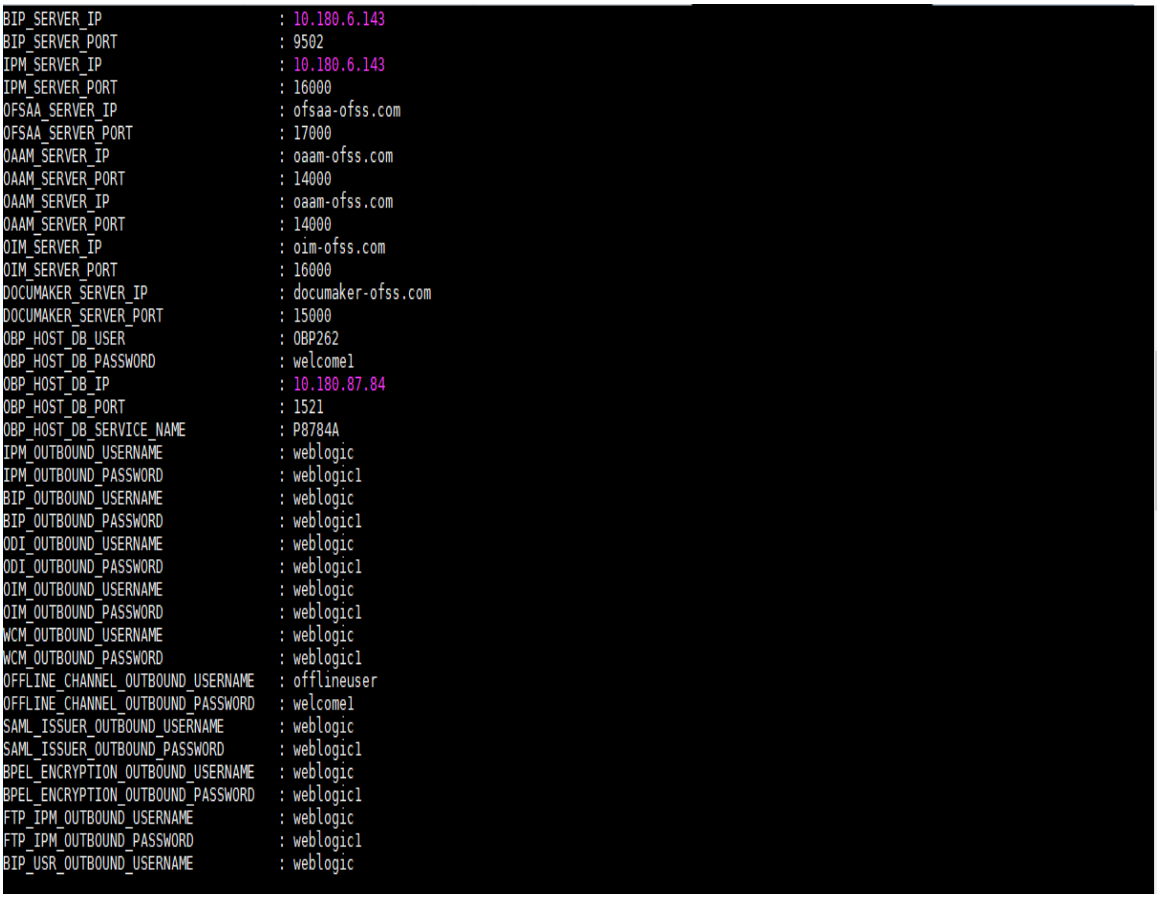


Figure 3–18 Host Domain Post Installation Script Execution (contd)

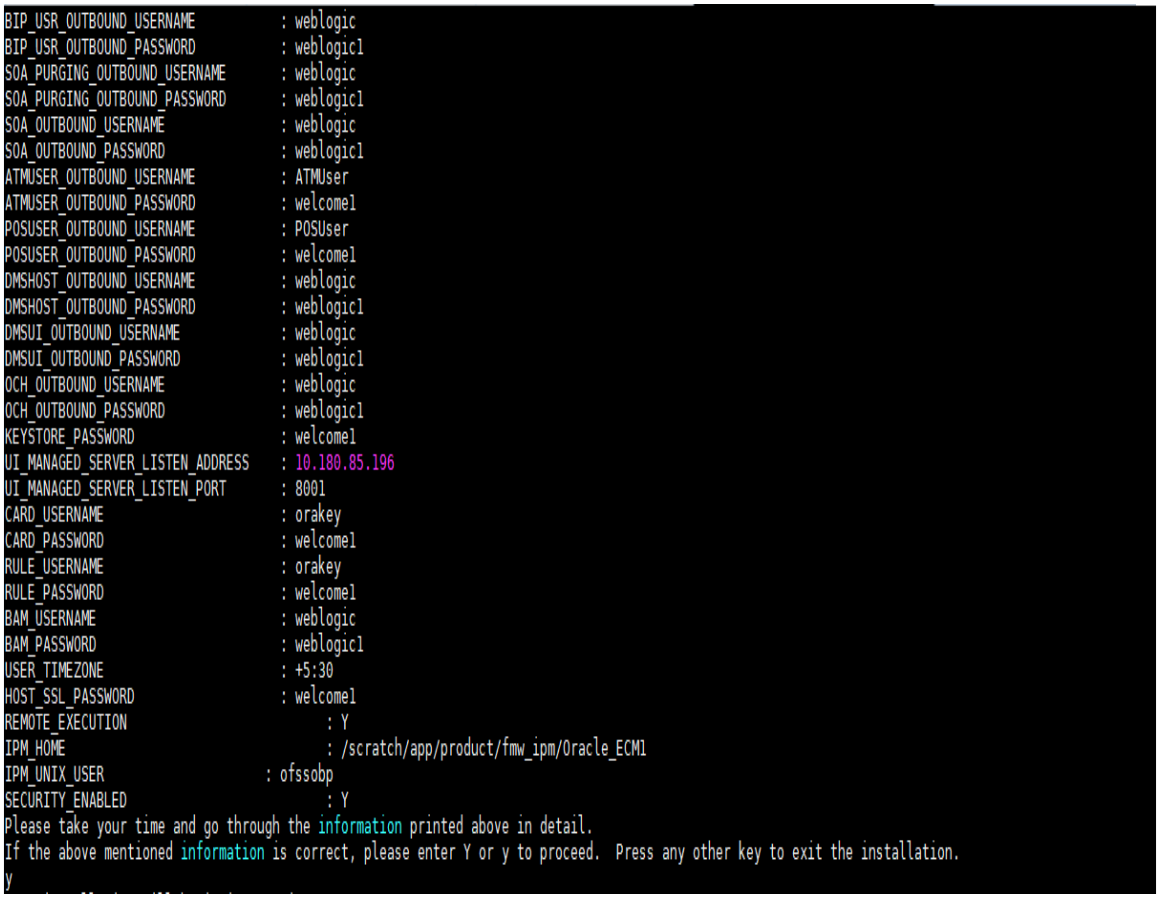


Figure 3–19 Host Domain Post Installation Script Execution (contd)

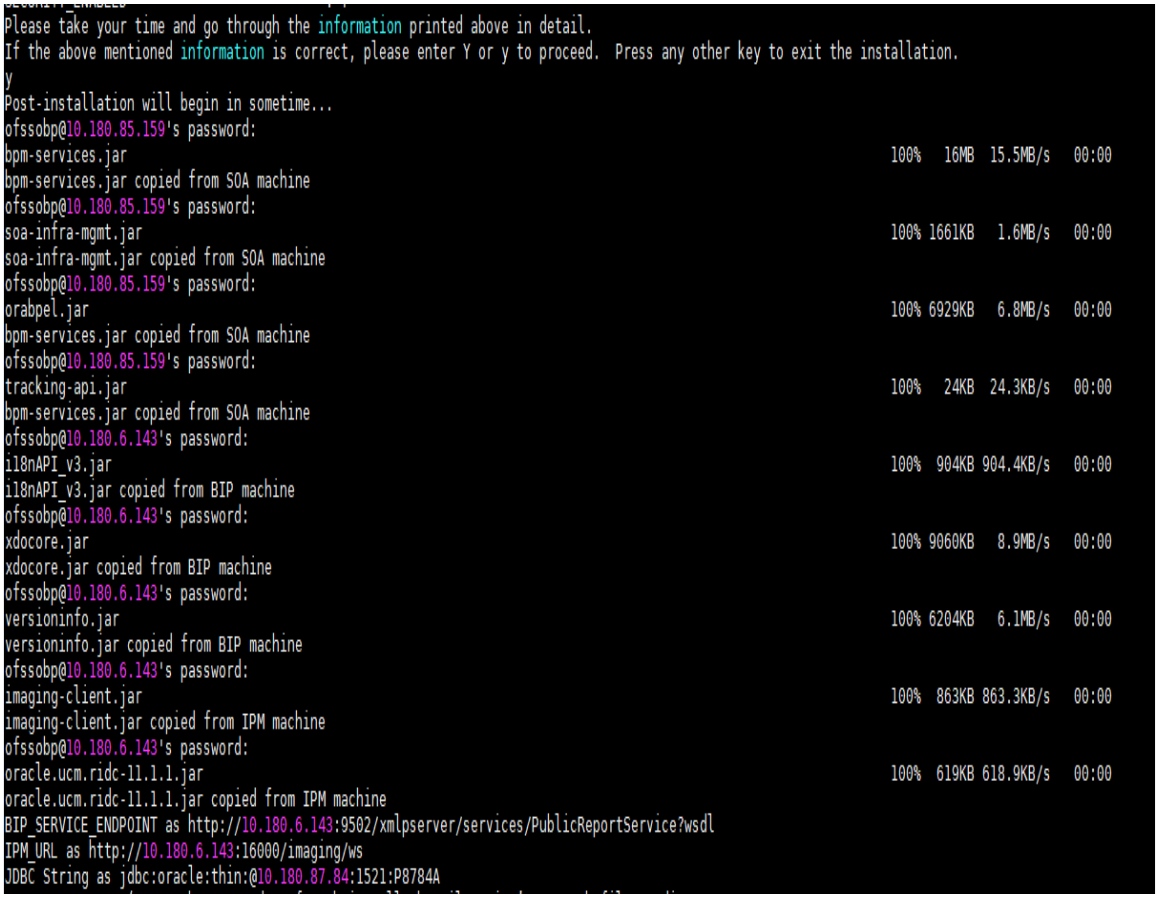
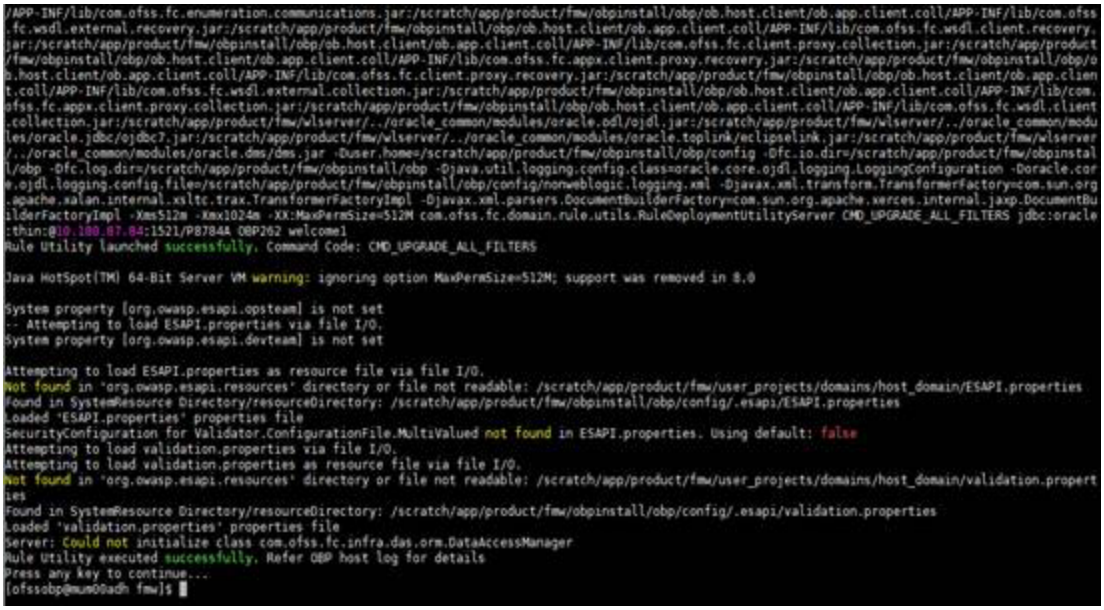


Figure 3–20 Host Domain Post Installation Script Execution Summary



Here, during the post installation part, at last execute the libovdadapterconfig script to create two adapters from the template. During execution, it will prompt for password. Pass weblogic console password (for example, weblogic1).

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. Then start the admin and managed servers to check the domain configuration status as described in verification part in Section 8.2 Host Domain Verification.

4 OBEDM US Localization Presentation Media Pack Installation

This chapter details every step involved in the installation of OBEDM US Localization Presentation (UI) Media pack. The subsequent section refers to the variable names specified in Section 2.2 Installation Checklist.

4.1 Installation and Configuration Procedure

This section details the installation procedure for the OBEDM US Localization Presentation Media Pack.

4.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBEDM 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 'obpus-ui.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 2.2 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 OBEDM US Localization Presentation Media Pack installation. The procedure can be started after HOST 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:

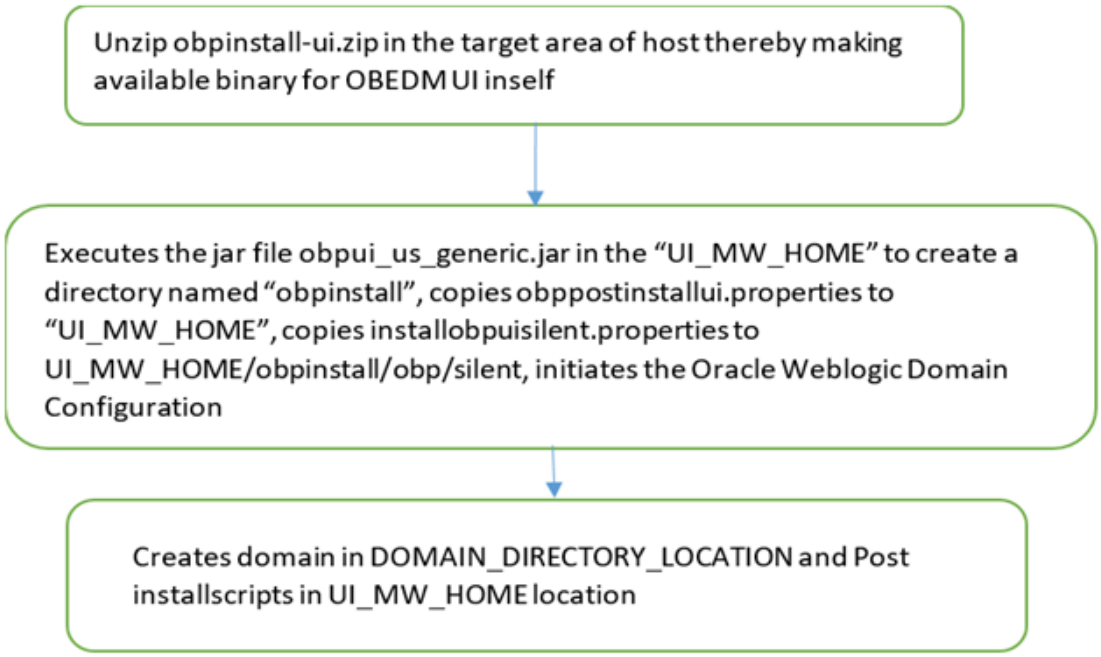
- Make sure required RCU schemas have been created. For more information, see Section 5.1 Pre-Installation Steps and Section 5.2 OBEDM Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against UI_TARGET 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.

4.1.3 Installation Steps

This section lists the installation steps required for the OBEDM 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 4–1 Steps in installobpui.sh script



A sample output is given here.

Figure 4–2 Confirmation to Proceed Domain Installation

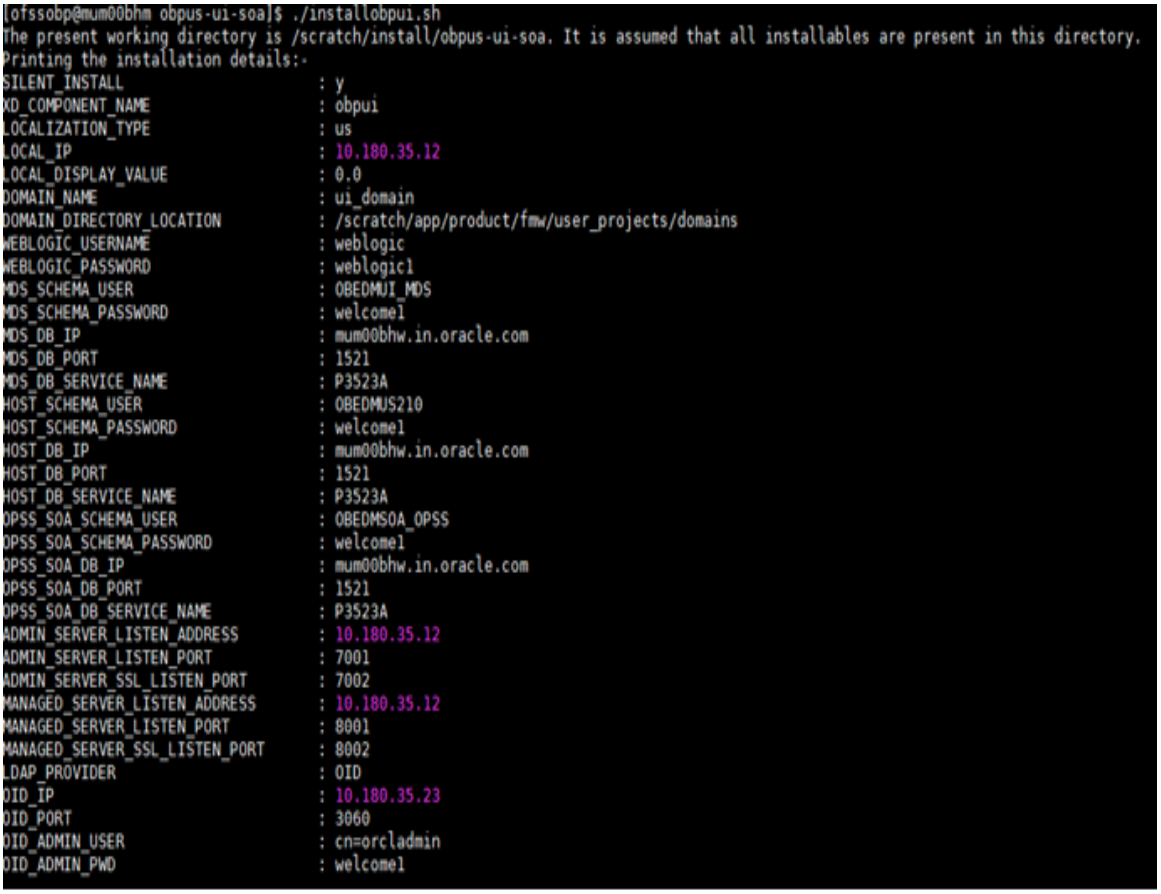


Figure 4–3 Confirmation to Proceed Domain Installation (contd)

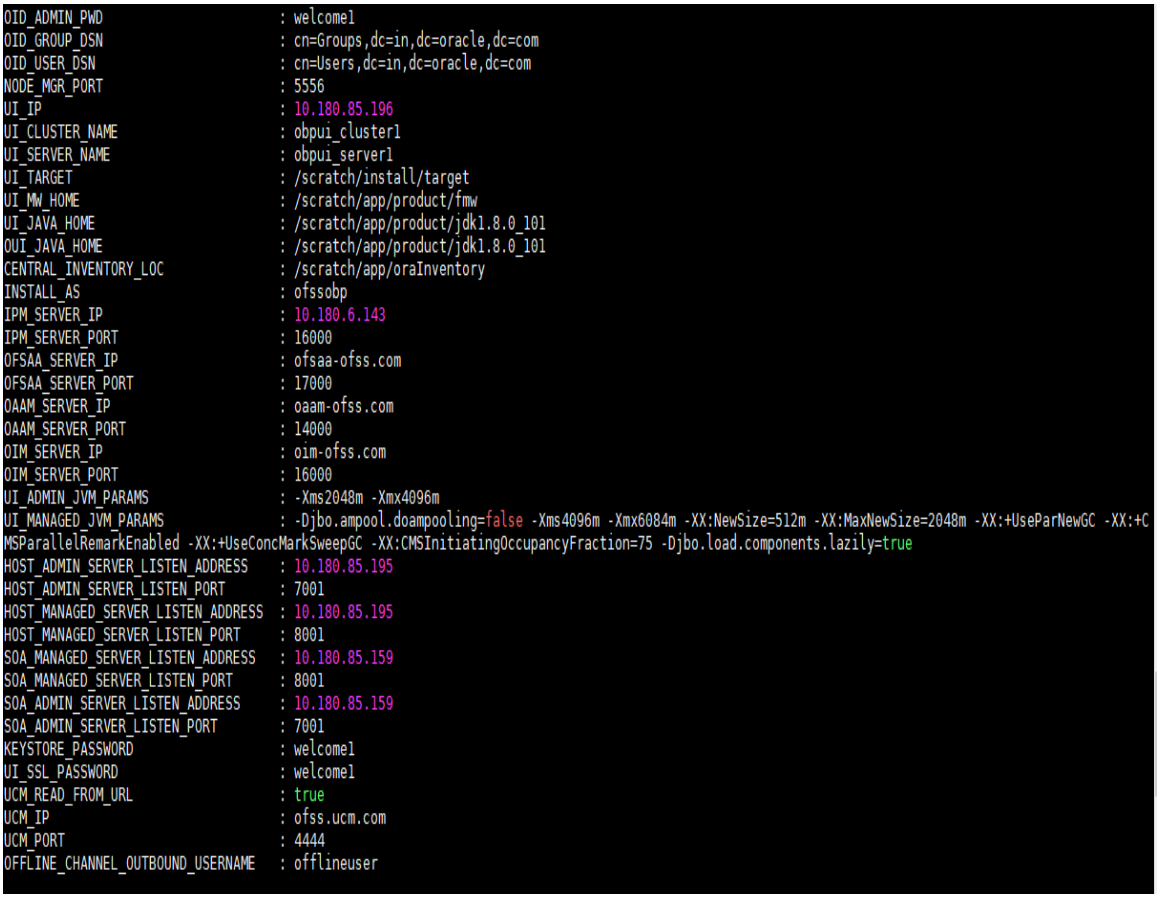
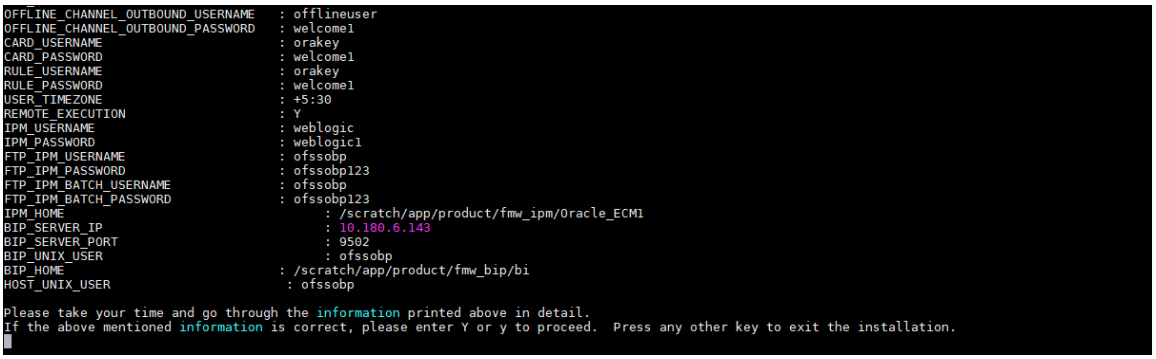


Figure 4–4 Confirmation to Proceed Domain Installation (contd)



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 4–5 Copying and Extraction of obpinstall-ui.zip

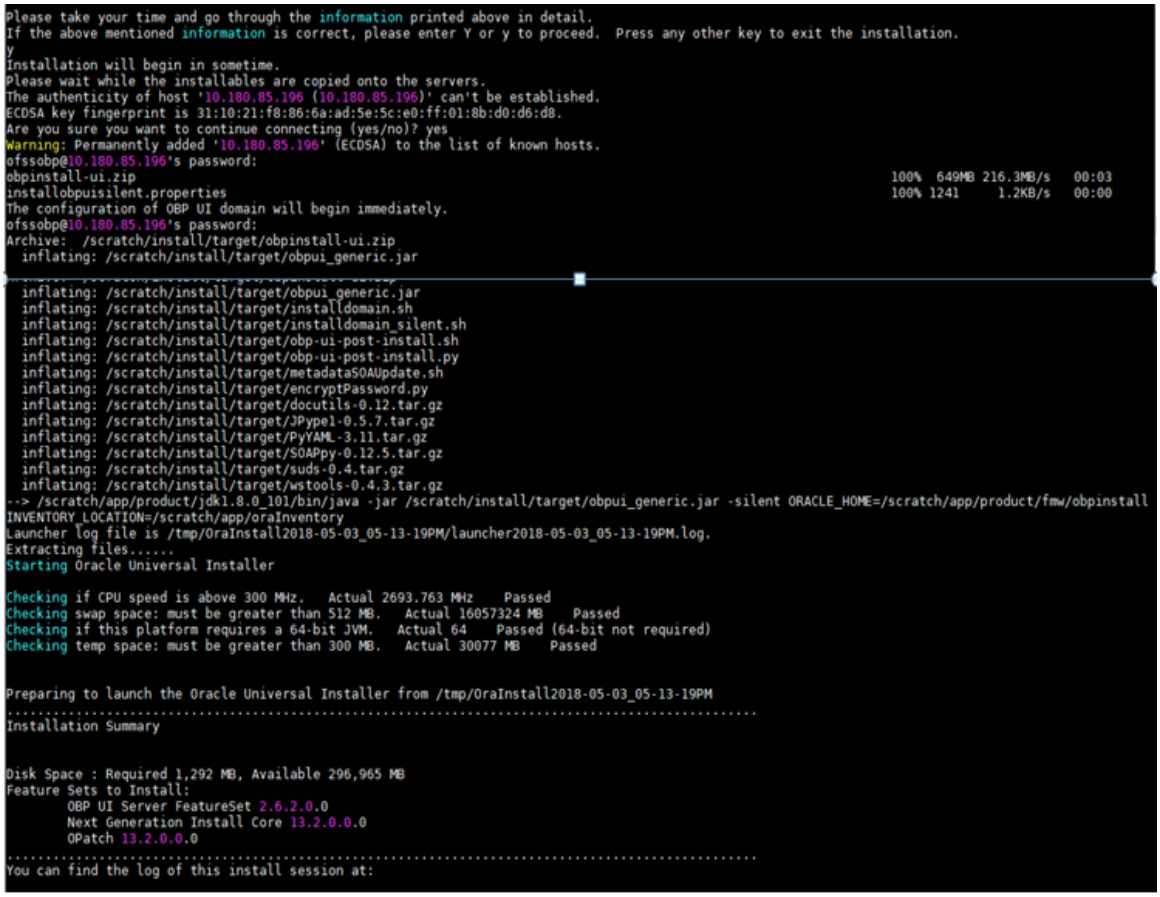


Figure 4–6 Copying and Extraction of obpinstall-ui.zip (contd)

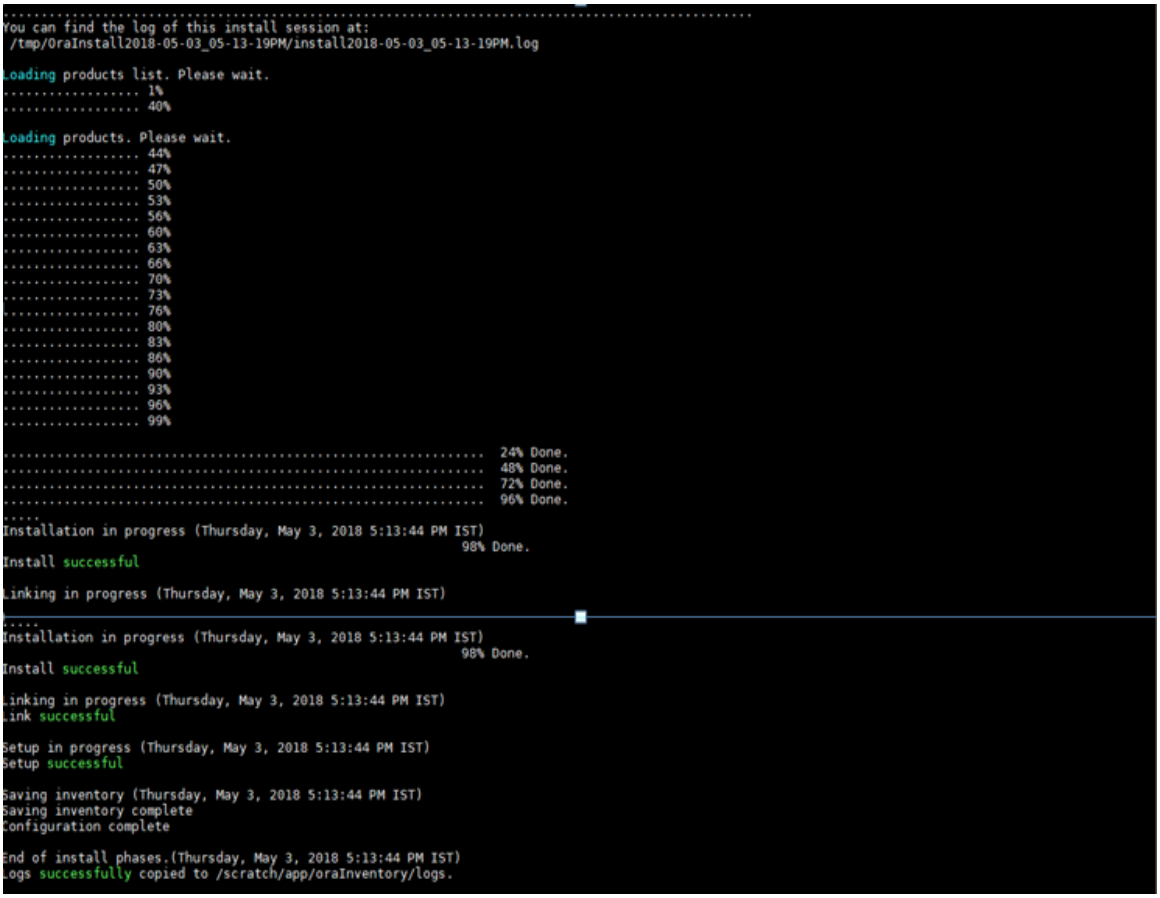
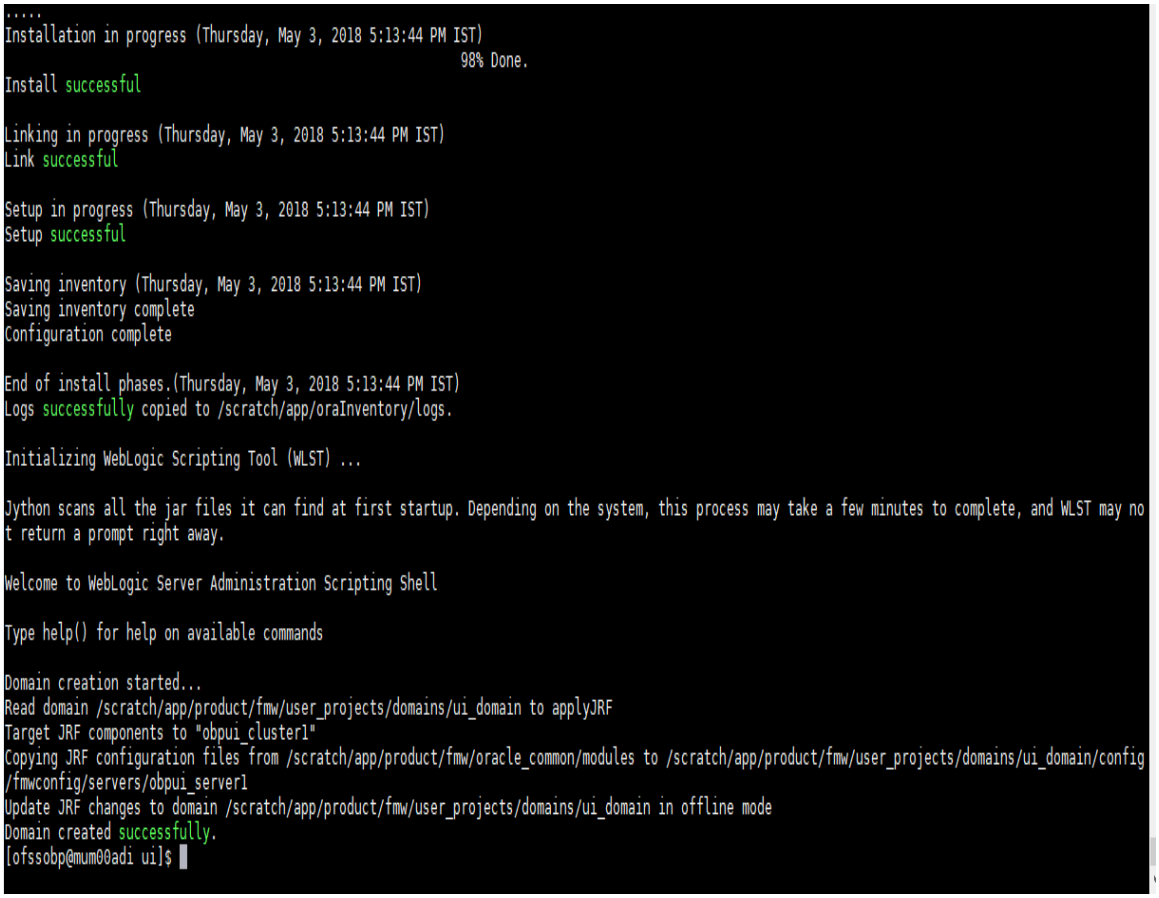


Figure 4–7 Domain Creation Confirmation



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 4.2 Post Installation Configuration.

4.2 Post Installation Configuration

This section describes the post installation configuration procedure for OBEDM 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 4–8 UI Admin Server Credentials

Figure 4–9 UI Admin Server Running

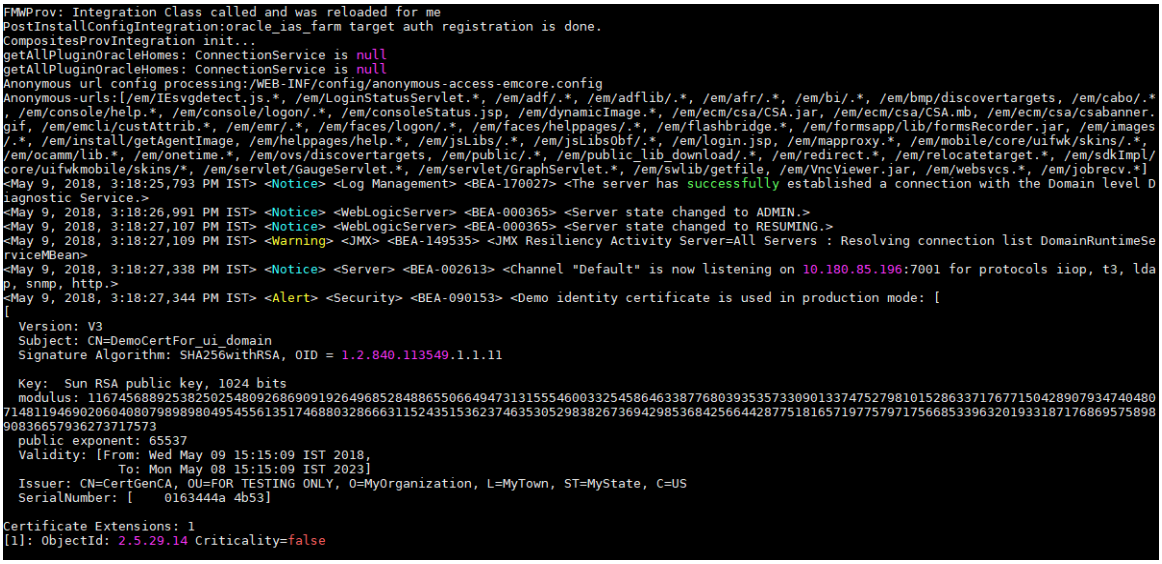


Figure 4–10 UI Admin Server Running (contd)

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 4–11 Starting Post Installation

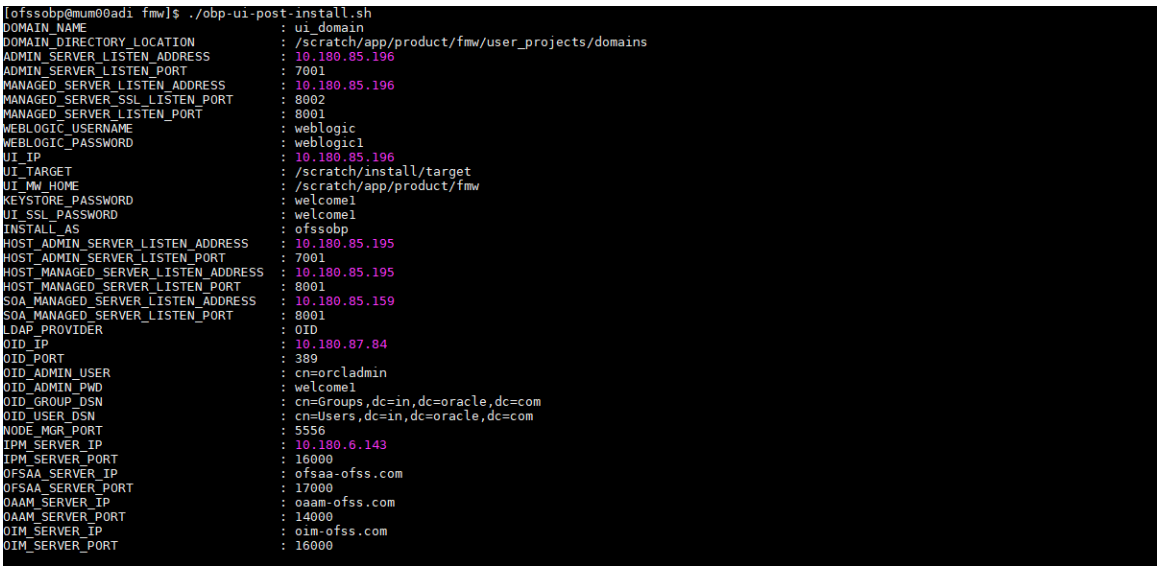


Figure 4–12 Starting Post Installation (contd)

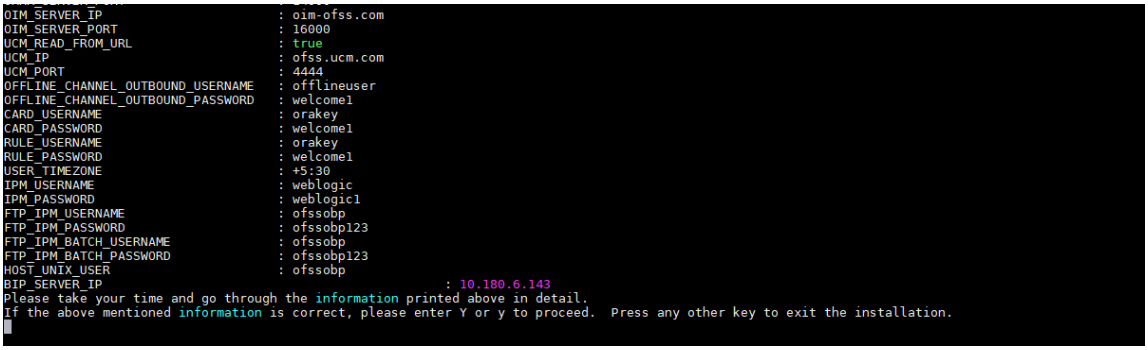


Figure 4–13 Continuation of Post-Installation

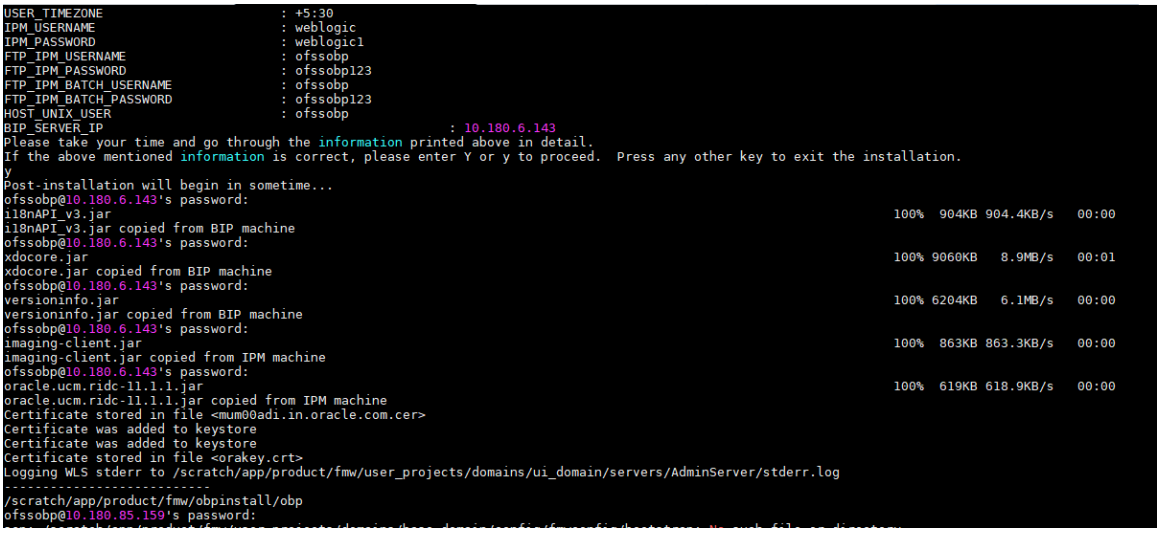
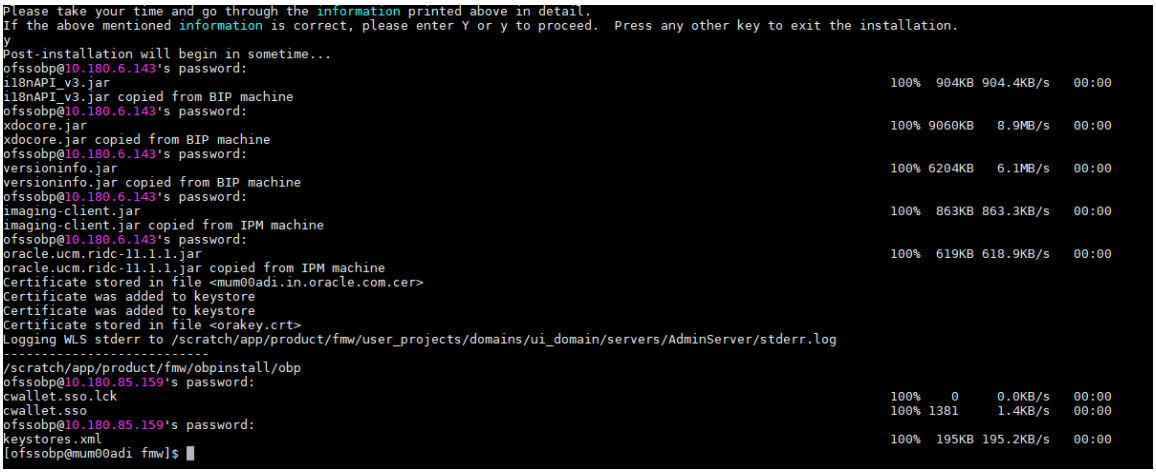


Figure 4–14 Continuation of Post-Installation (contd)



Here during post installation part, at last execute the libovdadapterconfig script to create two adapters from the template. During execution, it will prompt for password. Pass weblogic console password (for example, weblogic1).

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. Restart UI admin and UI managed server.

5 Standalone Database Setup

This chapter details the steps involved in OBEDM US Localization database which are primarily concerned with importing an existing database dump of the QA database.

5.1 Pre-Installation Steps

The following steps should be completed prior to the process of executing the installation steps for the OBEDM DB mentioned in Section 5.2 OBEDM Database Setup – RCU Installation:

1. Oracle Database Enterprise Edition 19c must be installed on the database server.
2. Obtain the tar file dbScripts_us.tar.gz from OBEDM Host media pack (dbScripts_us.tar.gz is present in obpus-host.zip) and copy it onto the database server.
3. Ensure that the ONS service is started after DB installation.

5.2 OBEDM Database Setup – RCU Installation

The steps that should be performed to create the OBEDM Host DB schema are provided in Section 5.3.1 Host DB Schema Creation and Verification

For other RCU schemas, while installing software on HOST and UI, specific RCU should execute to create schemas for 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 UI and HOST, respectively (please note, UI and HOST are the prefix in below schemas which is given during schema creation).

- UI_STB
- UI_OPSS
- UI_MDS
- UI_IAU_APPEND
- UI_IAU_VIEWER

- HOST_STB
- HOST_OPSS
- HOST_IAU_APPEND
- HOST_IAU_VIEWER
- HOST_MDS

UI_MDS and UI_STB schemas are used by UI component.

HOST_MDS and HOST_STB schemas are used by HOST component.

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

HOST_OPSS, HOST_IAU_APPEND and HOST_IAU_VIEWER schemas are shared by UI also pointed during post installation of HOST and UI.

5.3 OBEDM 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.

5.3.1 Host DB Schema Creation and Verification

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

Untar dbScripts_us.tar.gz 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
```

5.3.2 HOST DB schema ddl execution

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 which 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_OBEDM/welcome1@OBEDMDB
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 OBEDM tables are present.

5.3.3 HOST DB Schema Seeding

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_OBEDM/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 OBEDM DB seeding is completed, the control will return to the sql prompt.

5.3.4 System Configuration DB Update Script Execution

After the host db schema has been created successfully, copy the 'updateSystemDetails.sql' file from 'HOST_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_OBEDM@welcome1@OBEDMDB
D:\seed >@updateSystemDetails.sql
```

After above sql execution, execute following queries in application schema (i.e. DEV_ OBEDM@welcome1@OBEDMDB.

For enabling Local Policy Store instead of OPSS:

UPDATE FLX_FW_CONFIG_ALL_B SET PROP_VALUE = 'SQL' WHERE CATEGORY_ID = 'SecurityConstants'

AND PROP_ID = 'AuthorizationServiceProvider';

Figure 5–1 Enable Local Policy Store

For enabling local role based menu:

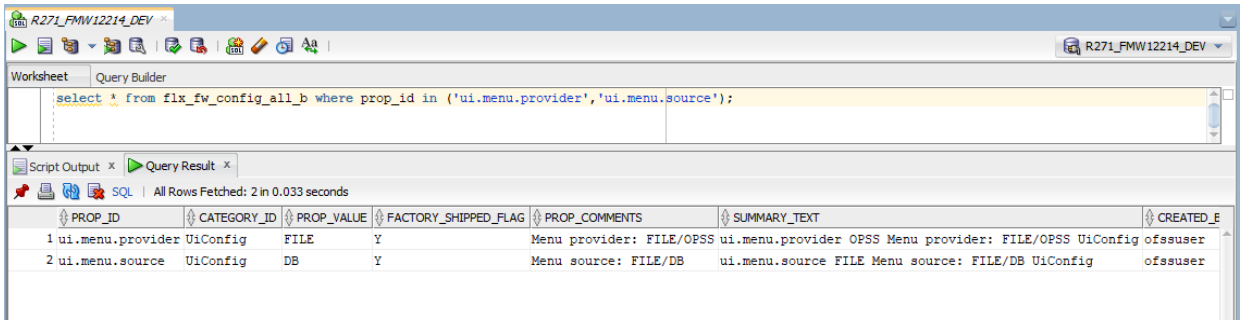
UPDATE flx_fw_config_all_b SET prop_value = 'FILE' WHERE prop_id = 'ui.menu.provider';

UPDATE flx_fw_config_all_b SET prop_value = 'DB' WHERE prop_id = 'ui.menu.source';

Verify using below query:

Select * from flx_fw_config_all_b WHERE prop_id IN ('ui.menu.provider','ui.menu.source');

Figure 5–2 Enable Local Role Based Menu



6 OBEDM and IPM Integration

This chapter details the steps involved in the integration of Oracle Banking Enterprise Default Management and Oracle Imaging and Process Management (IPM).

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

- Section 6.1 IPM Application Setup for OBEDM Content Management
- Section 6.2 IPM Report Upload Setup

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

6.1 IPM Application Setup for OBEDM Content Management

This is a mandatory configuration required on IPM to enable integration of OBEDM 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.

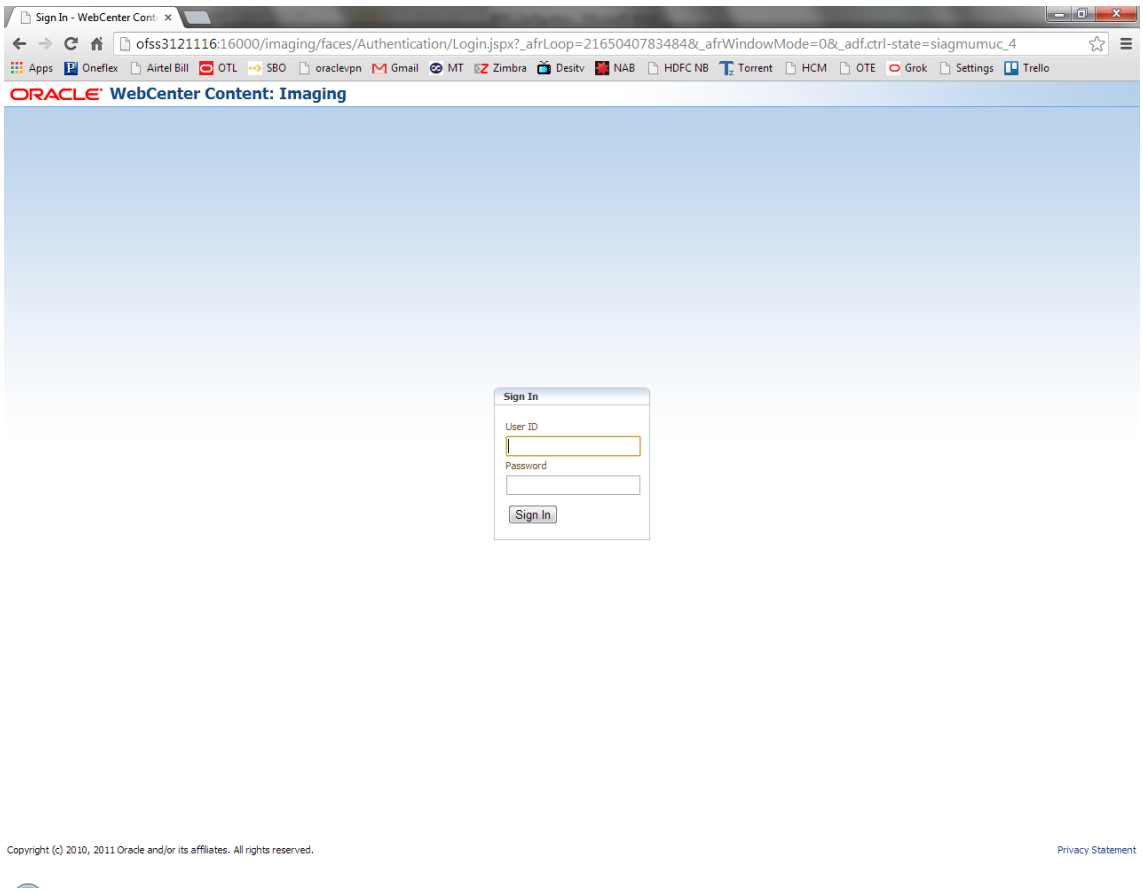
6.1.1 UCM Connection

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:

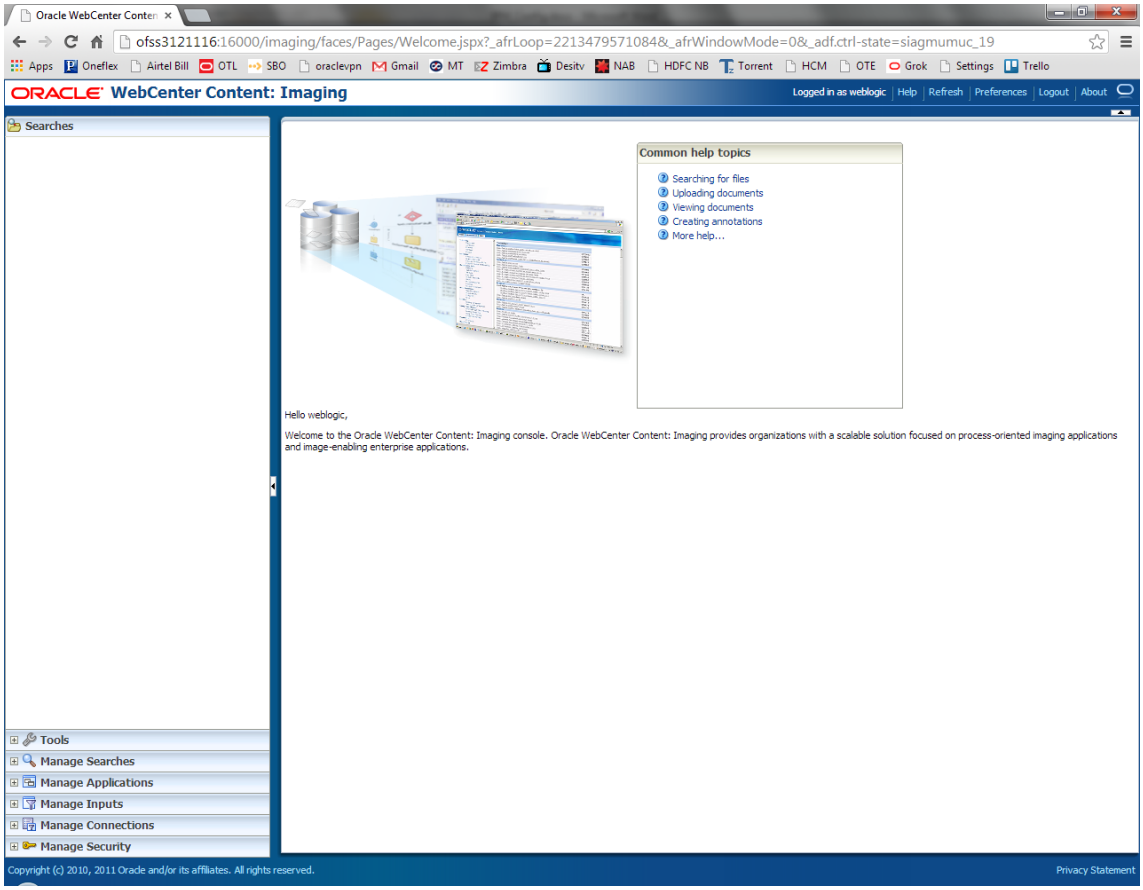
   http:// hostname:16000/imaging

Figure 6–1 IPM Imaging Console - Login page



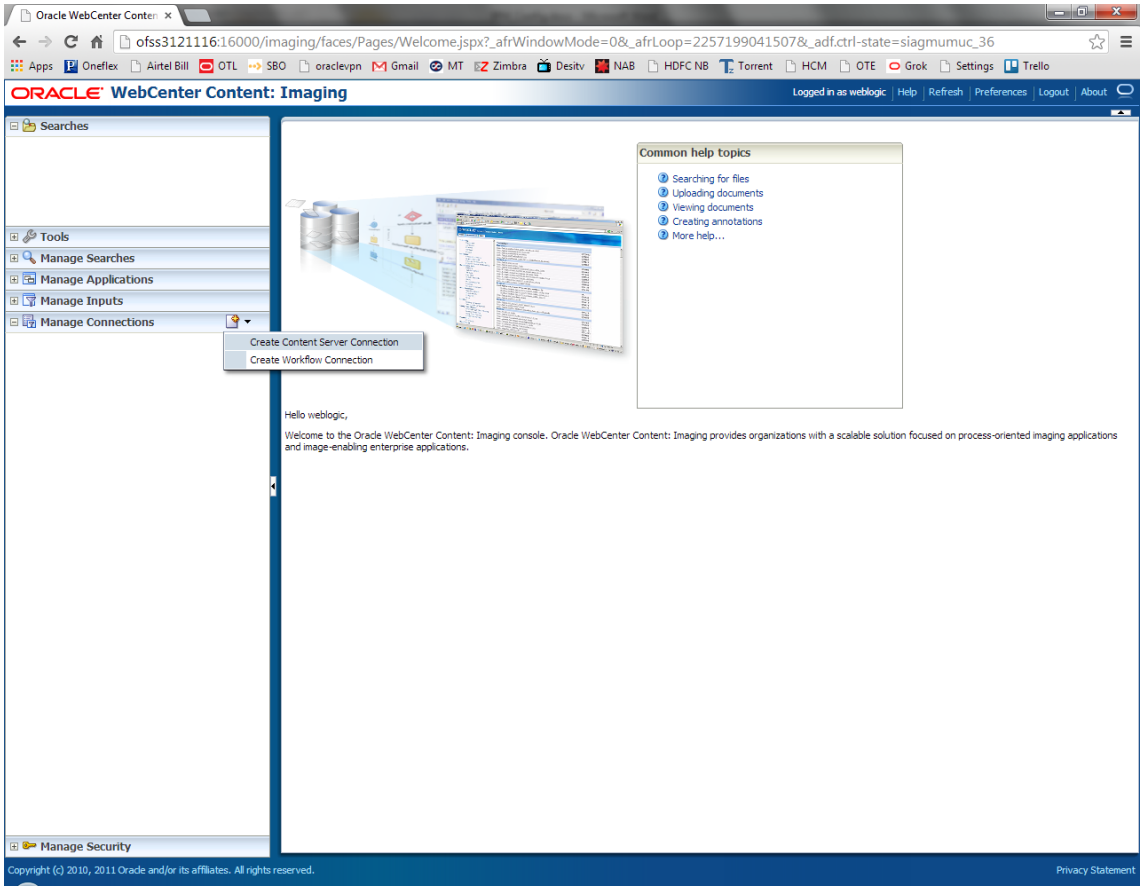
2. Enter the user ID and password set during IPM installation.

Figure 6–2 IPM - Welcome page



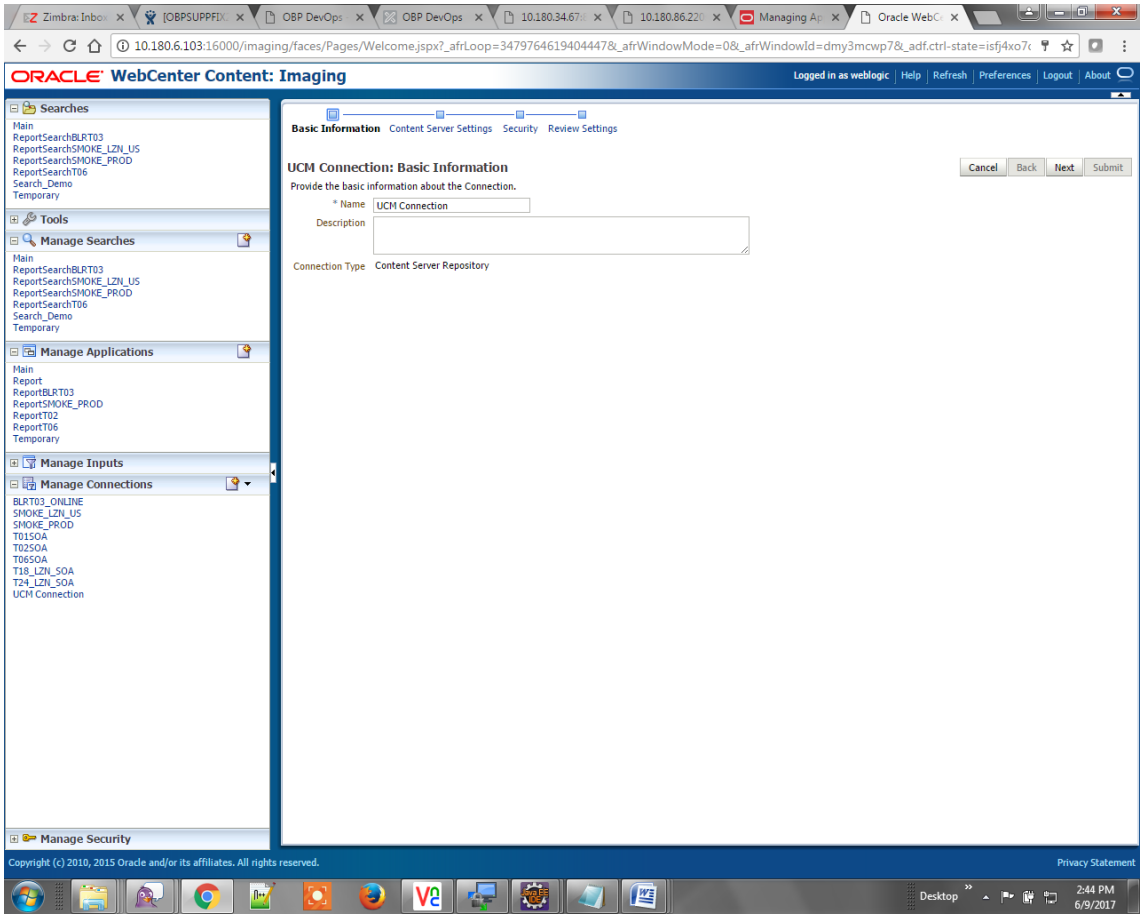
3. Navigate to Manage Connection and select Create Content Server Connection.

Figure 6–3 Create Content Server Connection



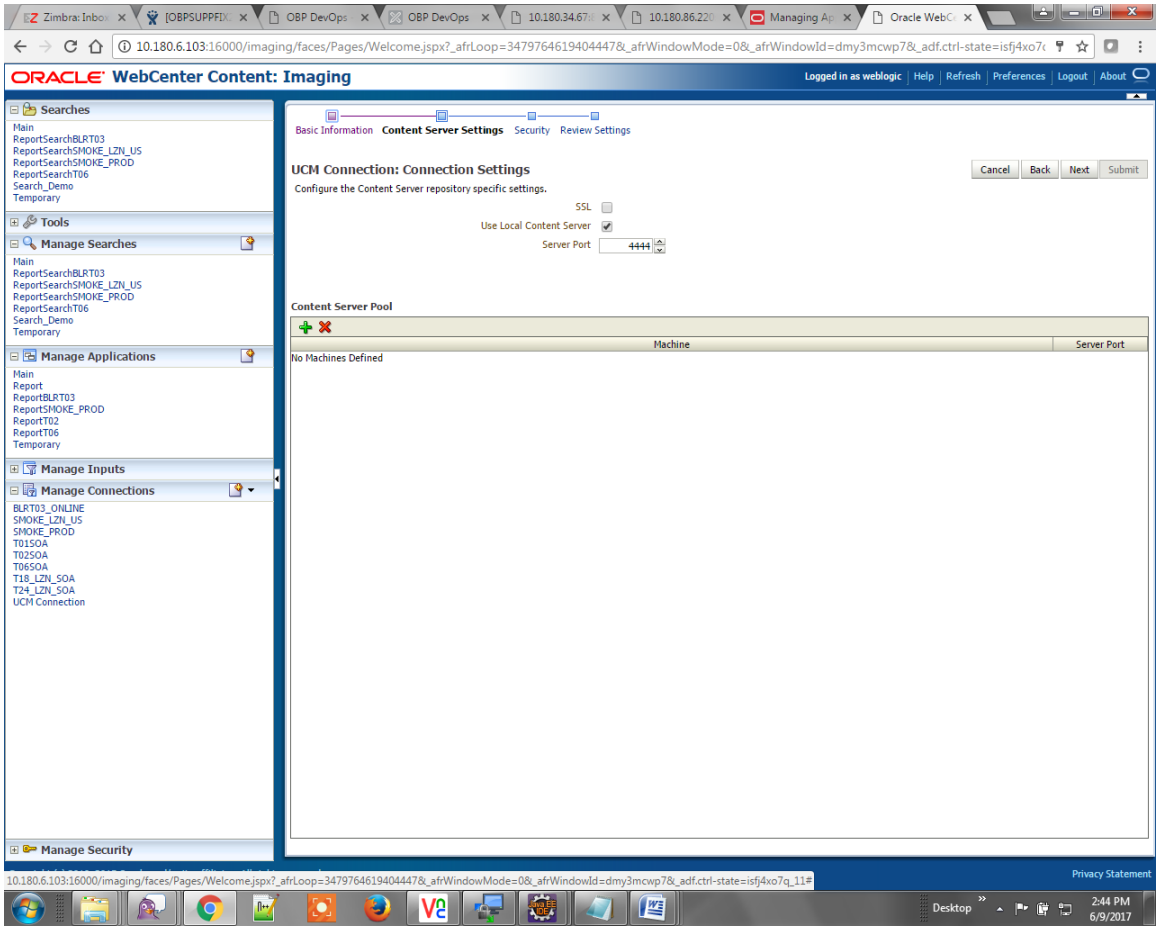
4. In the Basic Information stage, enter the name and description for Content Server Connection as UCM Connection and click Next.

Figure 6–4 UCM: Basic information



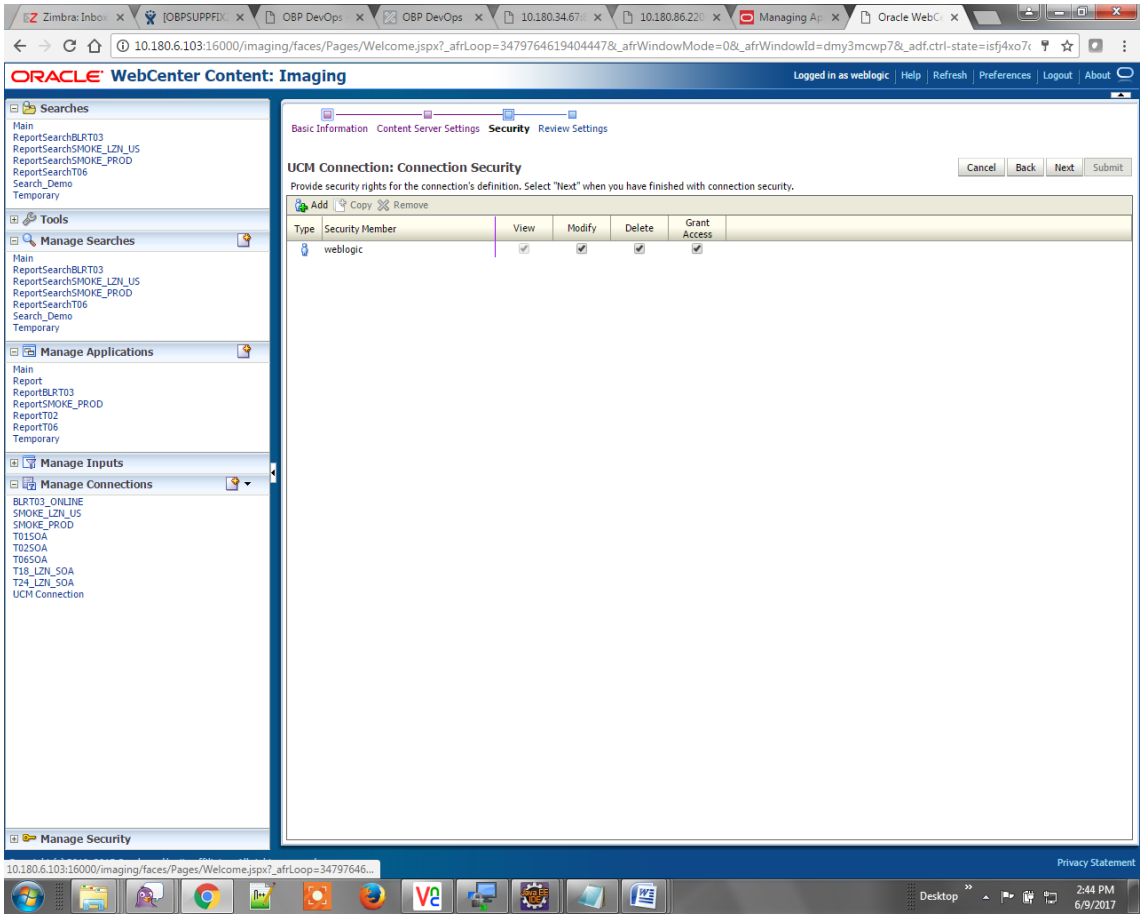
5. In the Content Server Settings page, select the Use Local Content Server check box and select the Server Port as 4444. Click Next.

Figure 6–5 UCM: Connection Settings



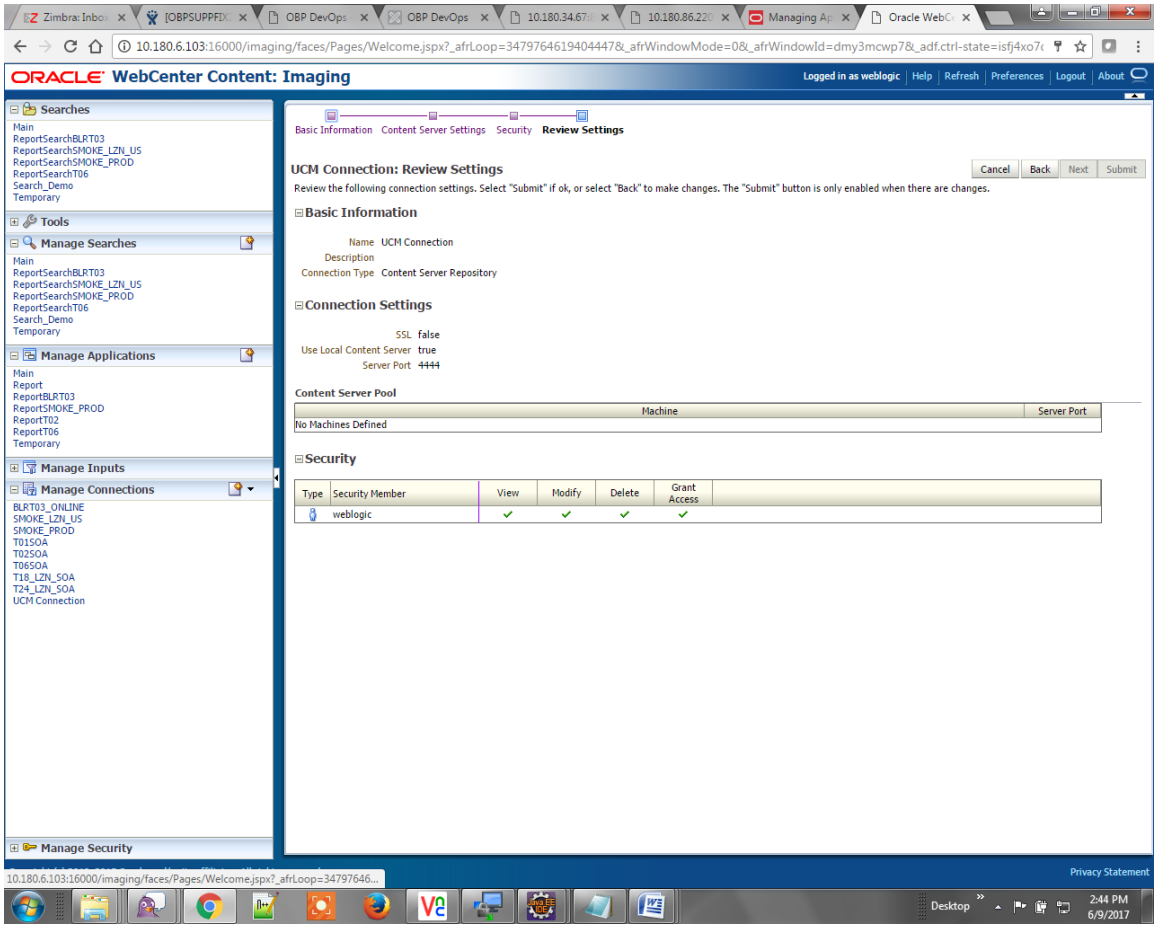
6. In the Security stage, select security rights for connection definition as shown below and click Next. If weblogic security member is not present, create it by clicking Add.

Figure 6–6 UCM: Connection Security



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

Figure 6–7 UCM: Review Settings



6.1.2 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.

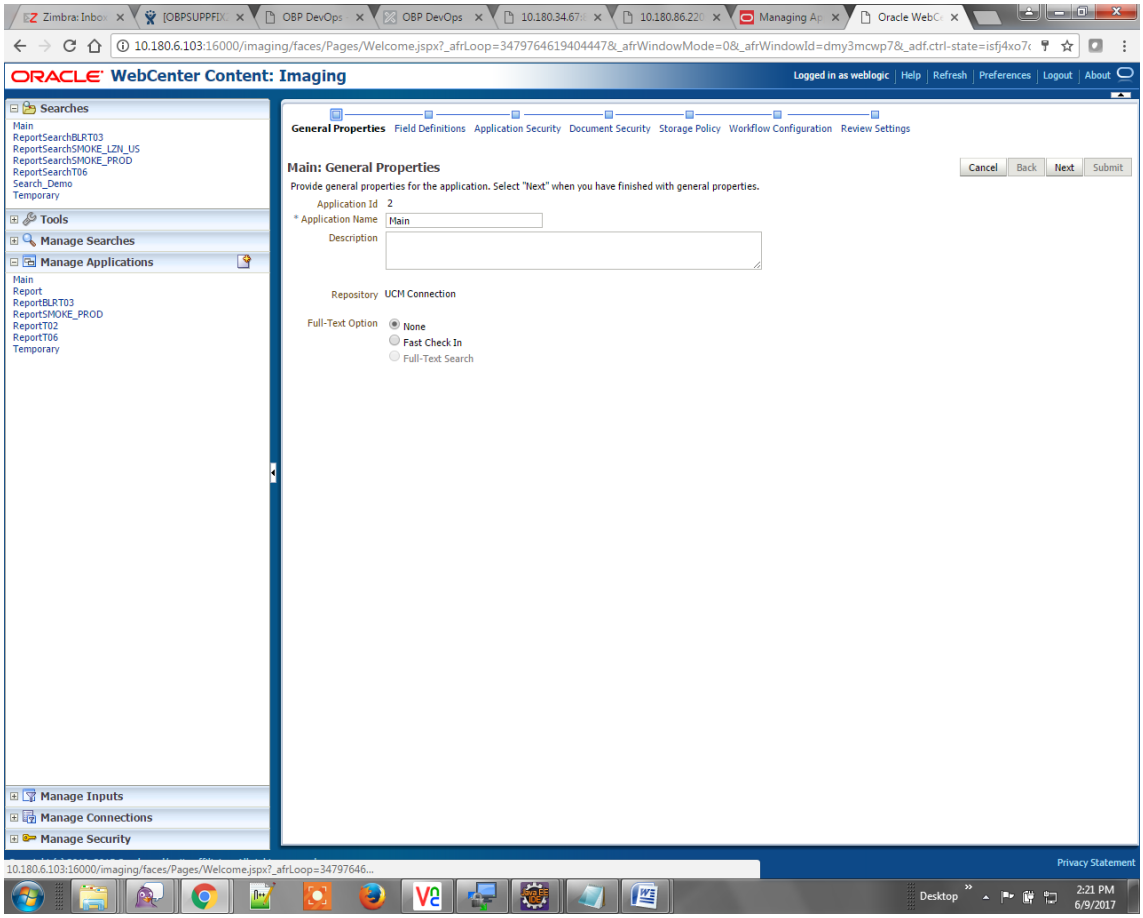
Create a main application and a temporary application in IPM.

6.1.2.1 Manage Application Configuration

To manage application configuration:

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

Figure 6–8 Main: General Properties



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

Figure 6–9 Main: Field Definitions

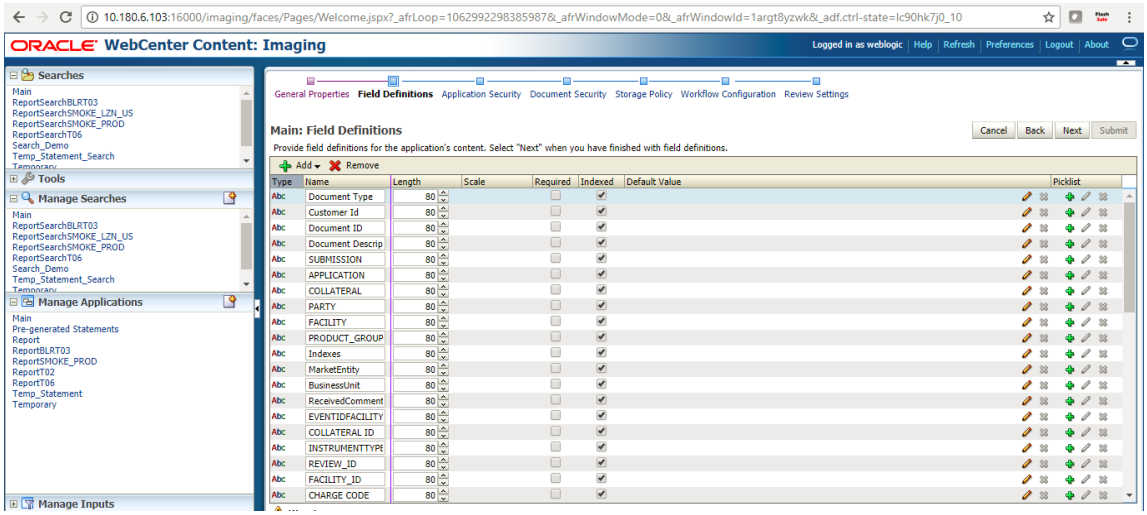
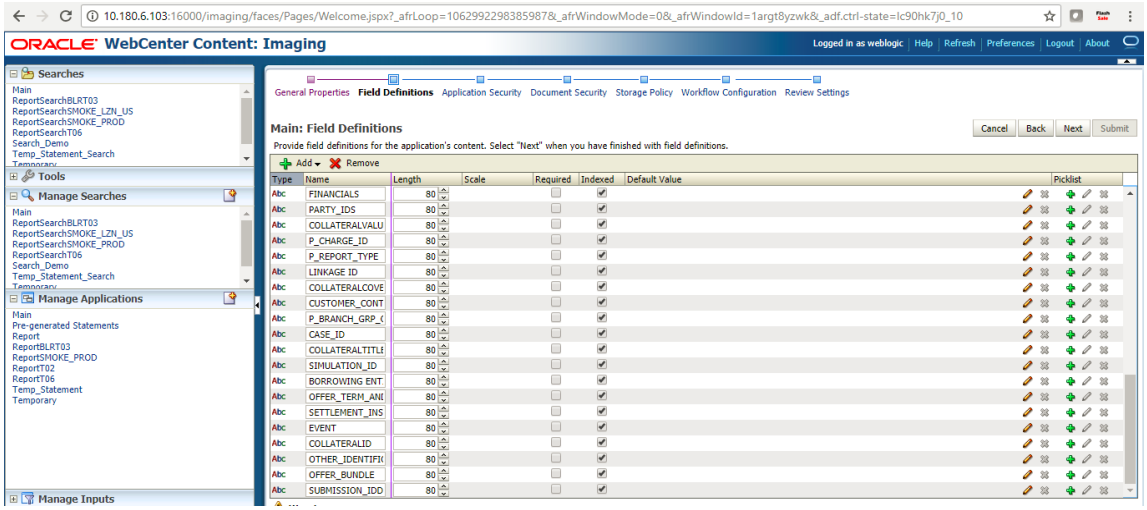


Figure 6–10 Field Definitions (cont.)



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

Figure 6–11 Main: Application Security

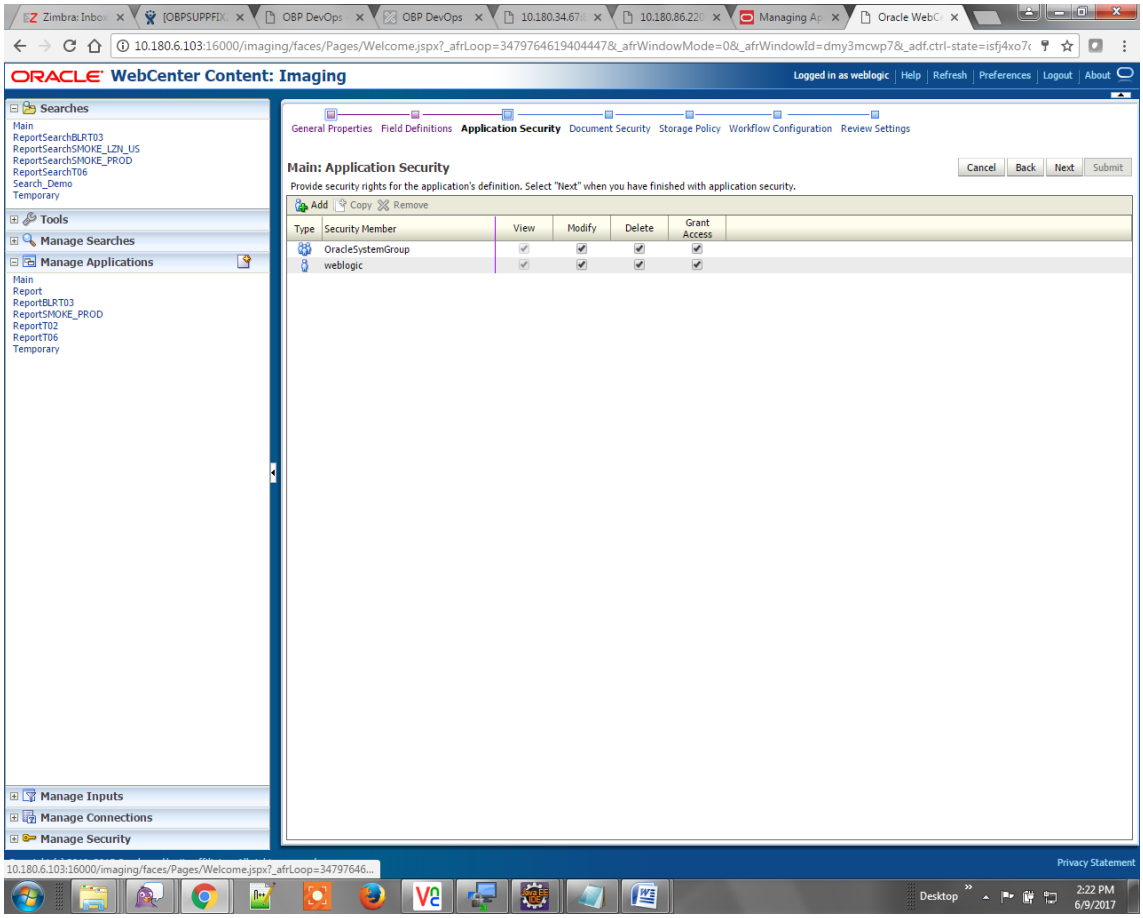
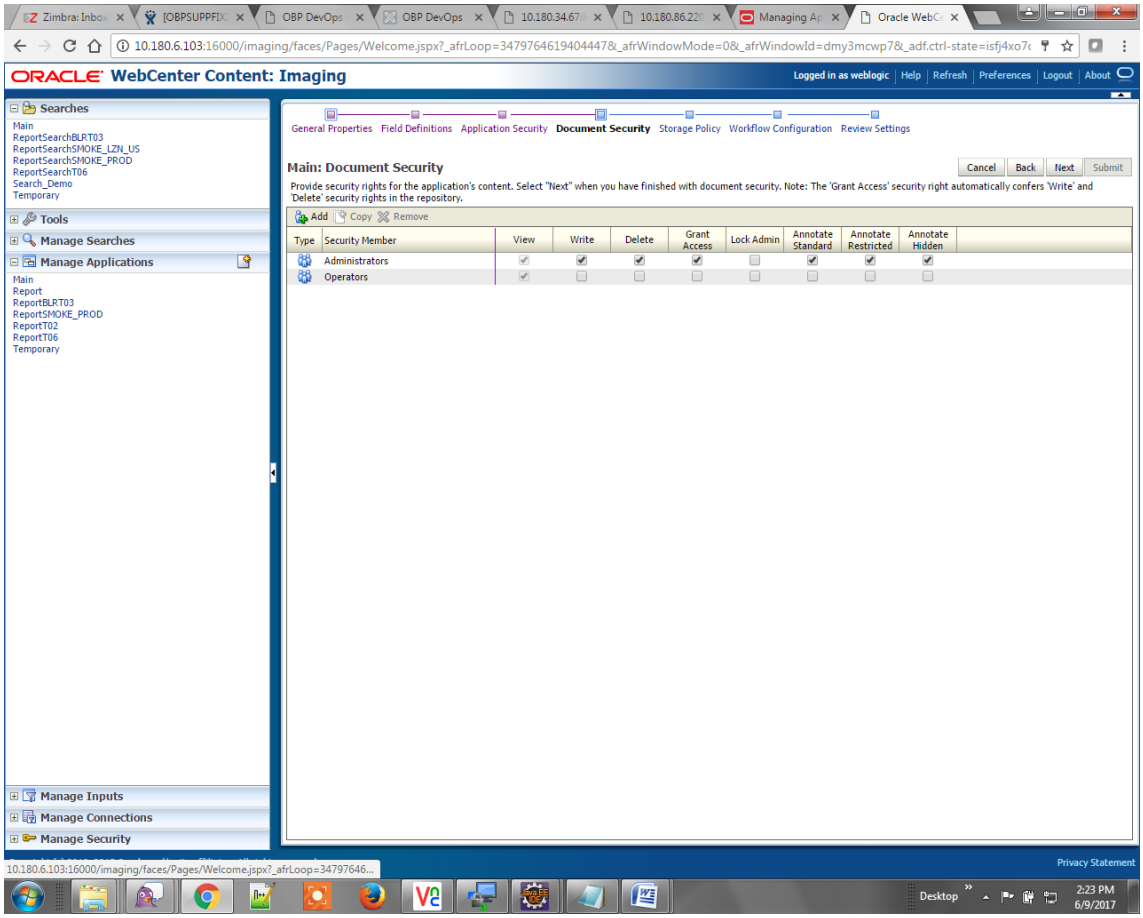
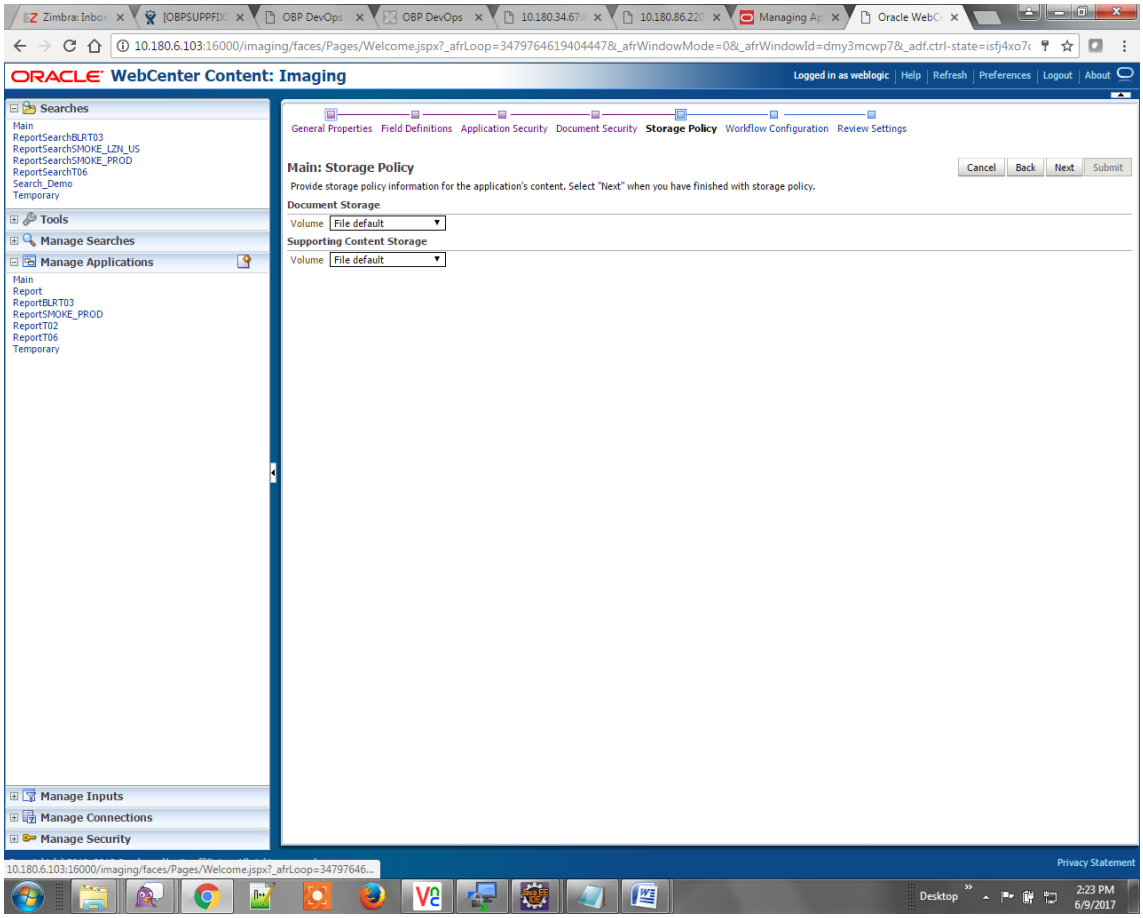


Figure 6–12 Main: Document Security



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

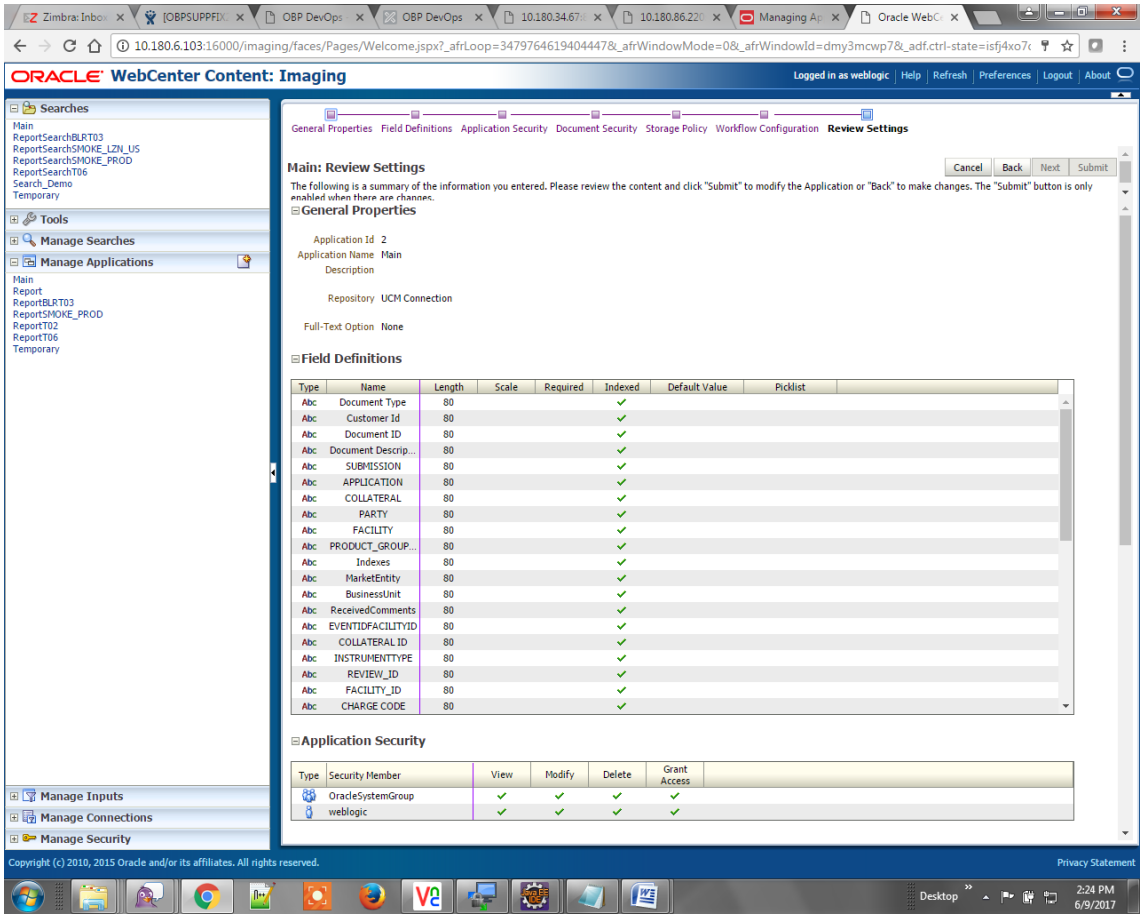
Figure 6–13 Main: Storage Policy



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

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

Figure 6–14 Main: Review Settings

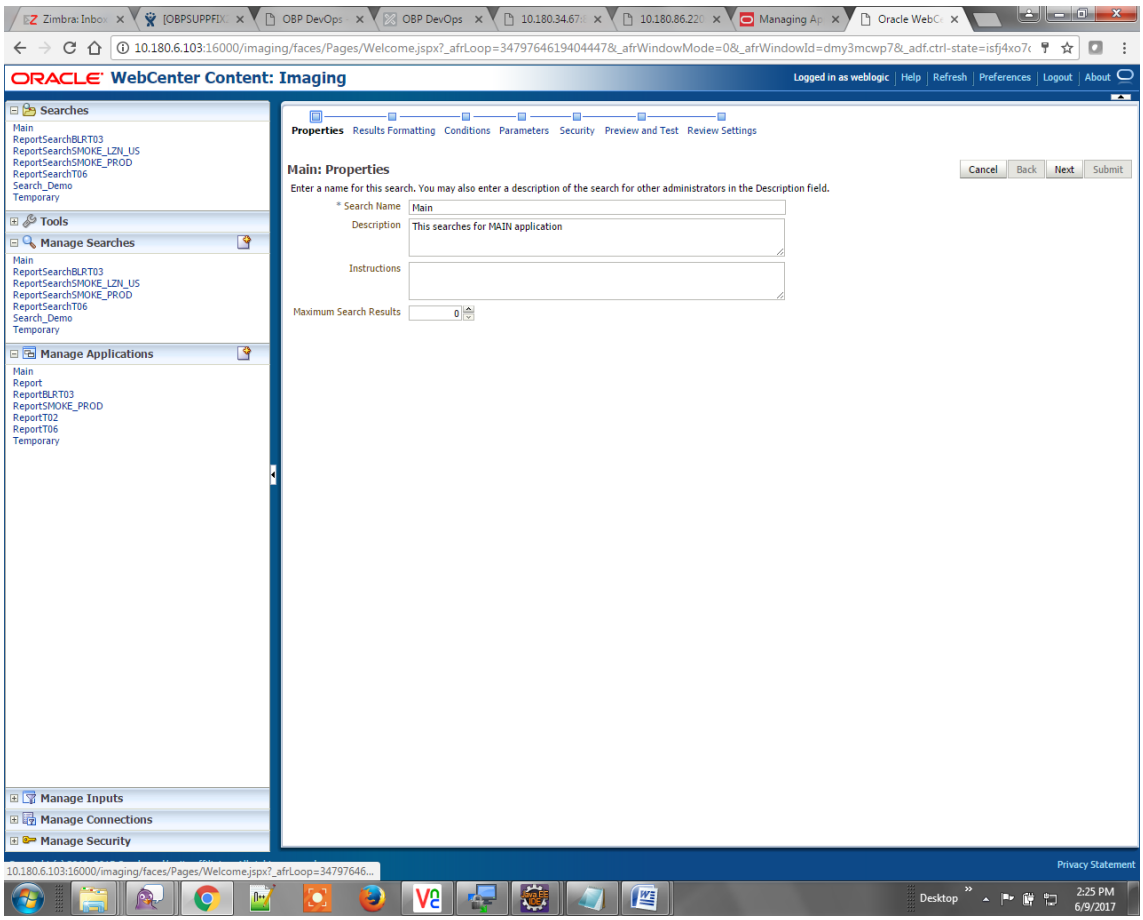


6.1.2.2 Manage Searches

To manage searches:

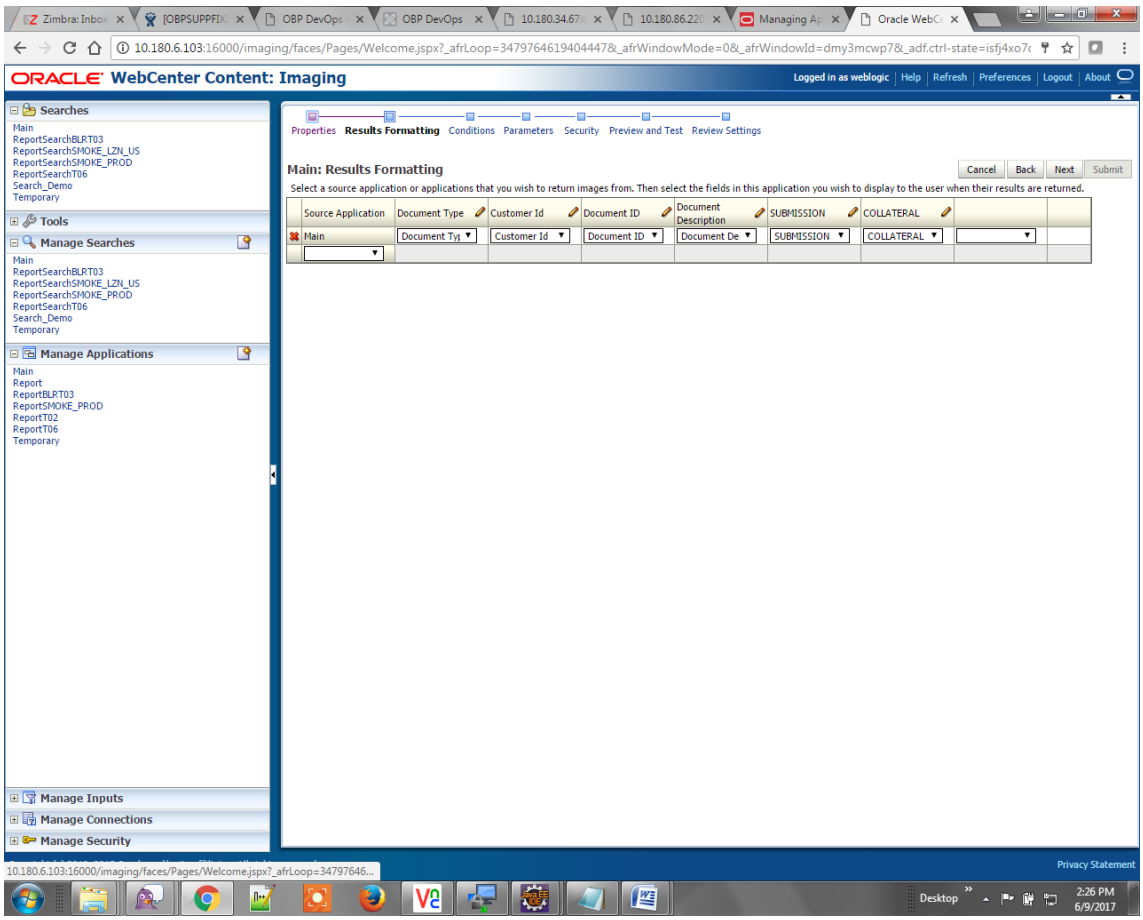
1. Click Manage Searches option and enter the search name with description.

Figure 6–15 Main: Properties



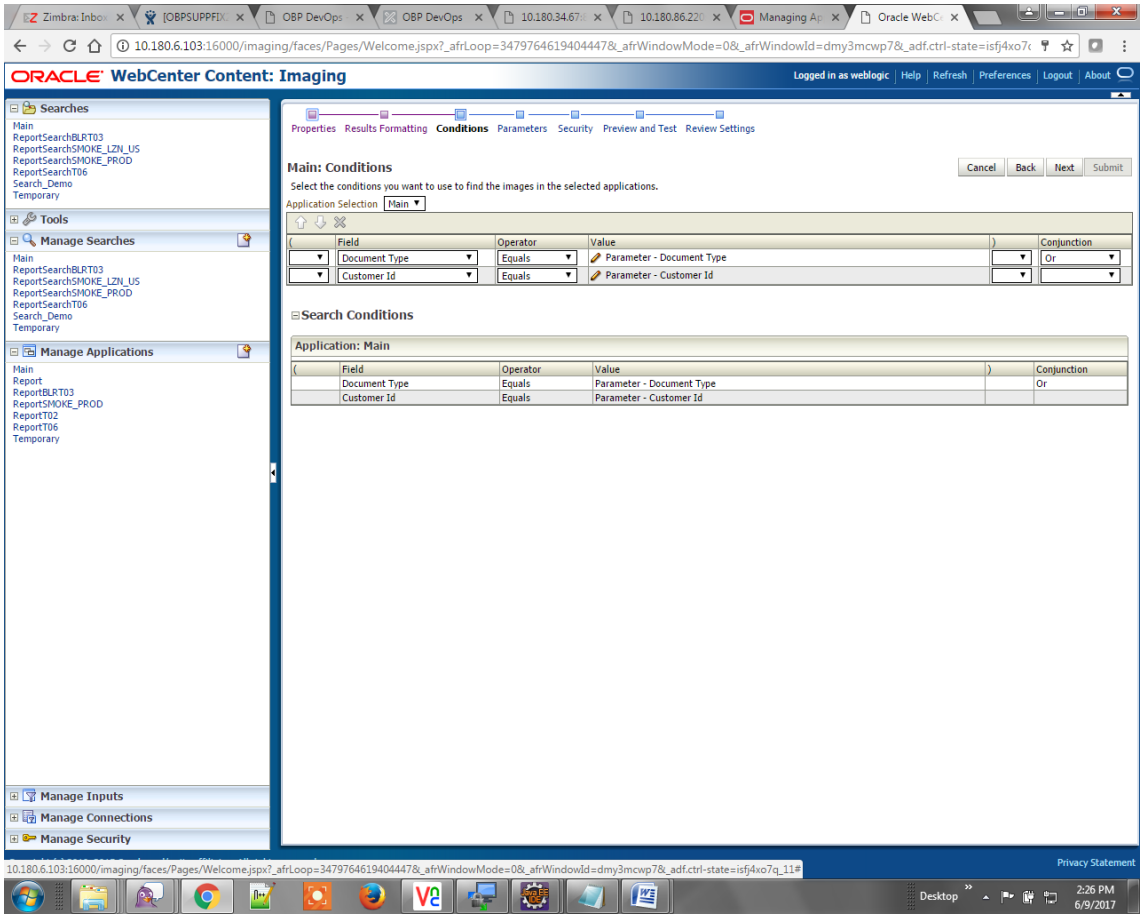
2. Click **Next.**
3. Select the source application along with its field details in the Results Formatting page.

Figure 6–16 Main: Results Formatting



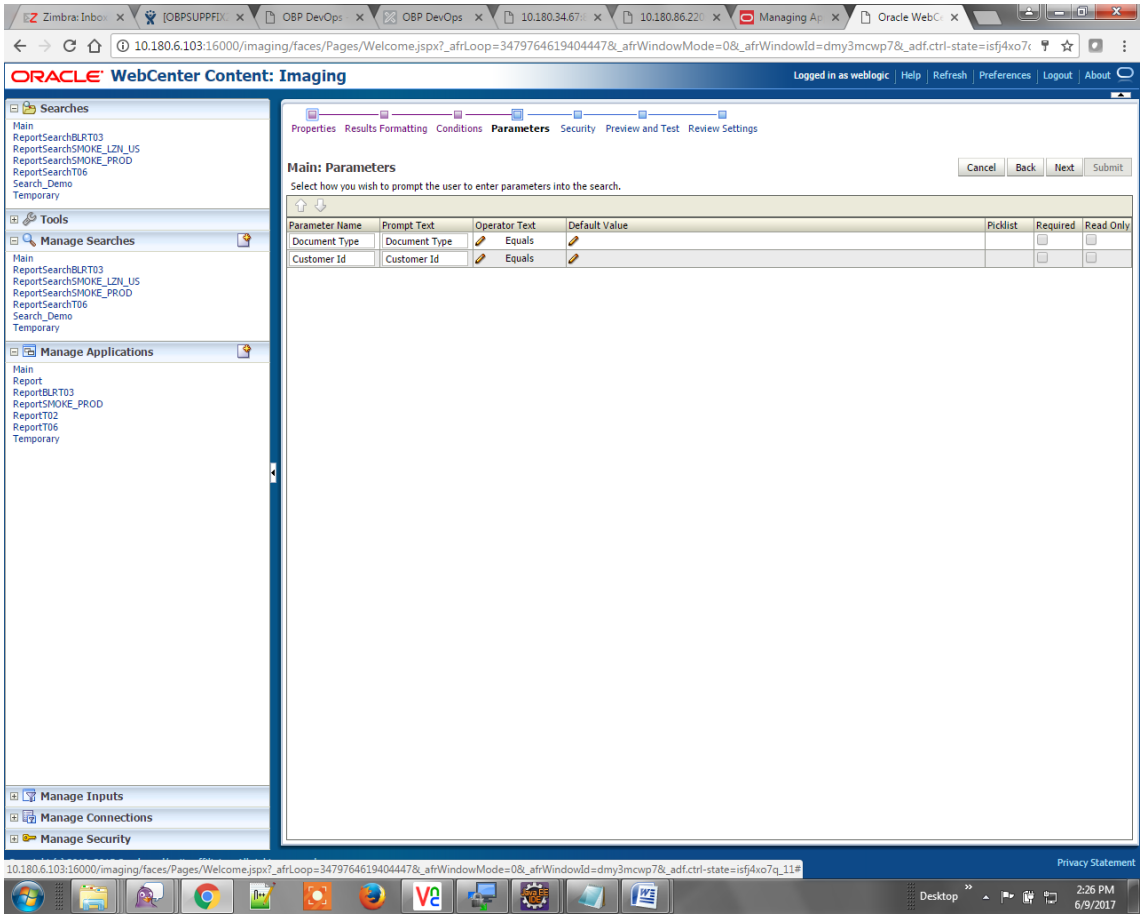
4. Select the appropriate conditions in the Conditions page as shown below.

Figure 6–17 Main: Conditions



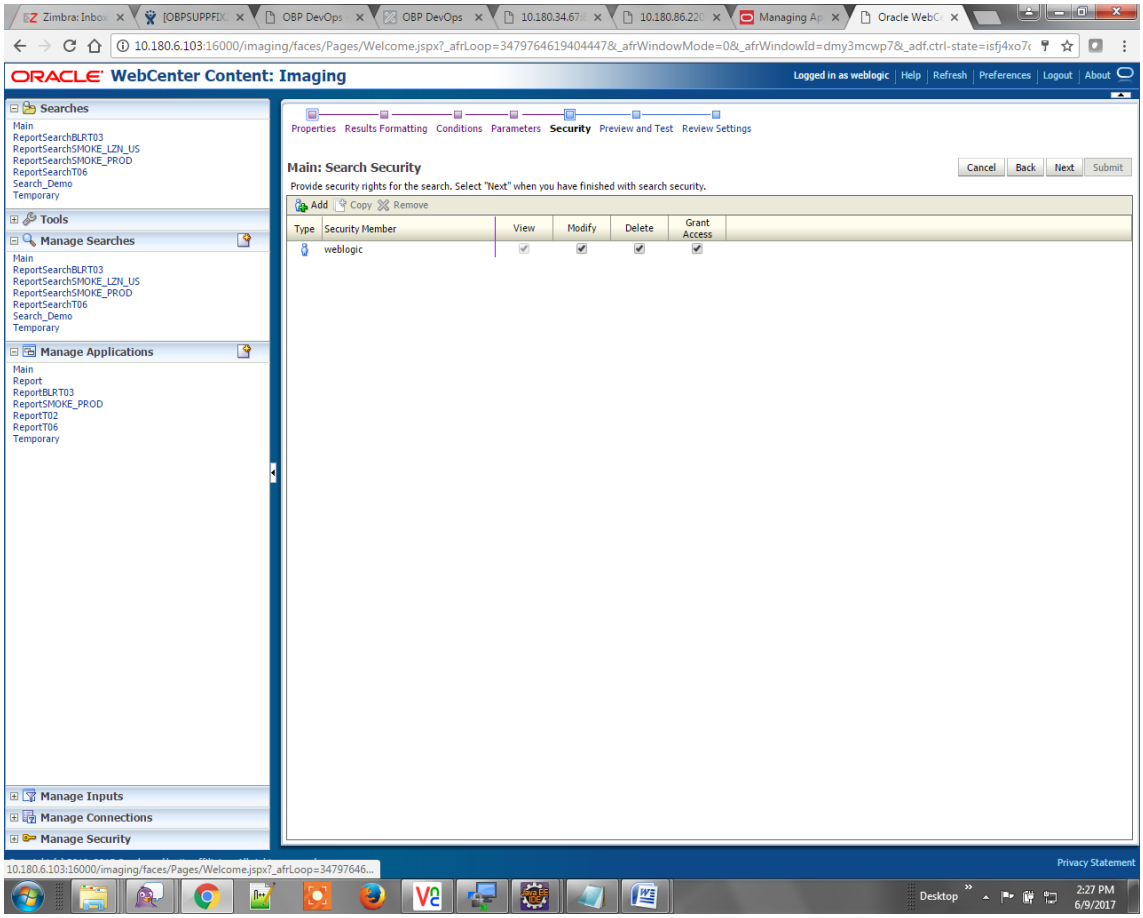
5. Select the appropriate settings in the Parameters page as shown below.

Figure 6–18 Main: Parameters



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

Figure 6–19 Main: Search Security



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

Figure 6–20 Main: Preview and Test

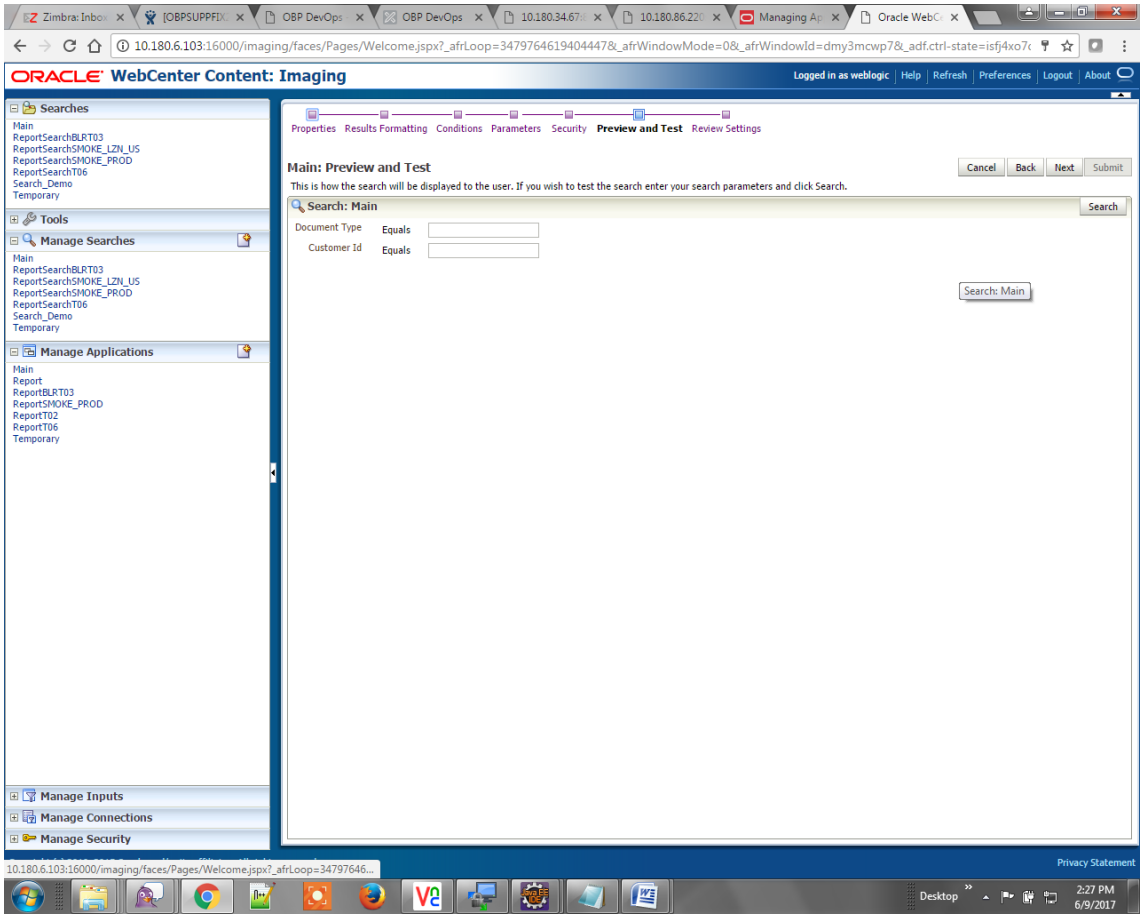
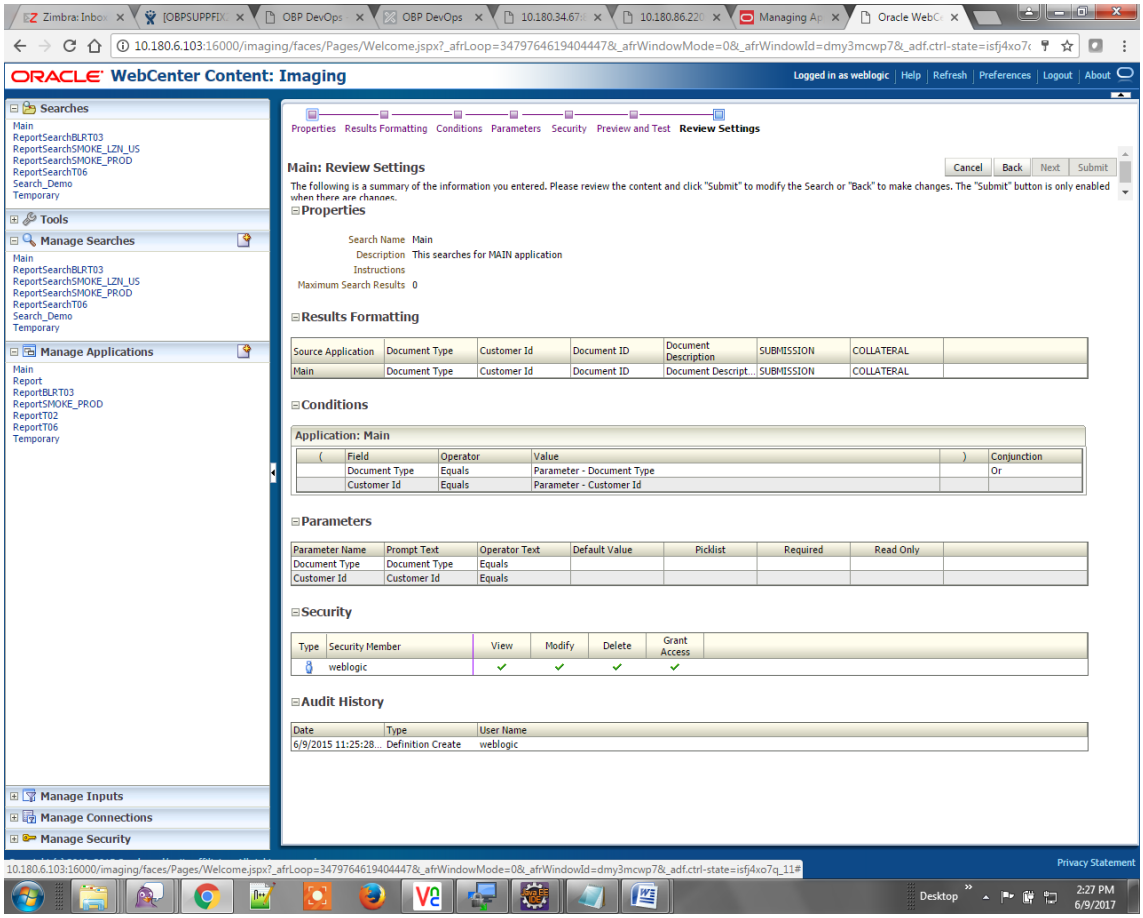


Figure 6–21 Main: Review Settings



6.1.3 Temp Application Configuration

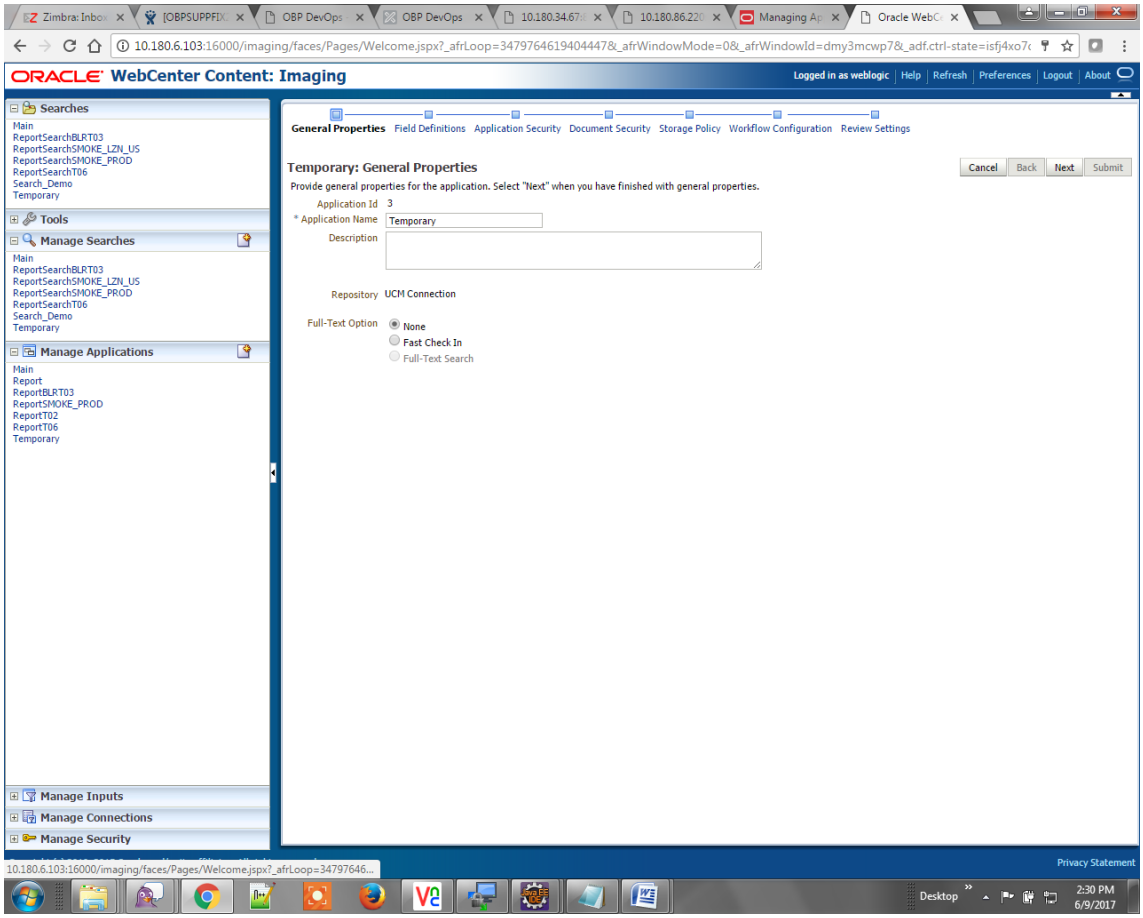
This section provides details about the temp application configuration.

6.1.3.1 Manage Application Configuration

To manage application configuration:

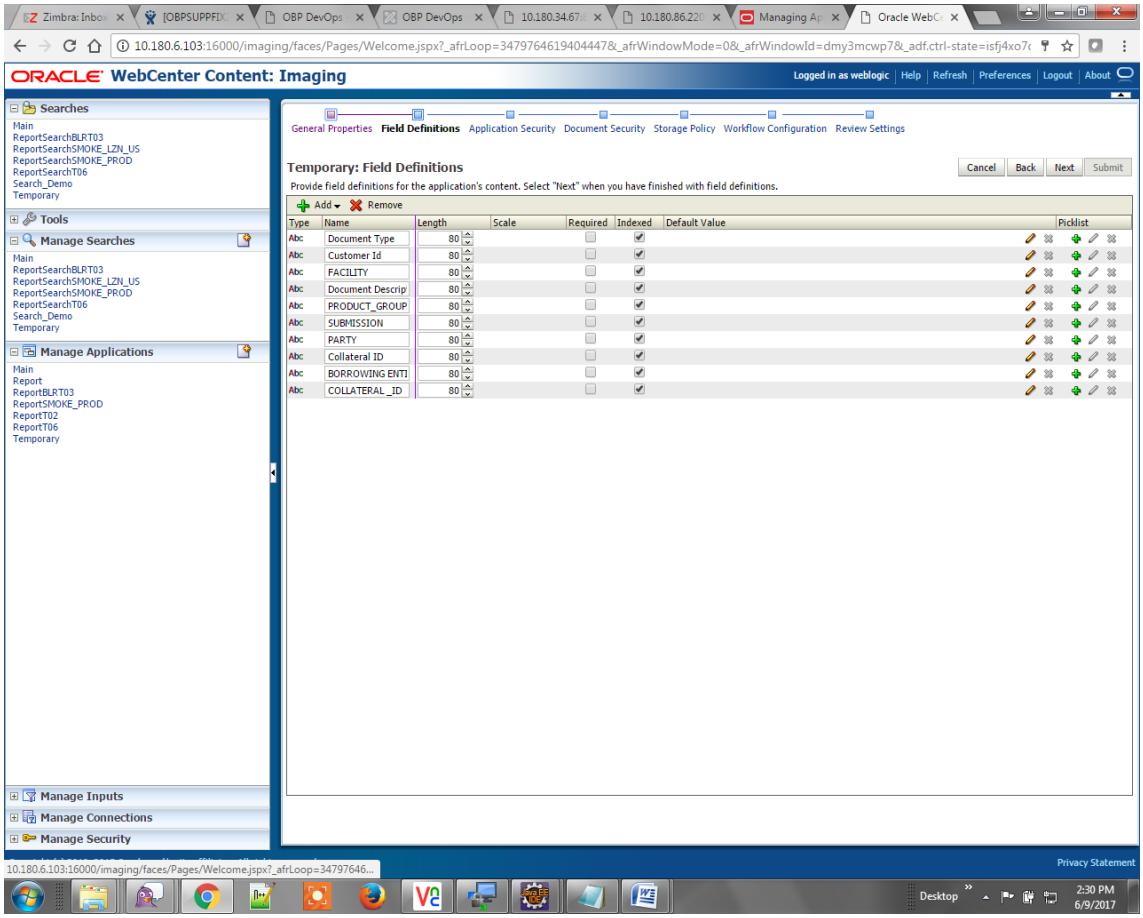
1. Select the Create New Application option.
2. Enter the general properties and click **Next.**

Figure 6–22 Temporary: General Properties



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

Figure 6–23 Temporary: Field Definitions



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

Figure 6–24 Temporary: Application Security

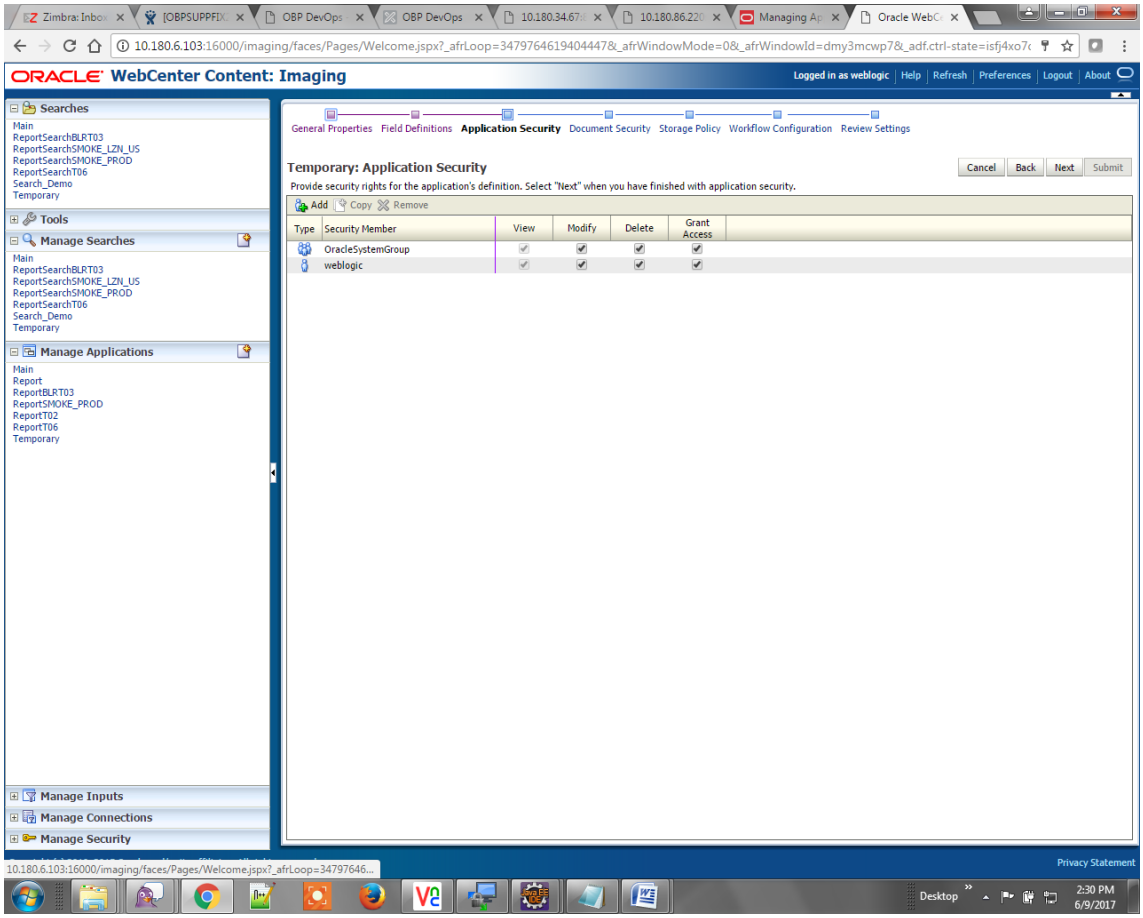
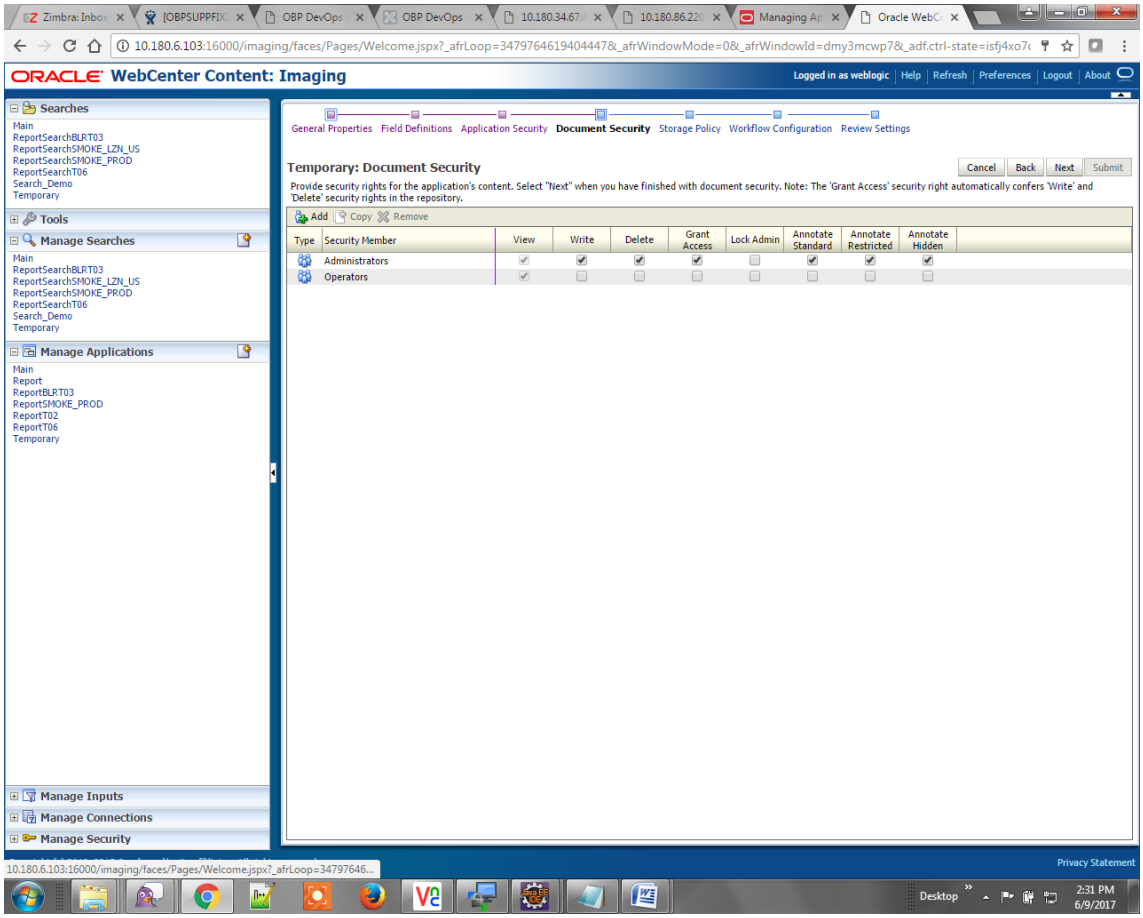
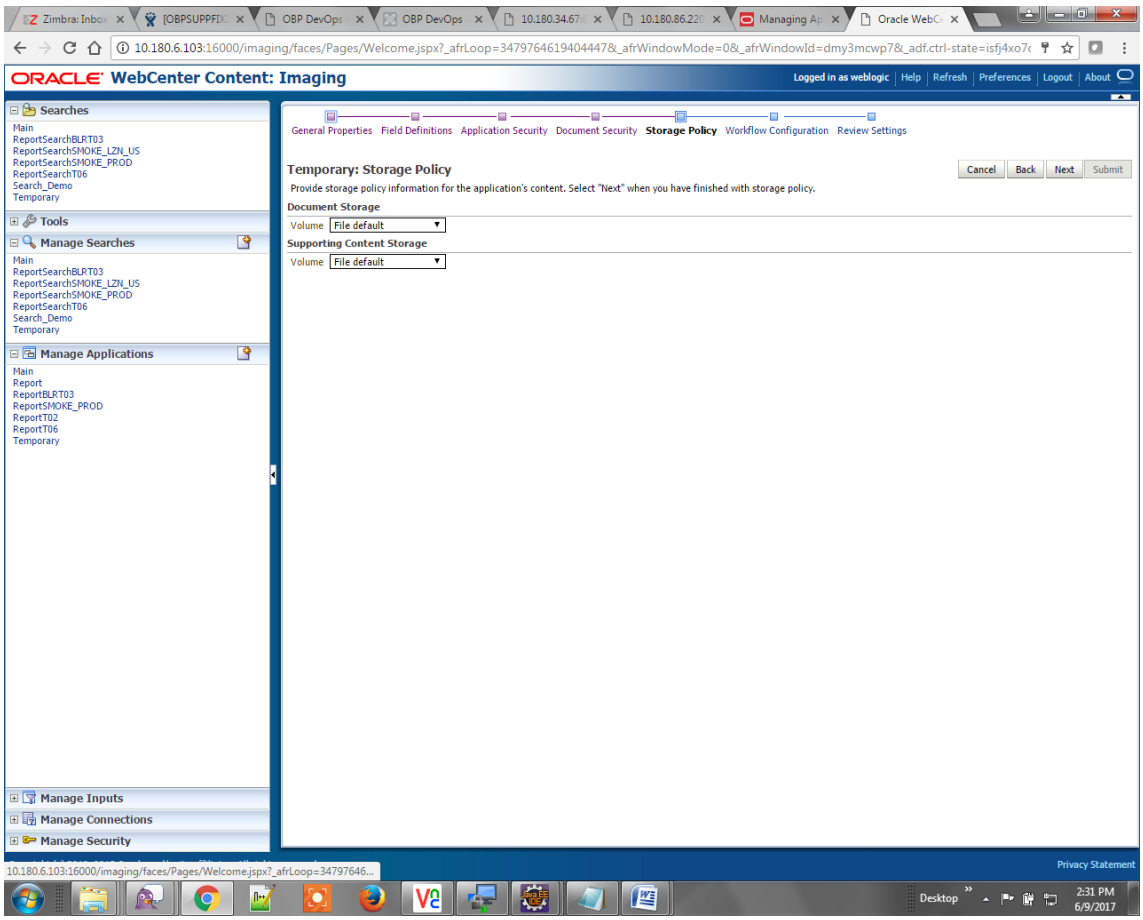


Figure 6–25 Temporary: Document Security



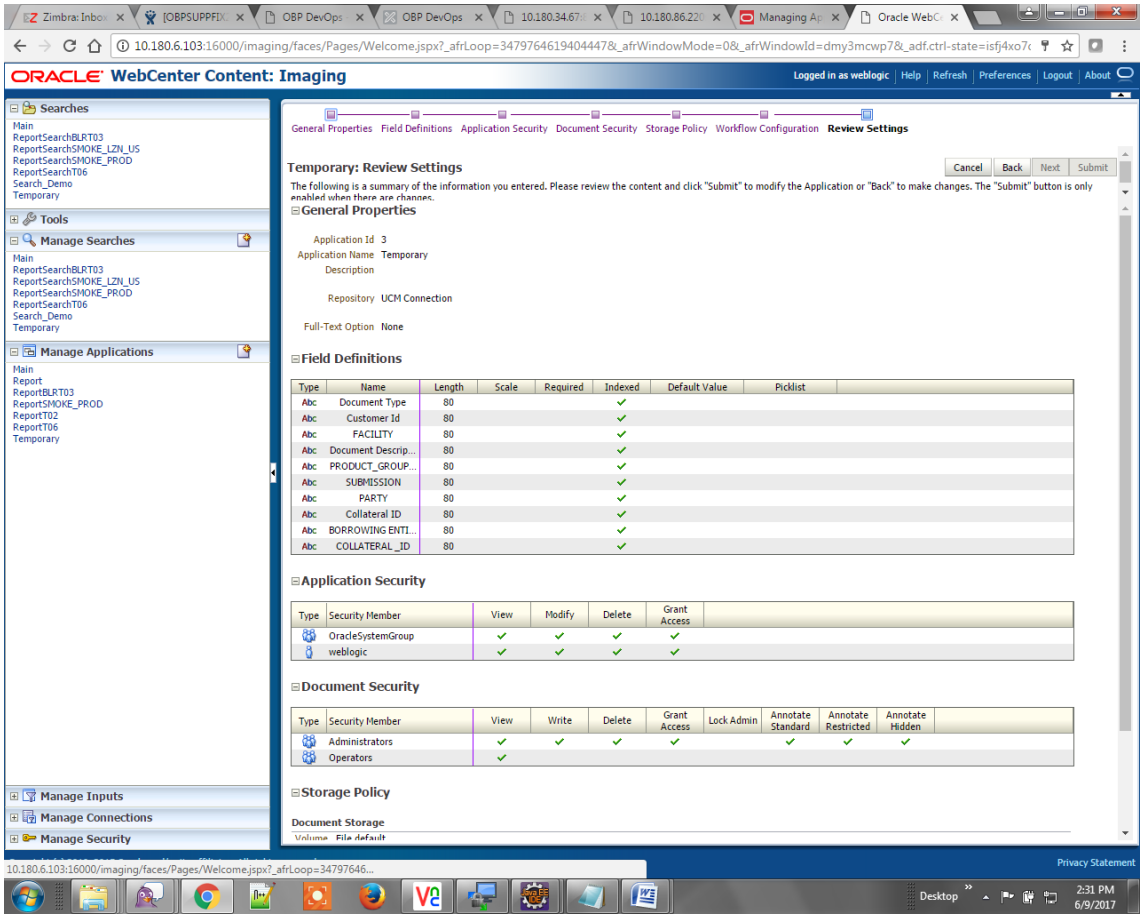
5. In the Storage Policy page, select the file default option has shown below.

Figure 6–26 Temporary: Storage Policy



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

Figure 6–27 Temporary: Review Settings

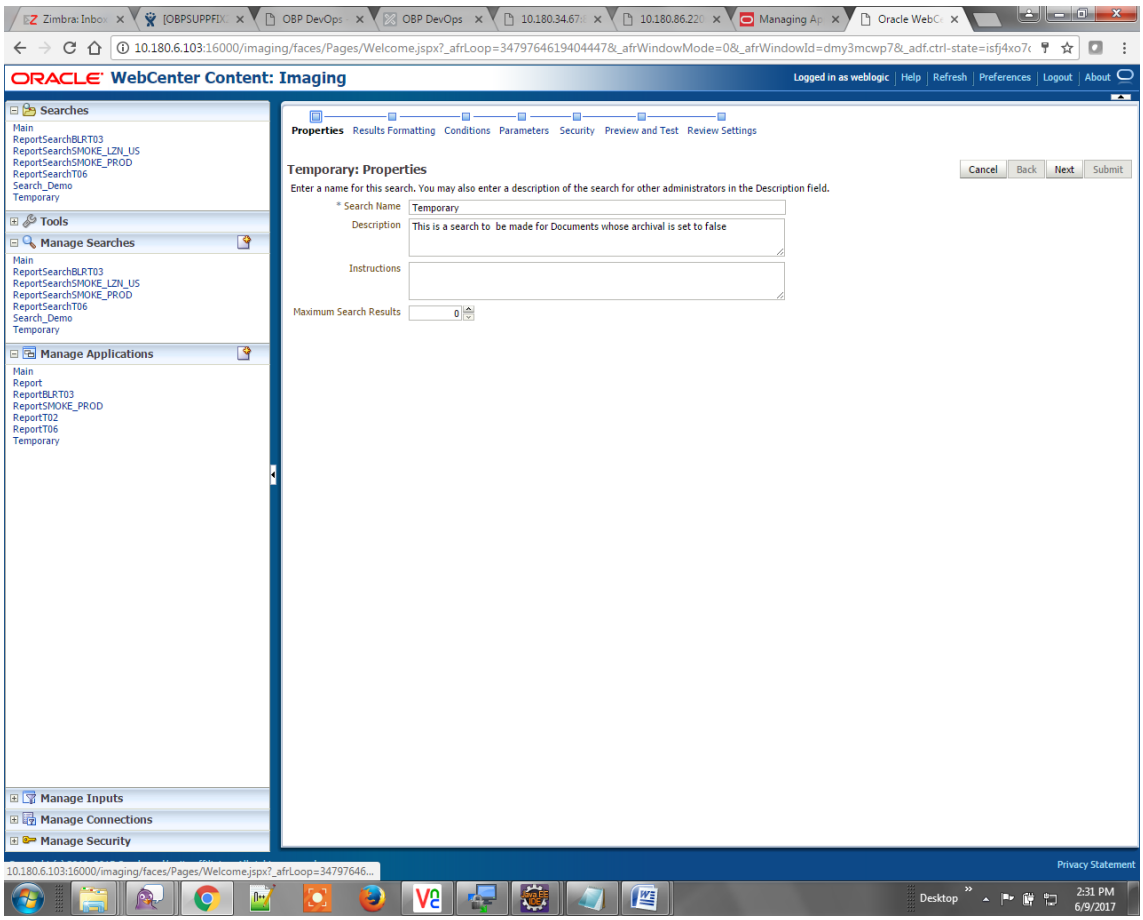


6.1.3.2 Manage Searches

To manage searches:

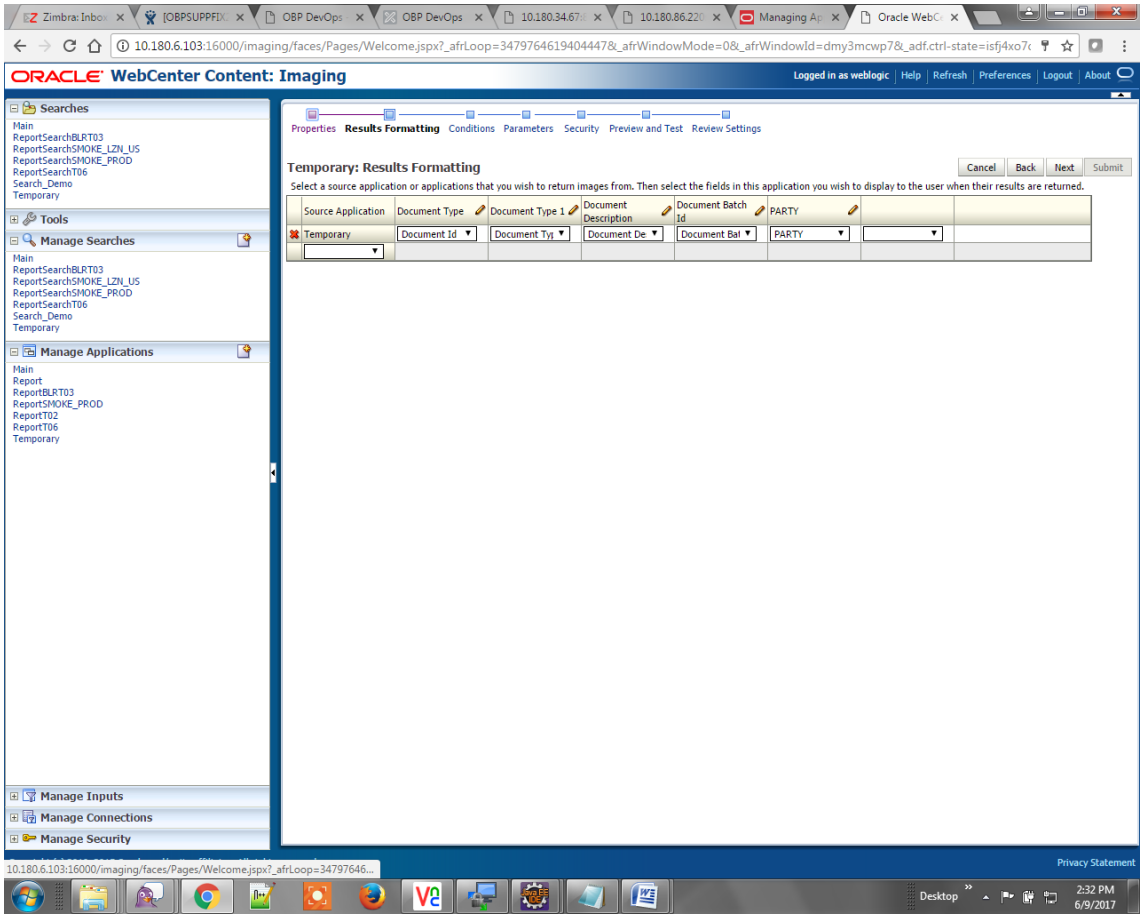
1. Click the Manage Searches option and enter the search name with description.

Figure 6–28 Temporary: Properties



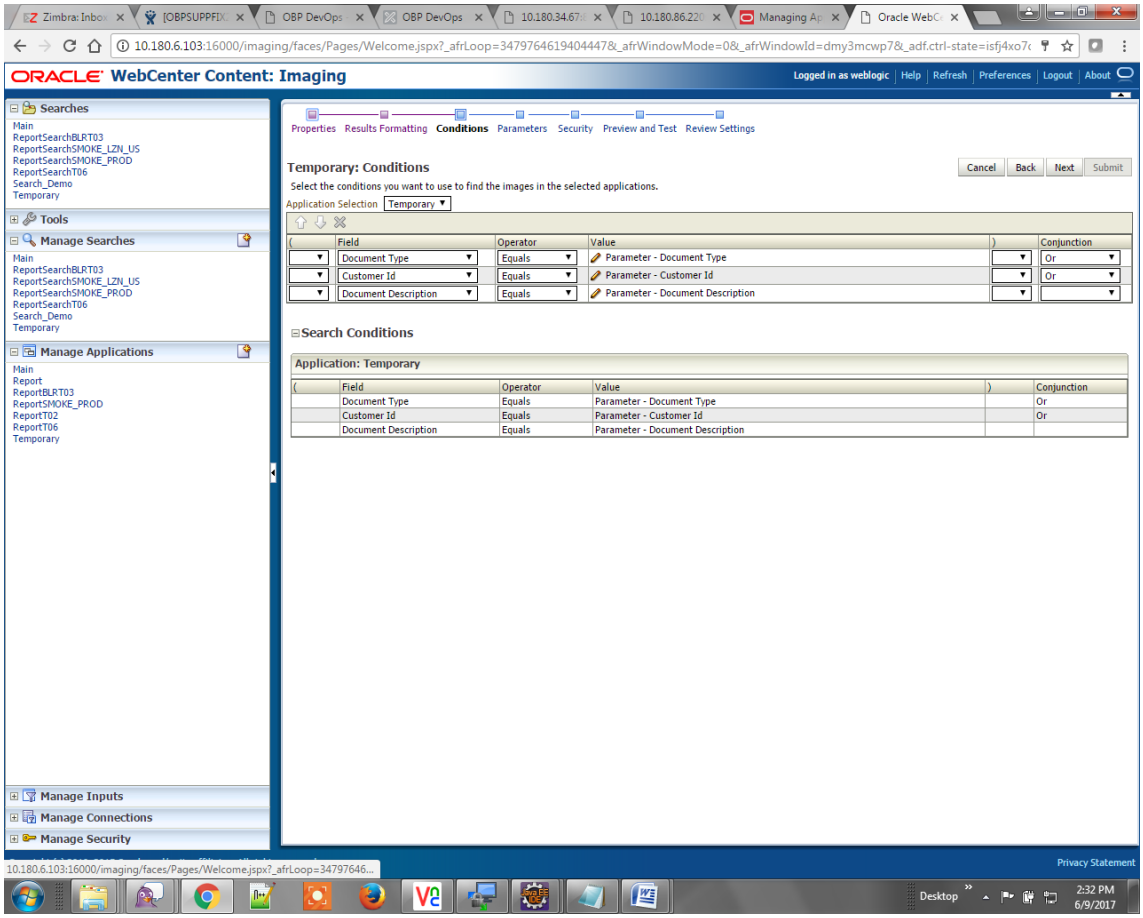
2. Select the source application along with its field details in the Results Formatting page.

Figure 6–29 Temporary: Results Formatting



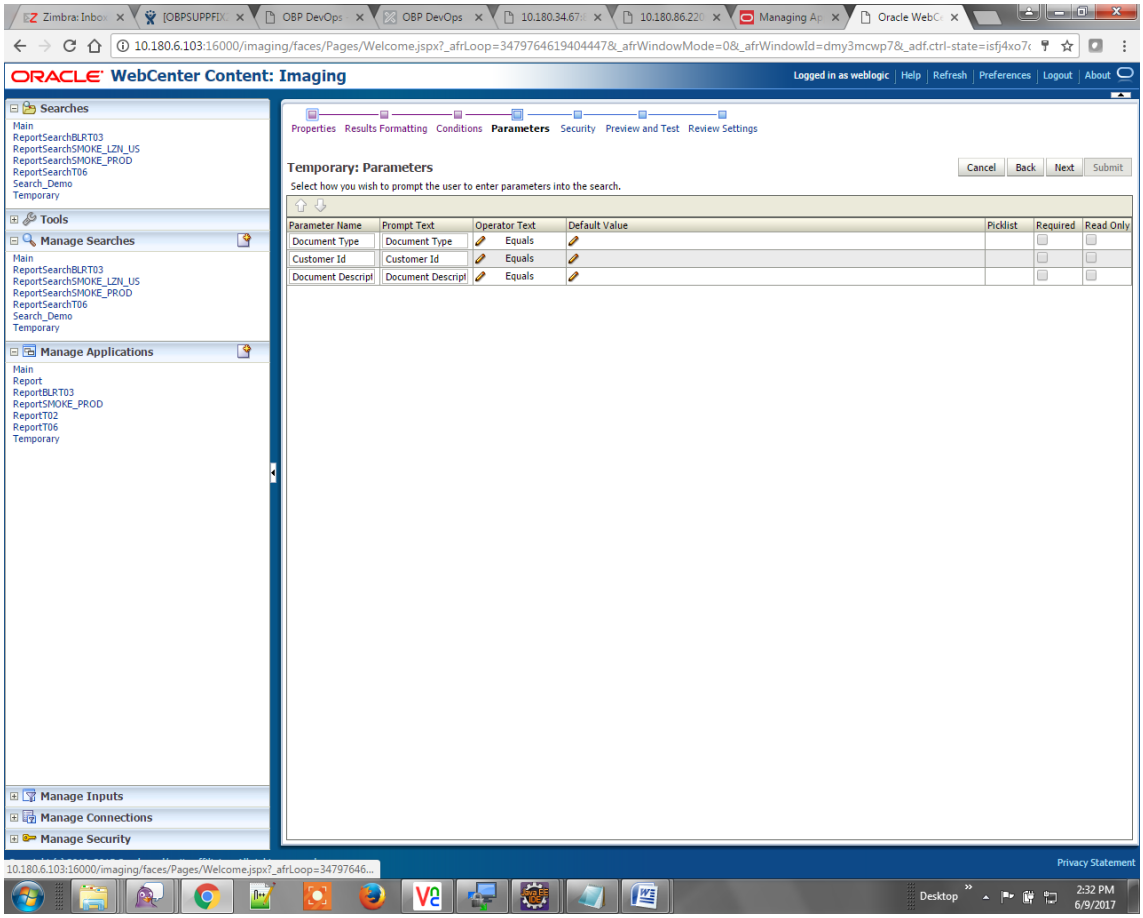
3. Select the appropriate conditions in the Conditions page as shown below.

Figure 6–30 Temporary: Conditions



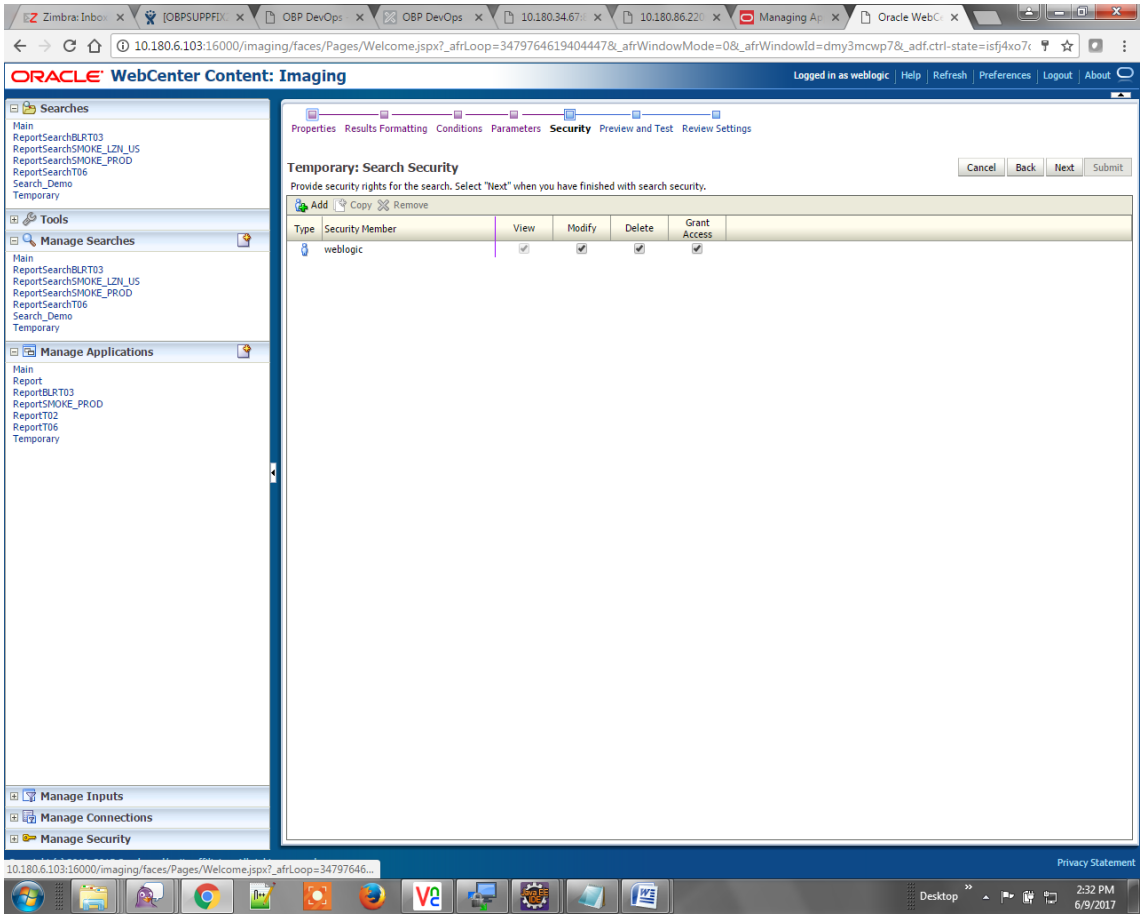
4. Select the appropriate settings in the Parameters page as shown below.

Figure 6–31 Temporary: Parameters



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

Figure 6–32 Temporary: Search Security



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

Figure 6–33 Temporary: Preview and Test

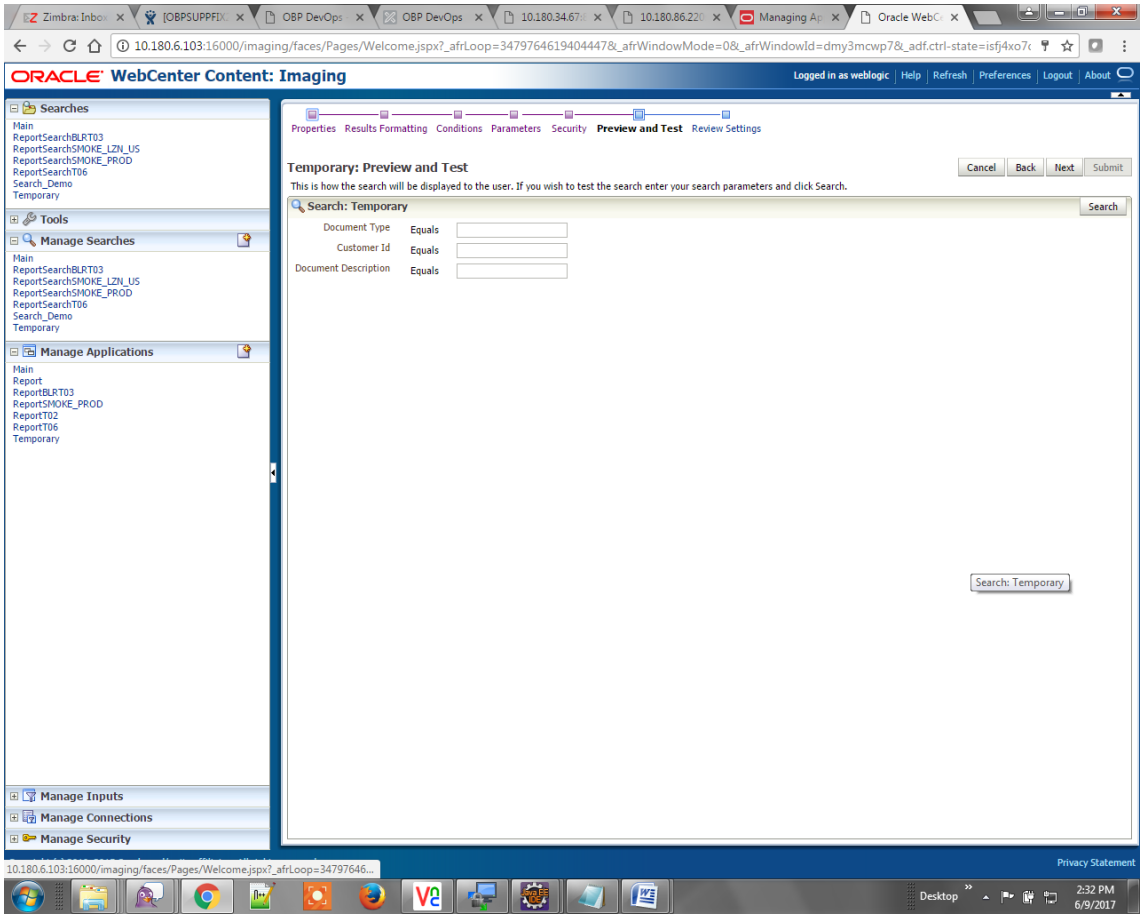
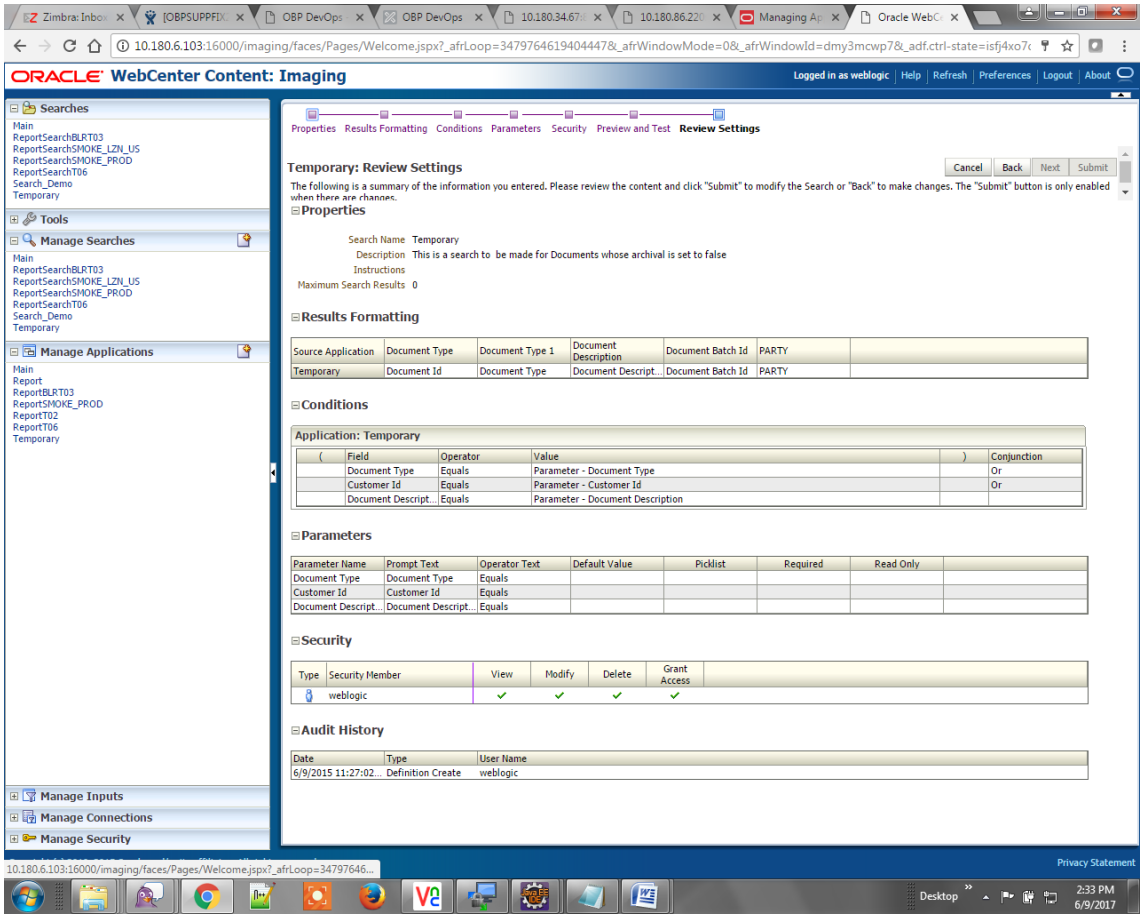


Figure 6–34 Temporary: Review Settings



The application ID generated for the main and temporary applications should be updated in the OBEDM 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';
```

6.2 IPM Report Upload Setup

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

6.2.1 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.

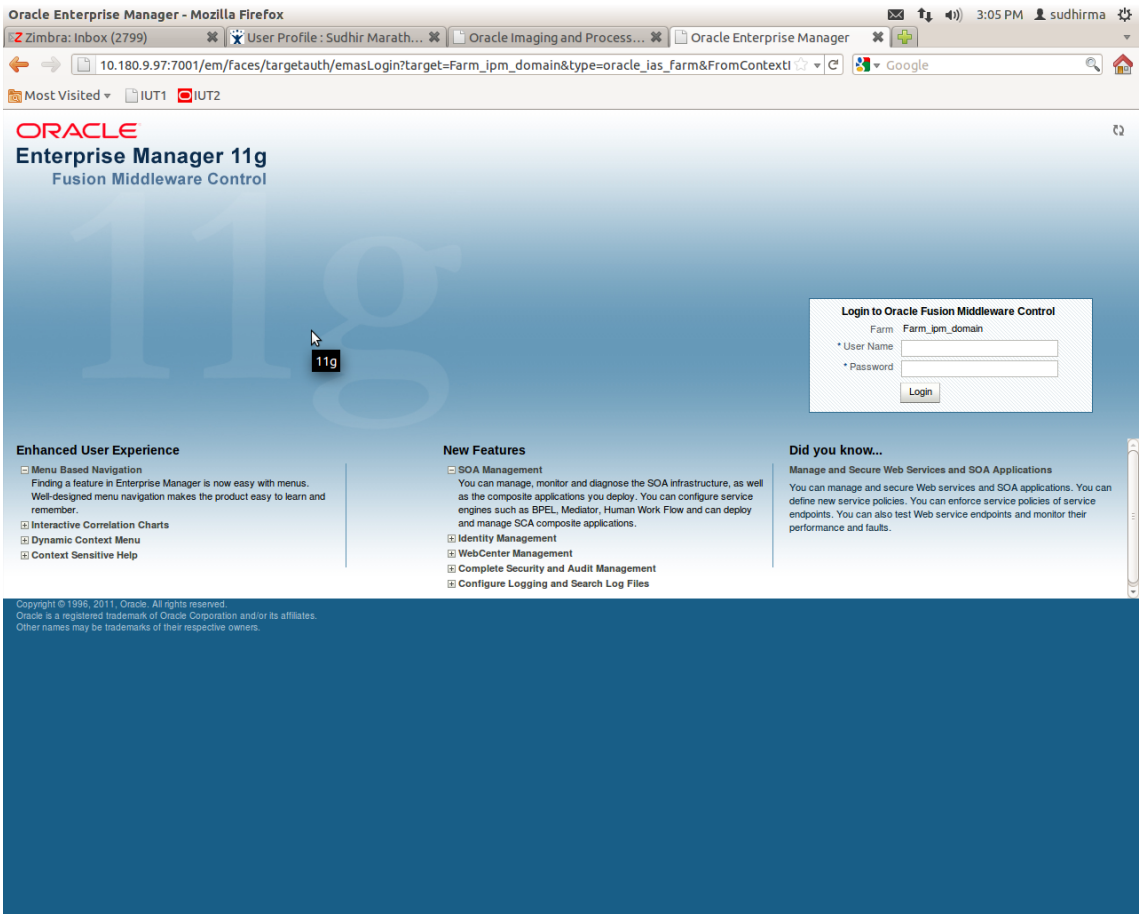
6.2.2 Setting up the Connection Name

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.

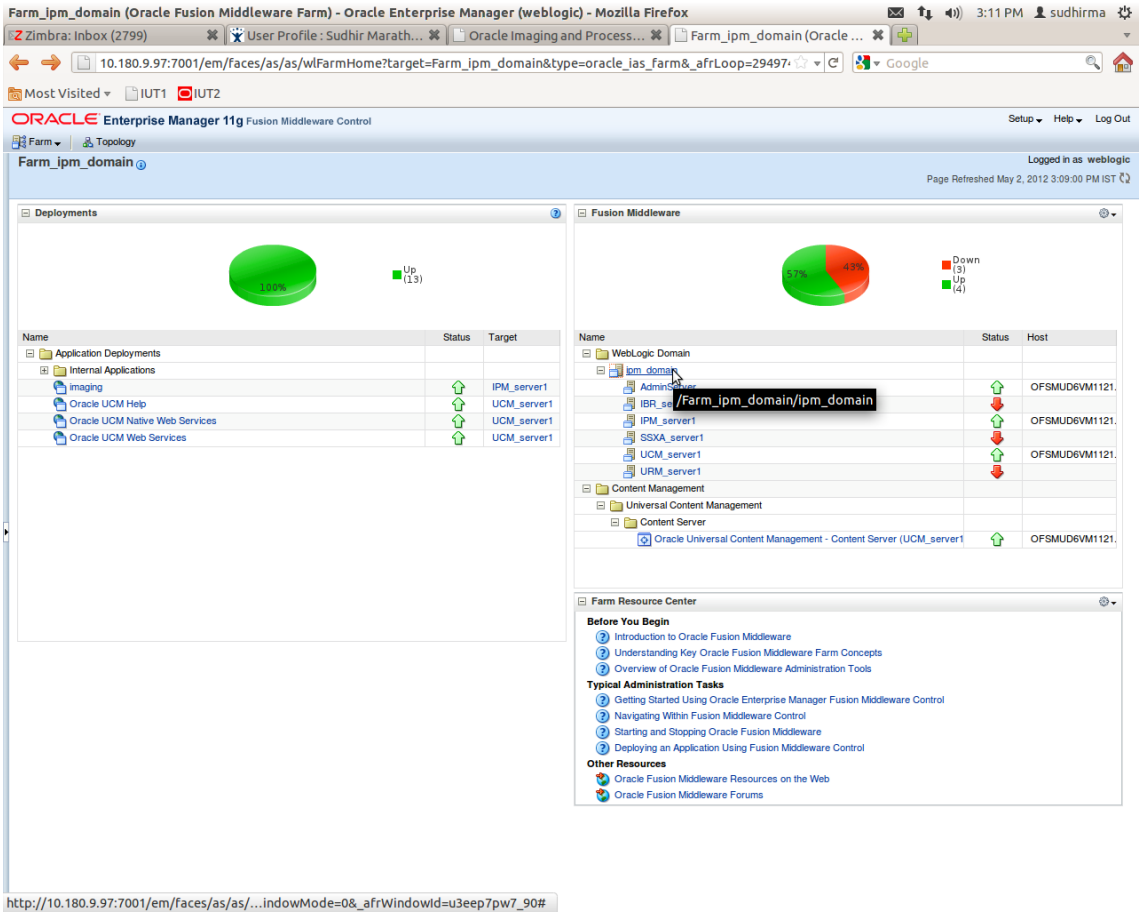
Figure 6–35 Log in to Enterprise Manager (EM) console



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

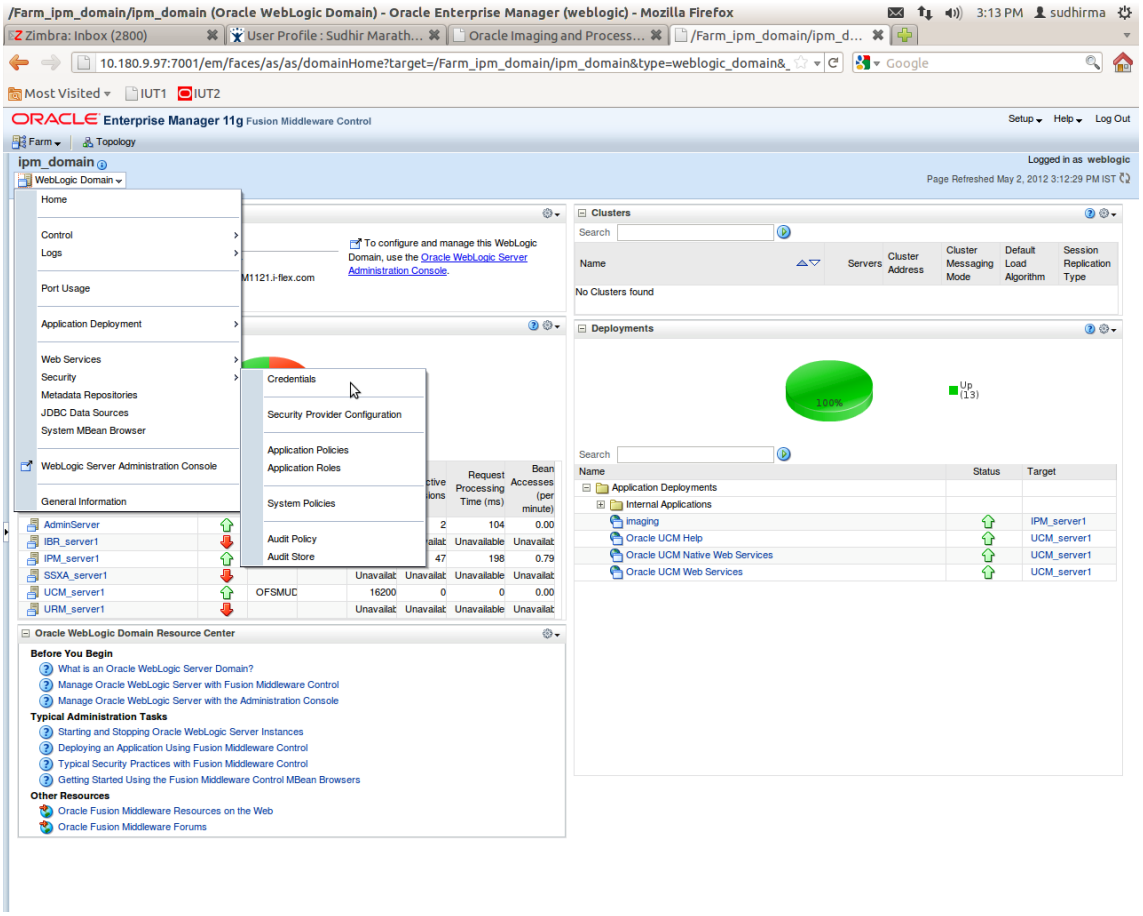
ipm server is installed).

Figure 6–36 Click Weblogic Domain: ipm domain



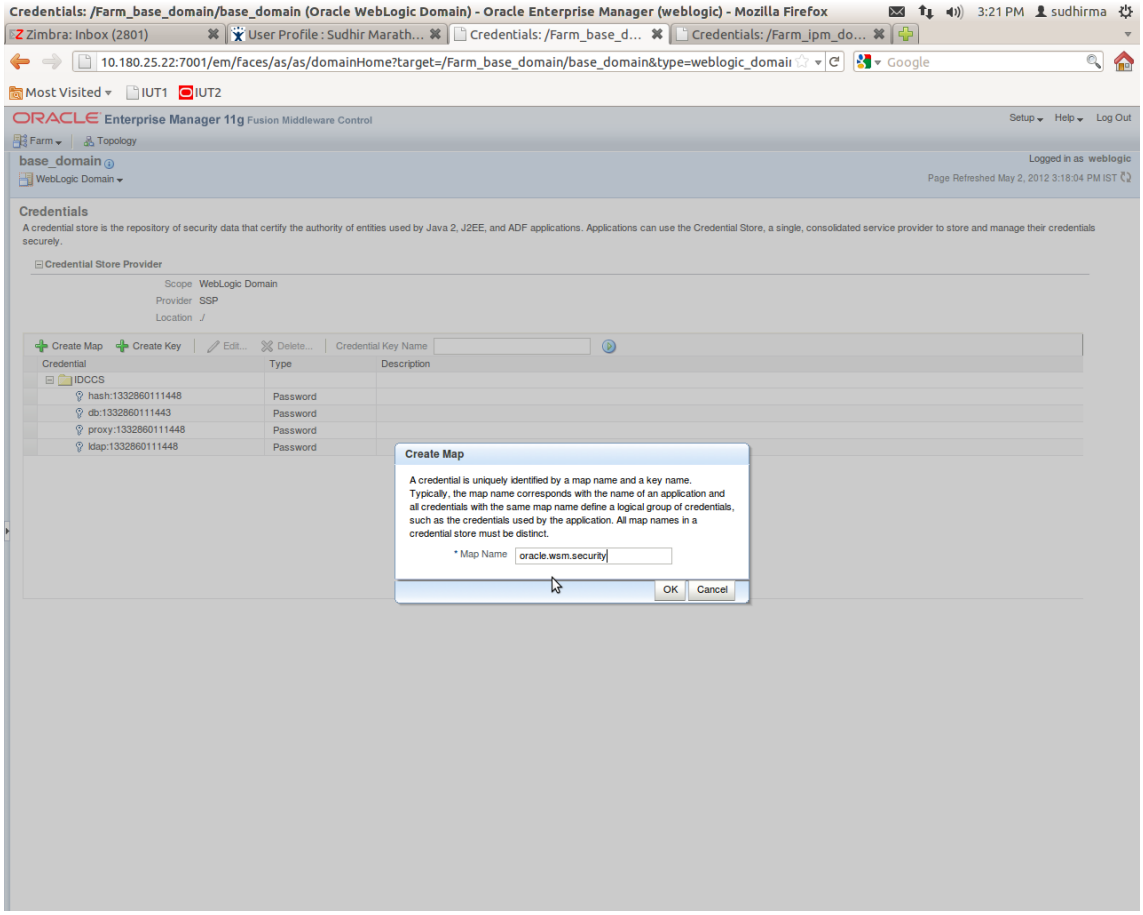
3. In the top menu, click **Weblogic Domain.** The corresponding menu appears.
4. Navigate to **Security > Credentials.** The Credentials page appears.

Figure 6–37 Navigate to Weblogic Domain --> Security --> Credentials



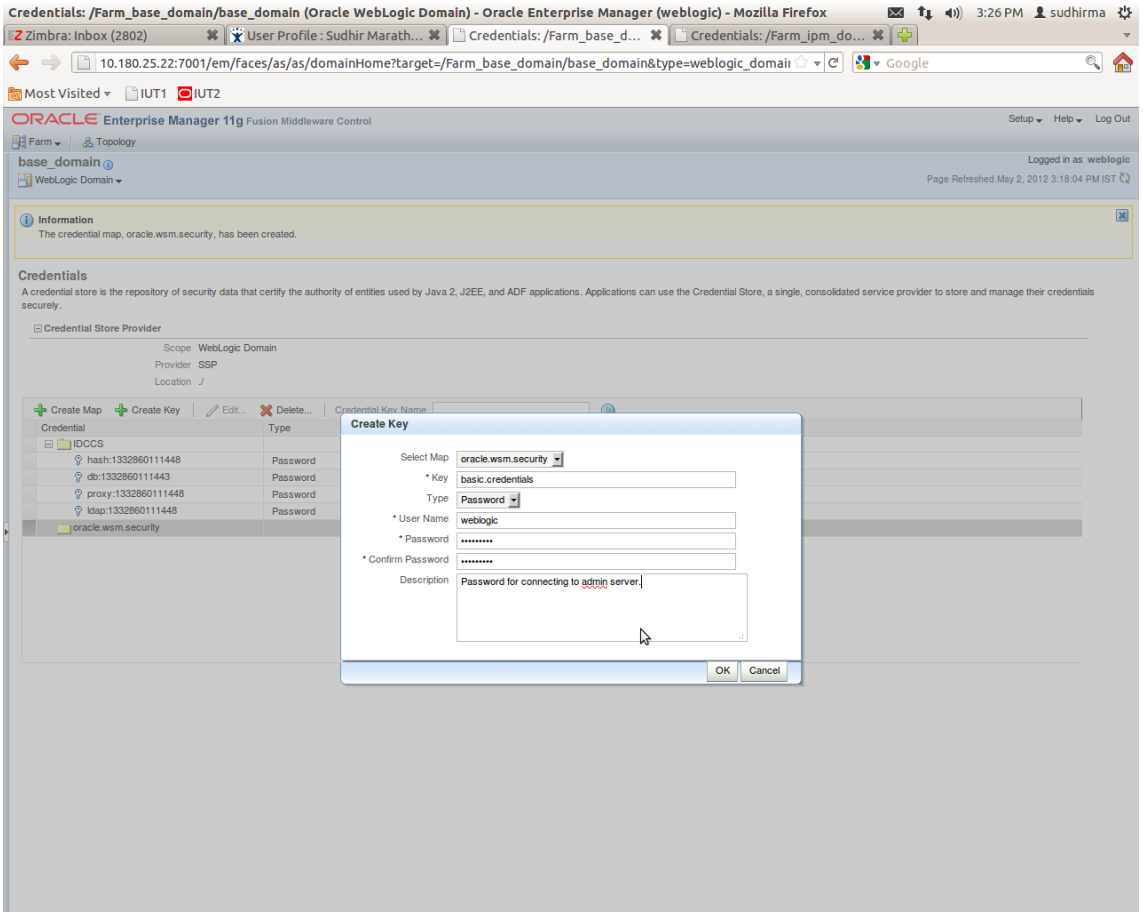
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 6–38 Create Map oracle.wsm.security



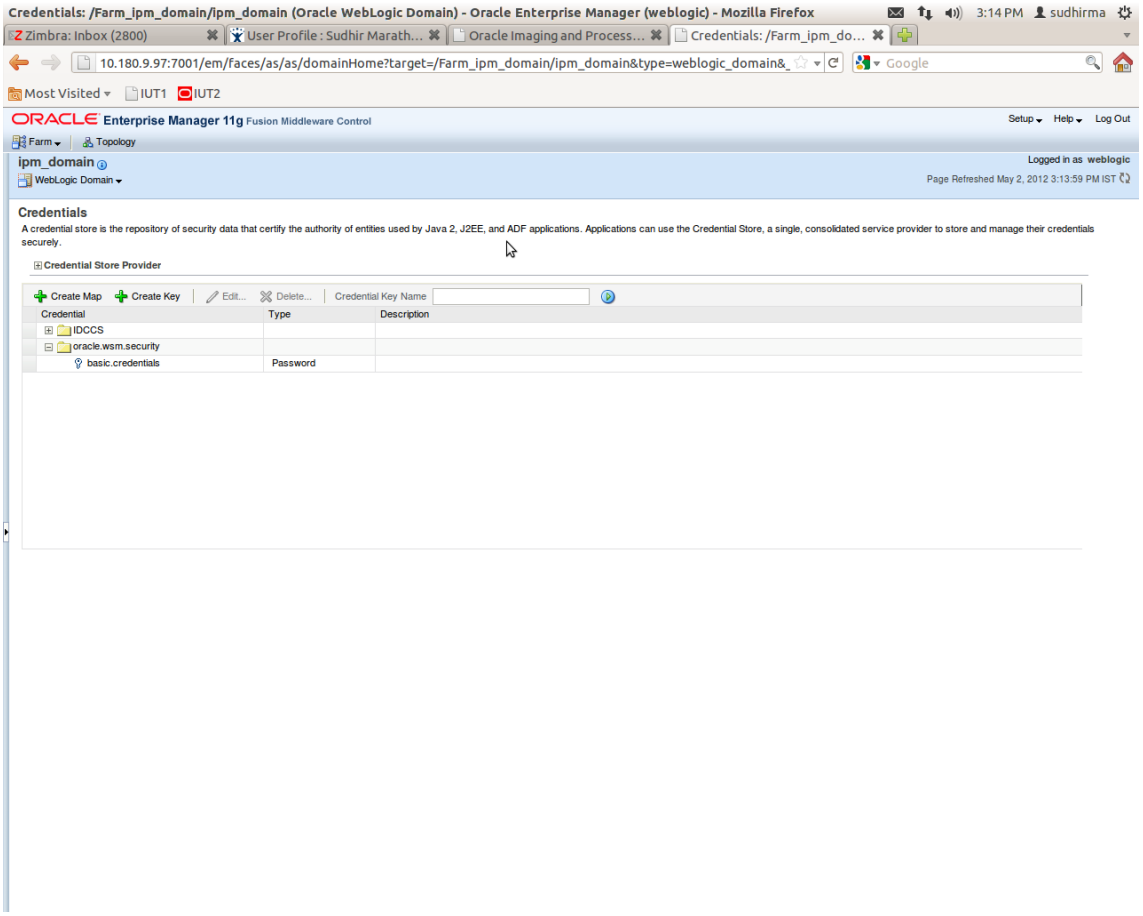
6. Click **Create Key** to create a key under the map **oracle.wsm.security.**

Figure 6–39 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 6–40 ipm_domain: Credentials Created

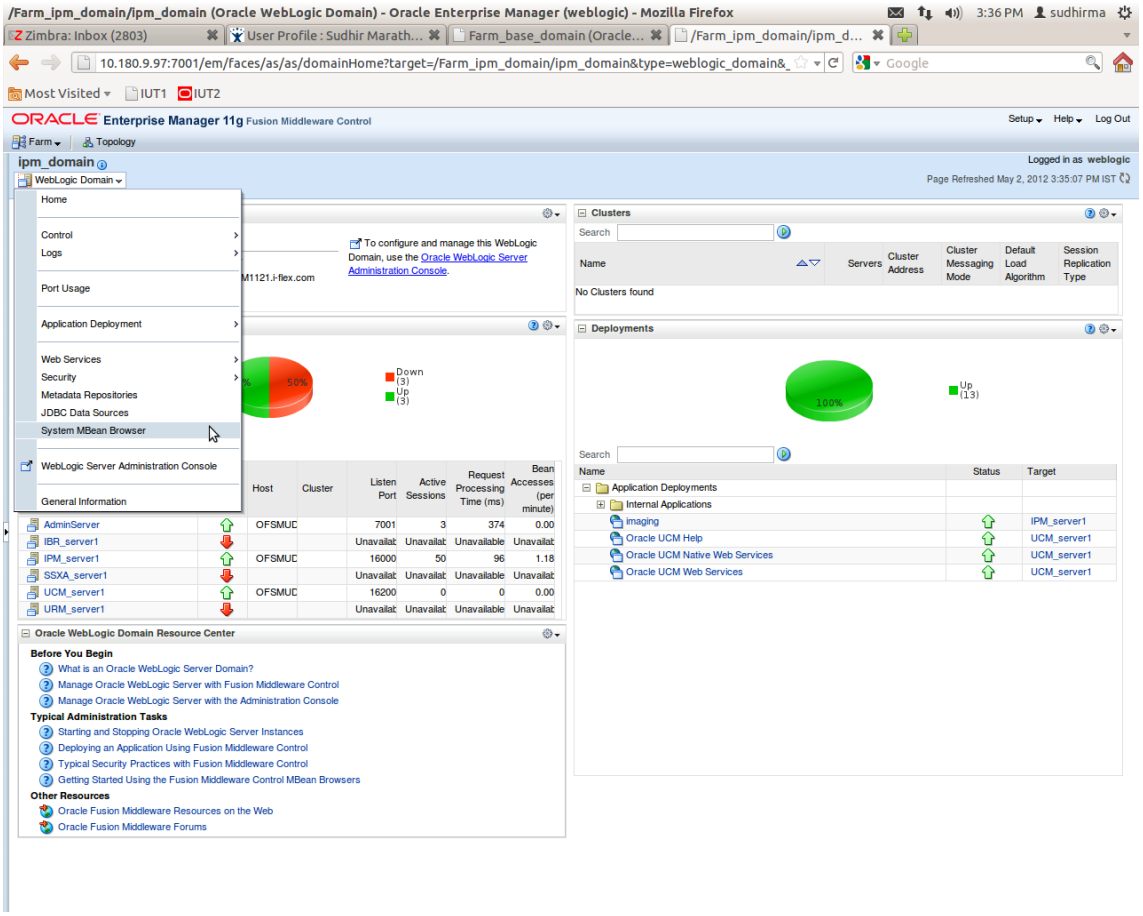


6.2.3 Setting up Input Agent Path

To set up input agent path:

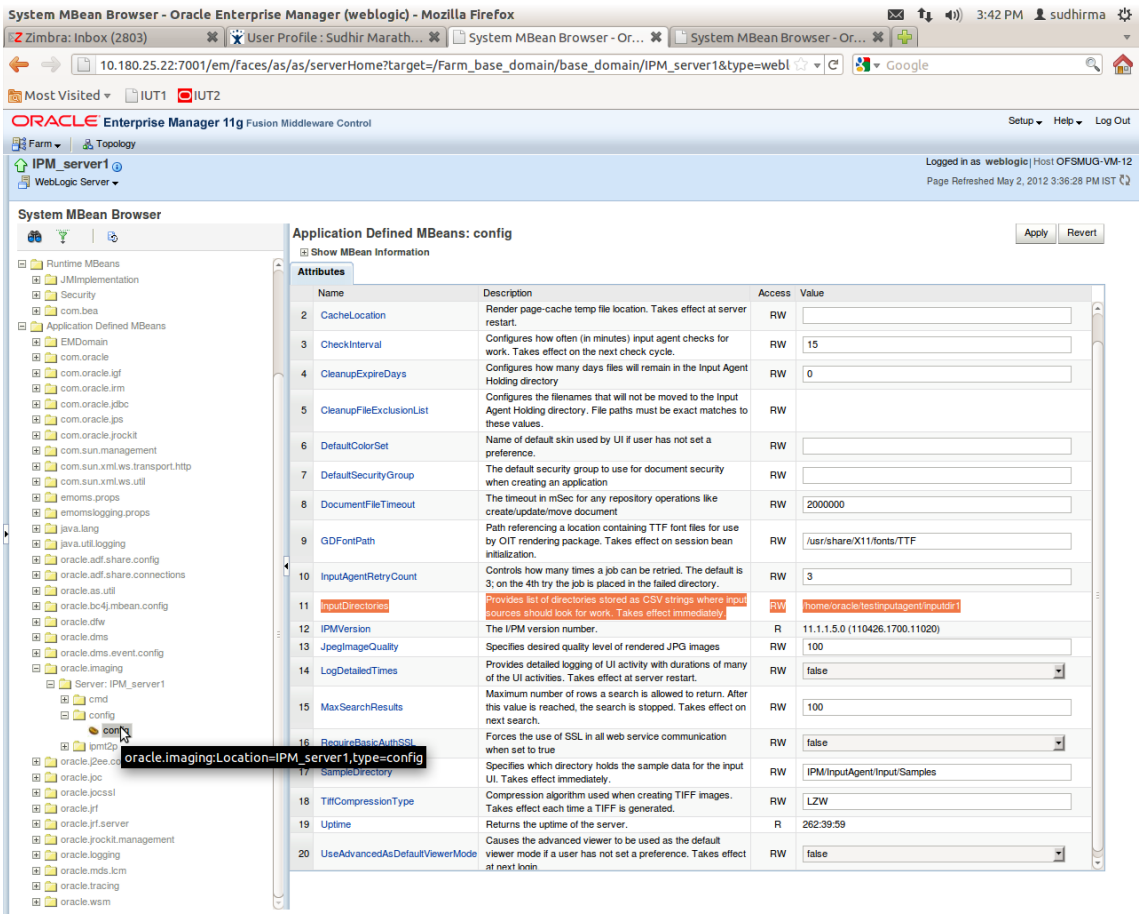
1. Log in to Enterprise Manager (EM) console.
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain**.
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

Figure 6–41 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.
7. Change the highlighted path value to /scratch/ofssobp/testinputagent/inputdir1.

Figure 6–42 InputDirectories: Enter Input Agent Path

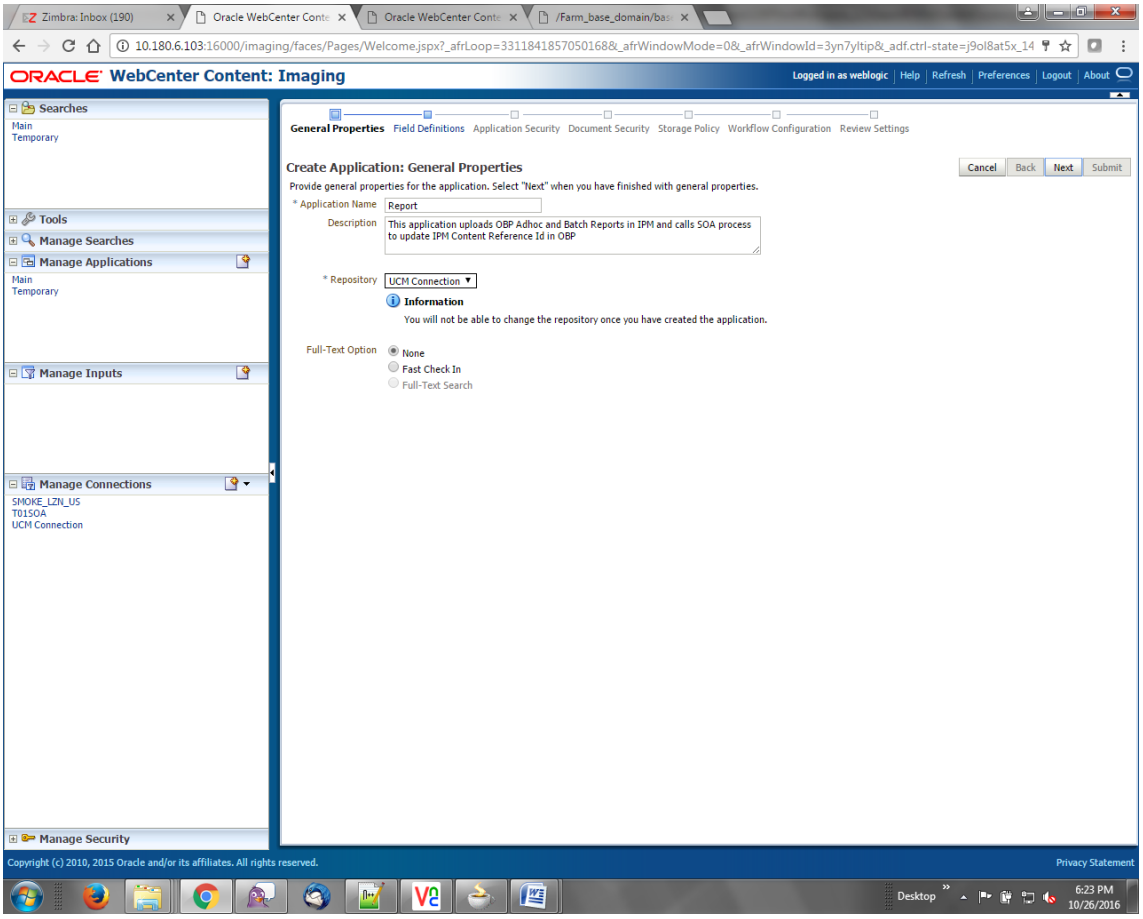


8. Restart IPM server.

6.2.4 Manage Application Configuration

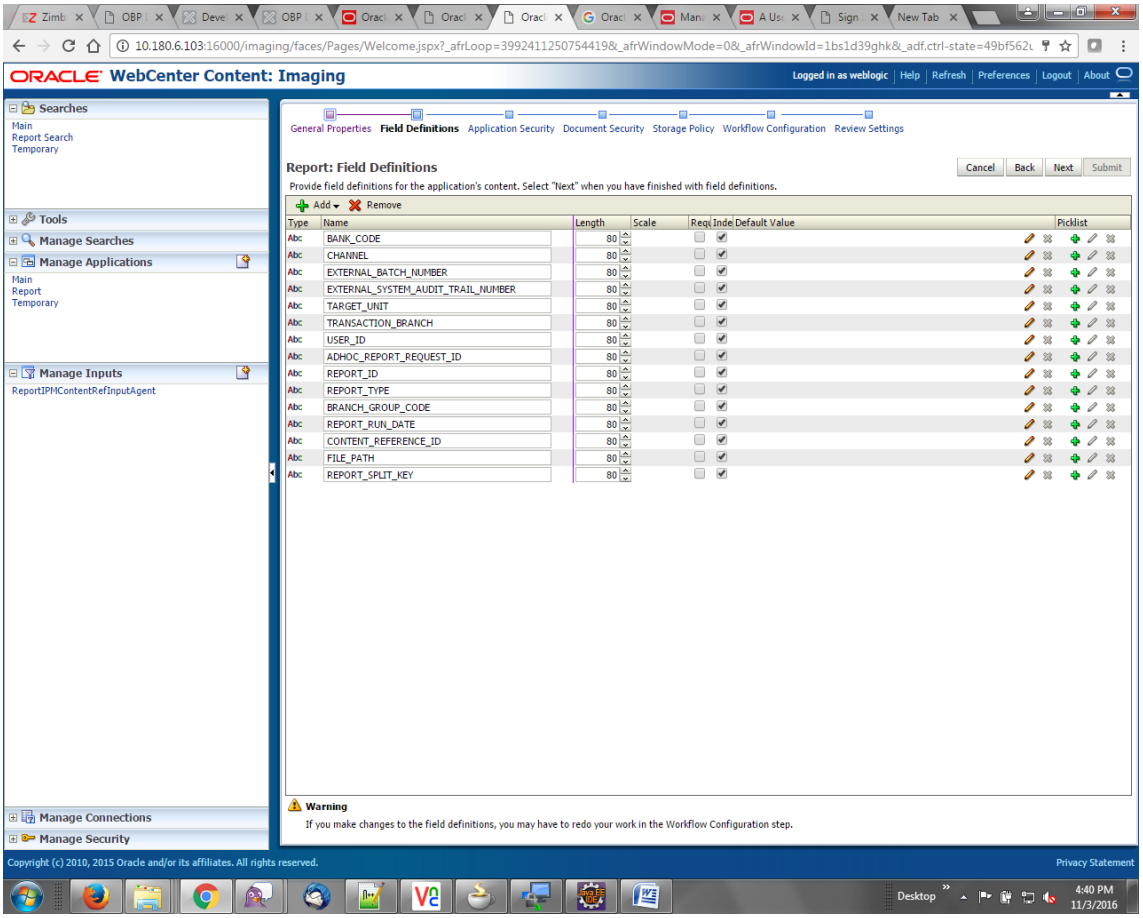
1. Navigate to the Manage Applications section.
2. Select Create New Application option. The Create Application: General Properties page appears.

Figure 6–43 Create Application: General Properties



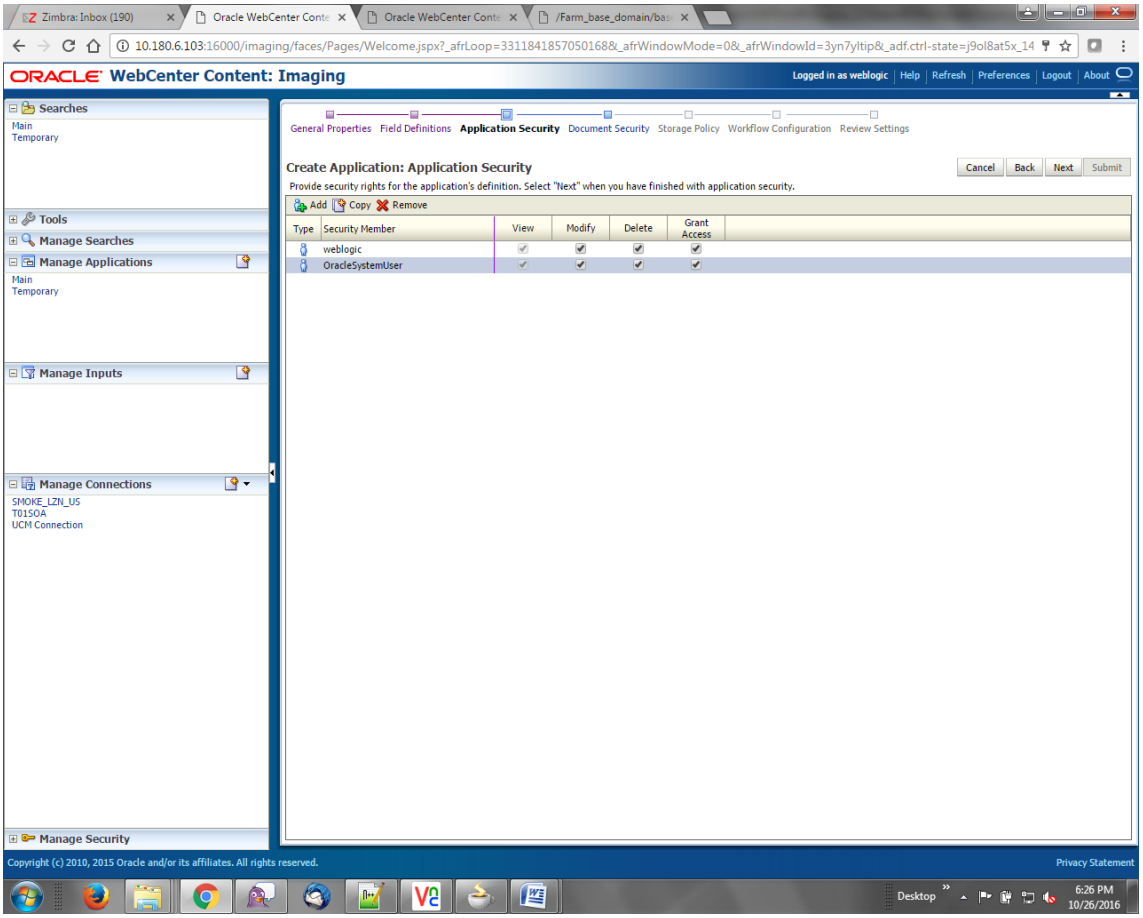
3. Enter the general properties for the application and click **Next.** The Report: Field Definitions page appears.

Figure 6–44 Report: Field Definitions



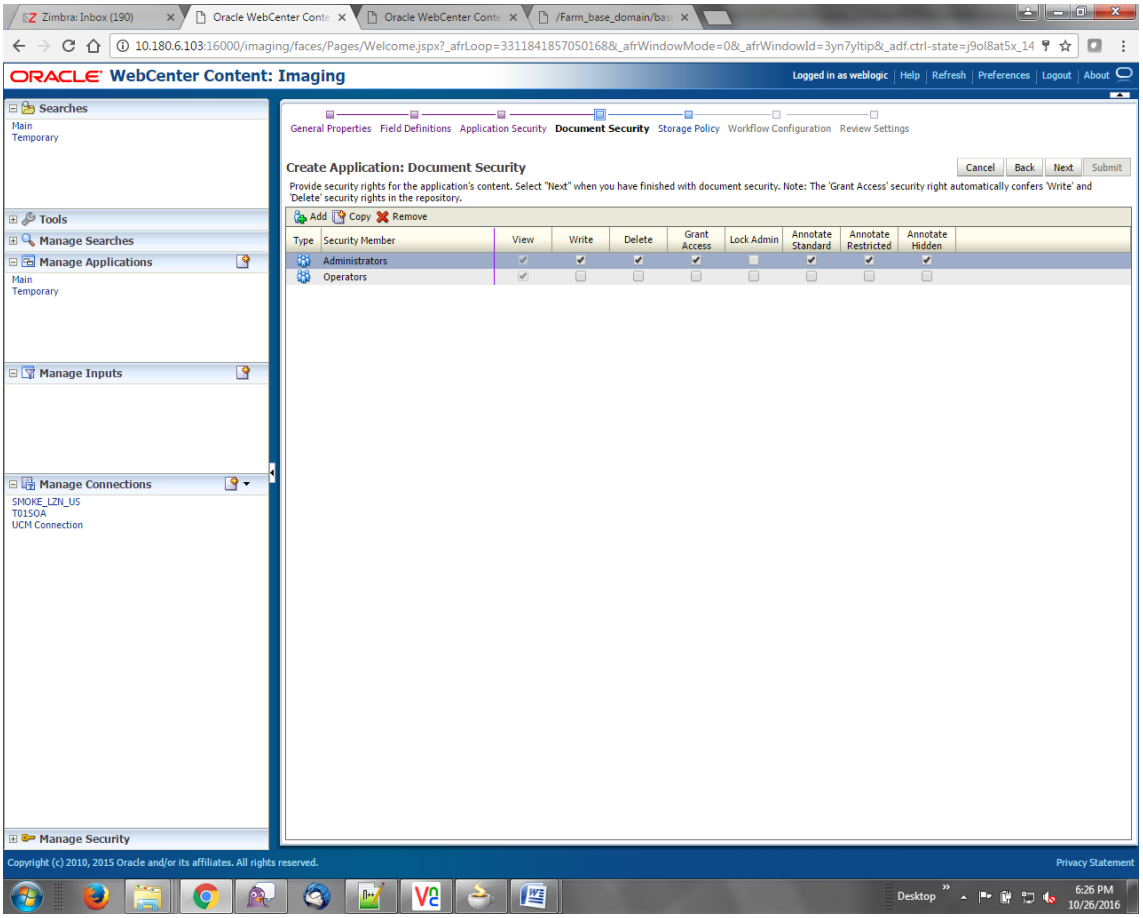
4. Enter the field definition details and click **Next.** The Create Application: Applications Security page appears.

Figure 6–45 Create Application: Applications Security



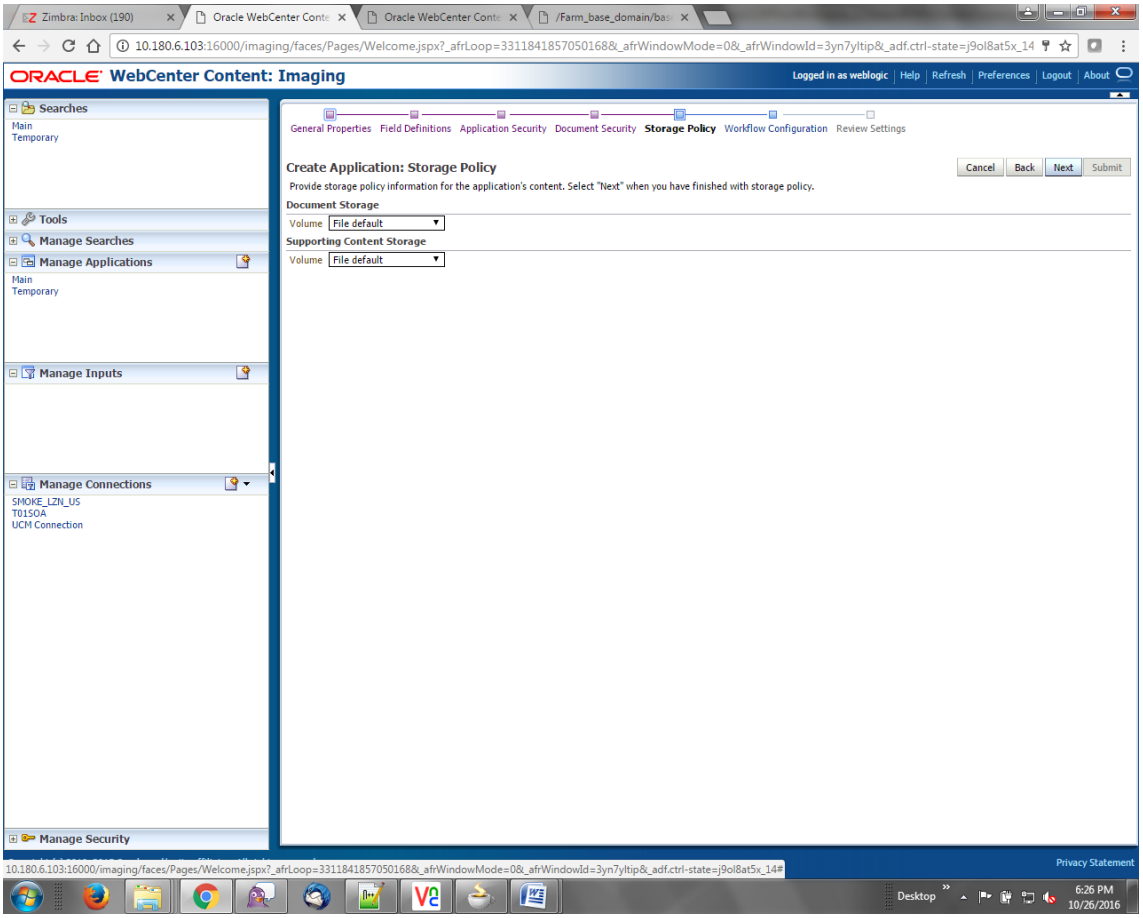
5. In the Application Security section, select the access rights for users and click **Next.** The Create Application: Document Security page appears.

Figure 6–46 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 6–47 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 6–48 Report: Workflow Configuration - Server Properties

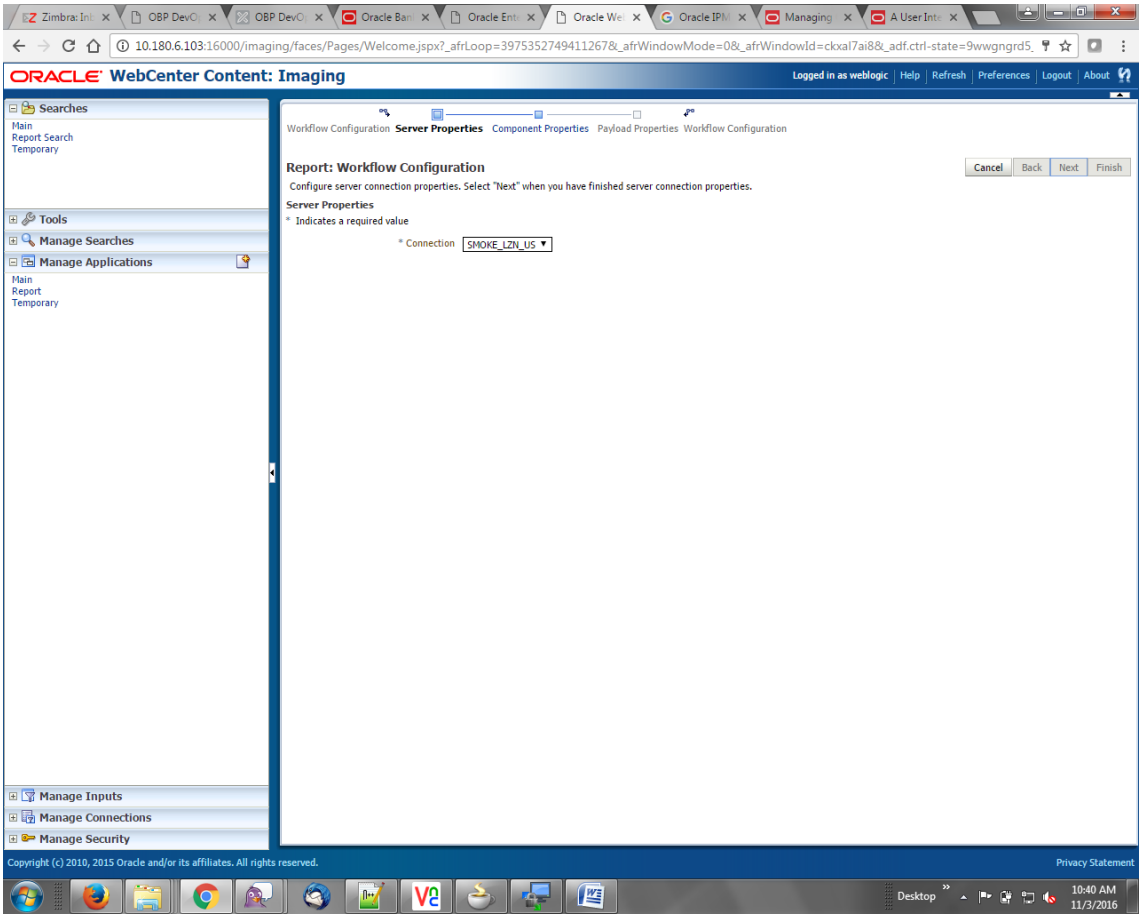


Figure 6–49 Report: Workflow Configuration - Component Properties

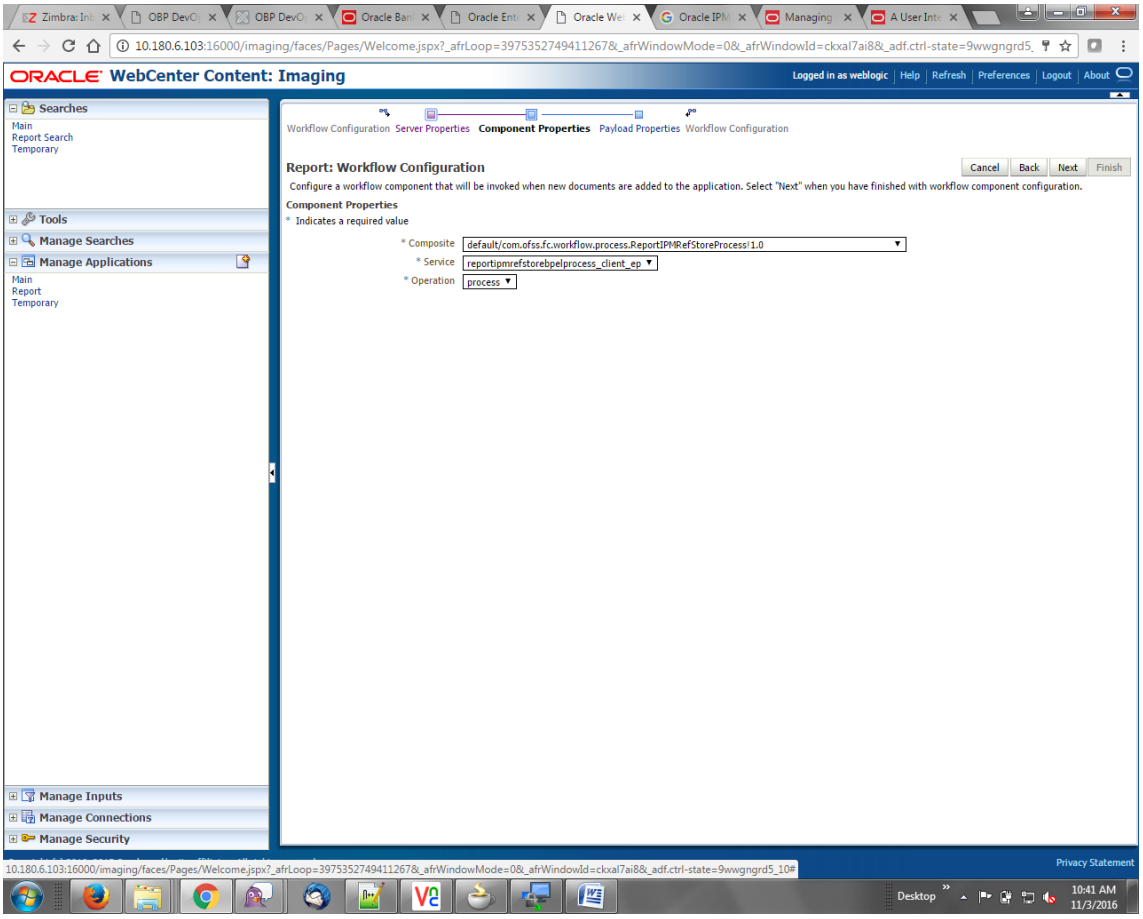
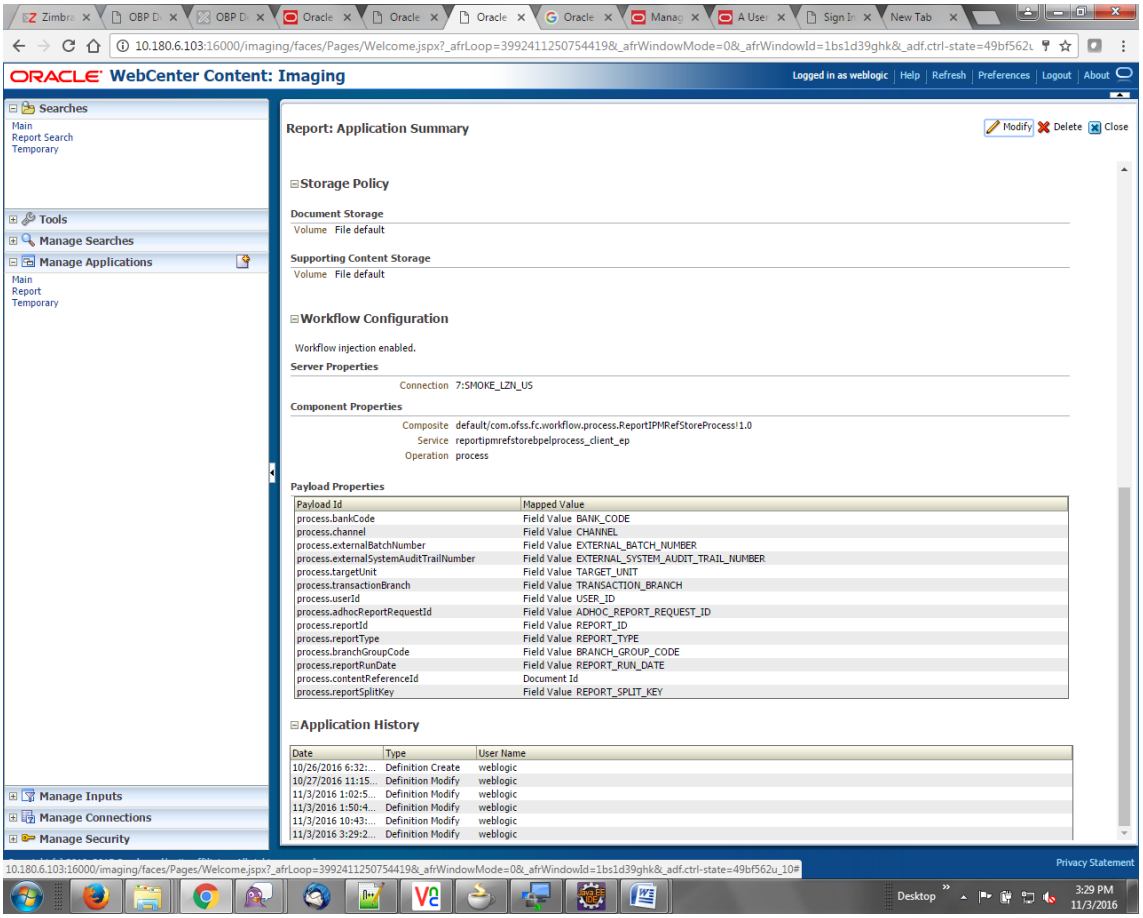
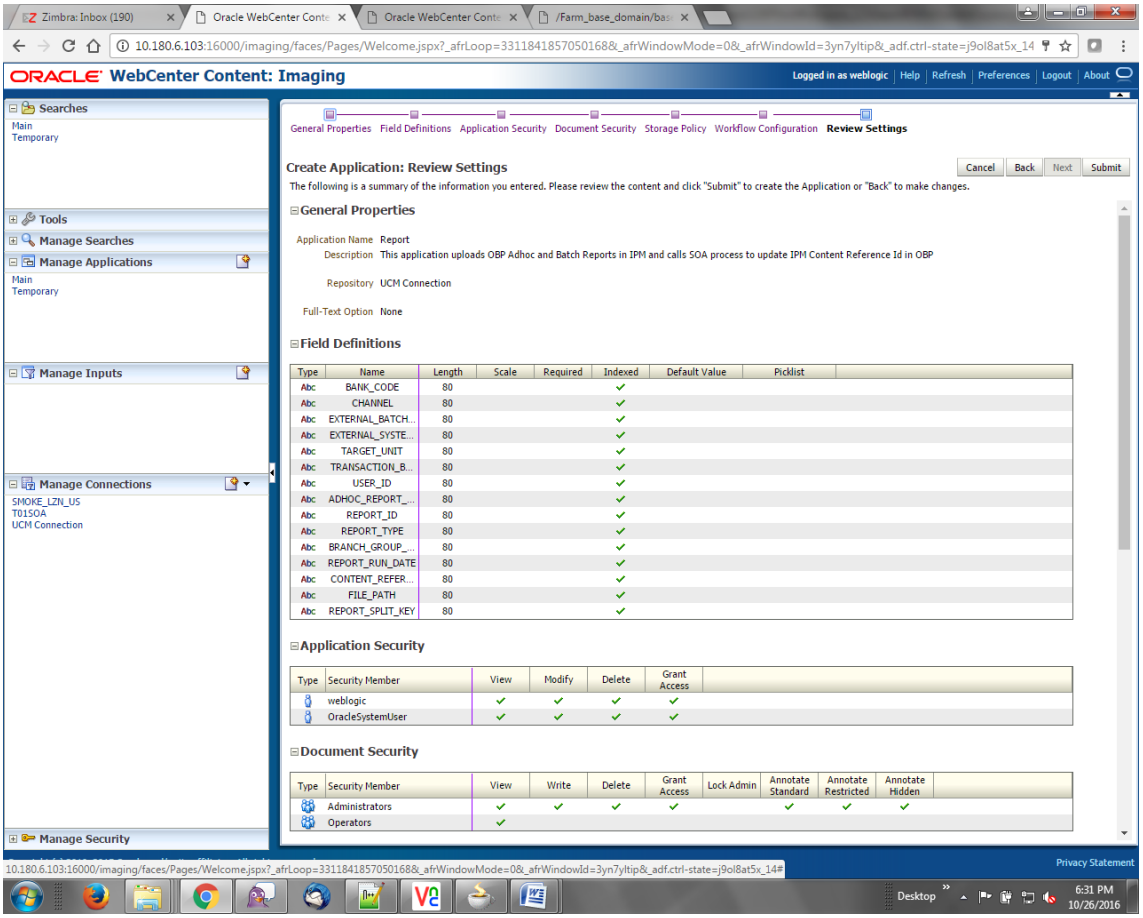


Figure 6–50 Report: Application Summary



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

Figure 6–51 Create Application: Review Settings

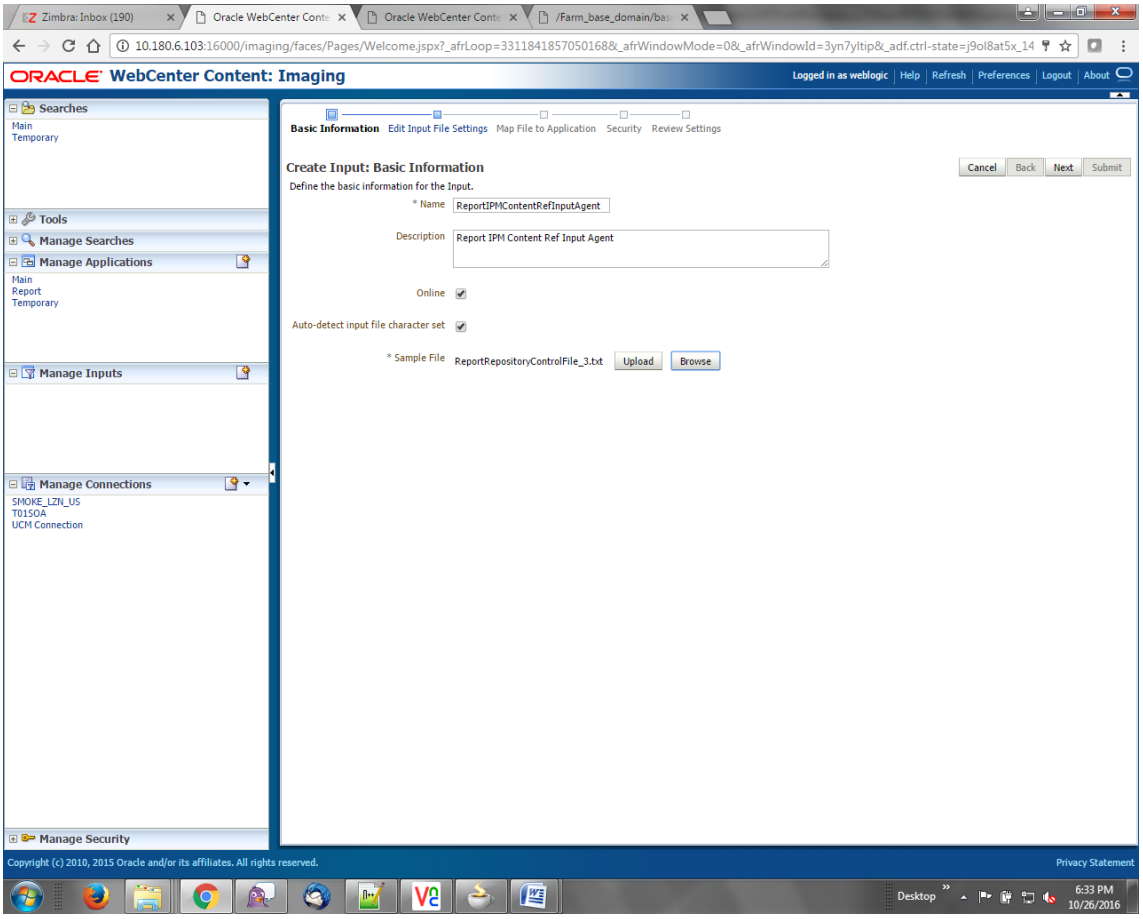


6.2.5 Manage Inputs for Input Agents

To manage workflow configuration:

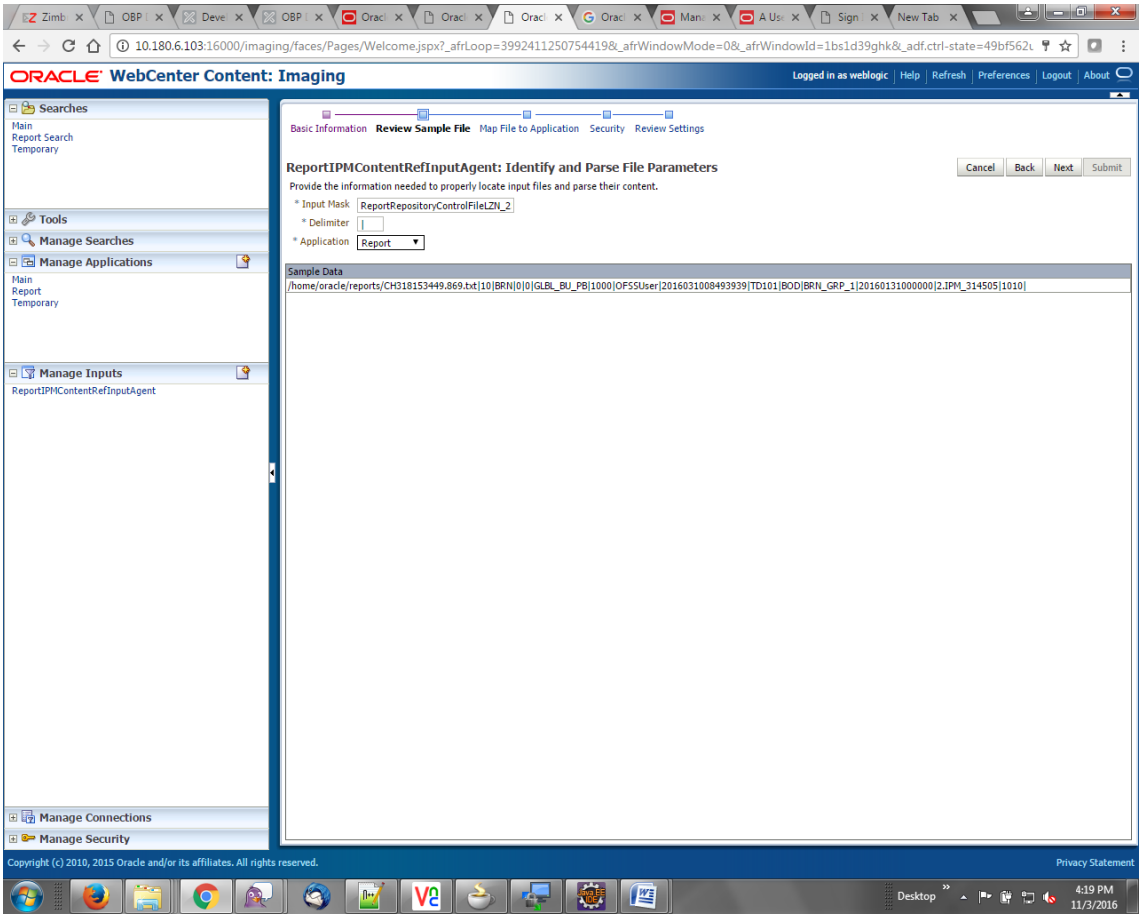
1. Log in to Image Processing Management (IPM).
2. Navigate to Manage Inputs section.

Figure 6–52 Manage Inputs



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

Figure 6–53 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

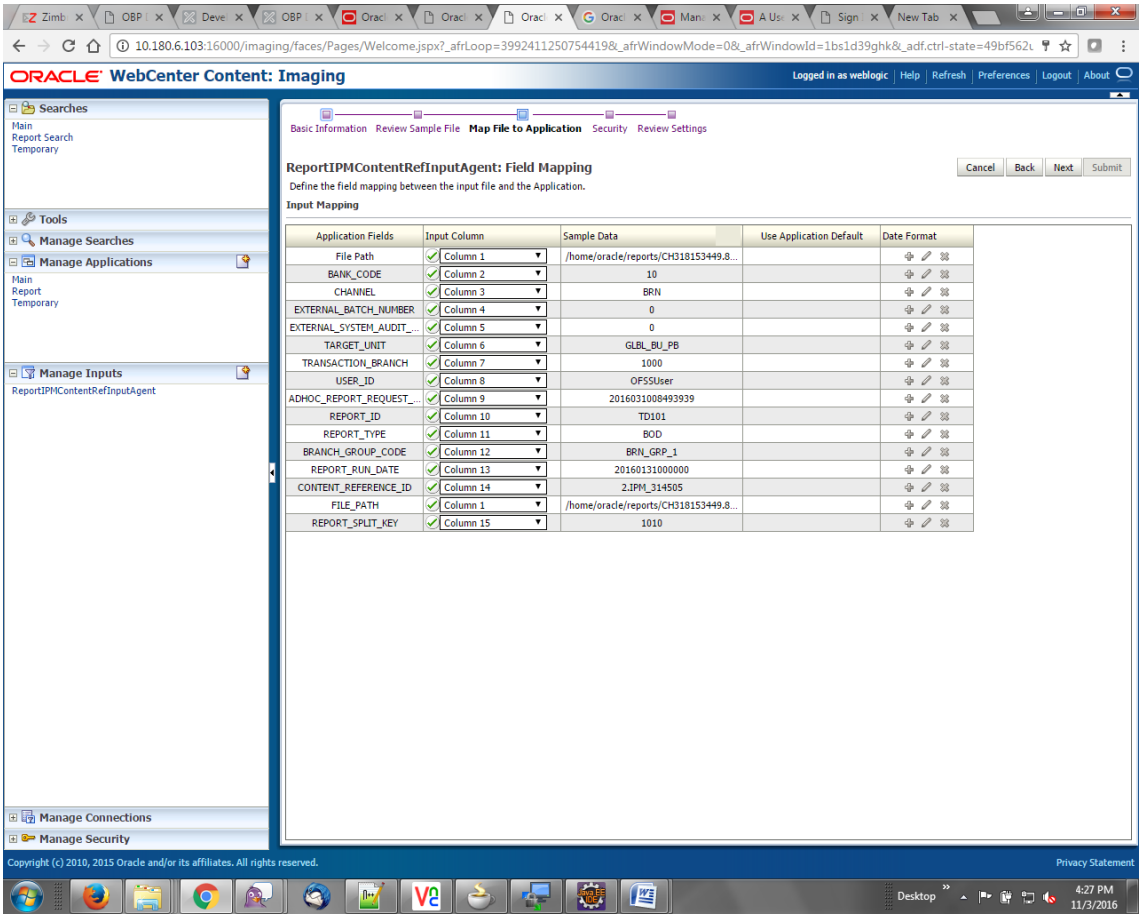
   select prop_value from flx_fw_config_var_b where prop_id = env.name;

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.

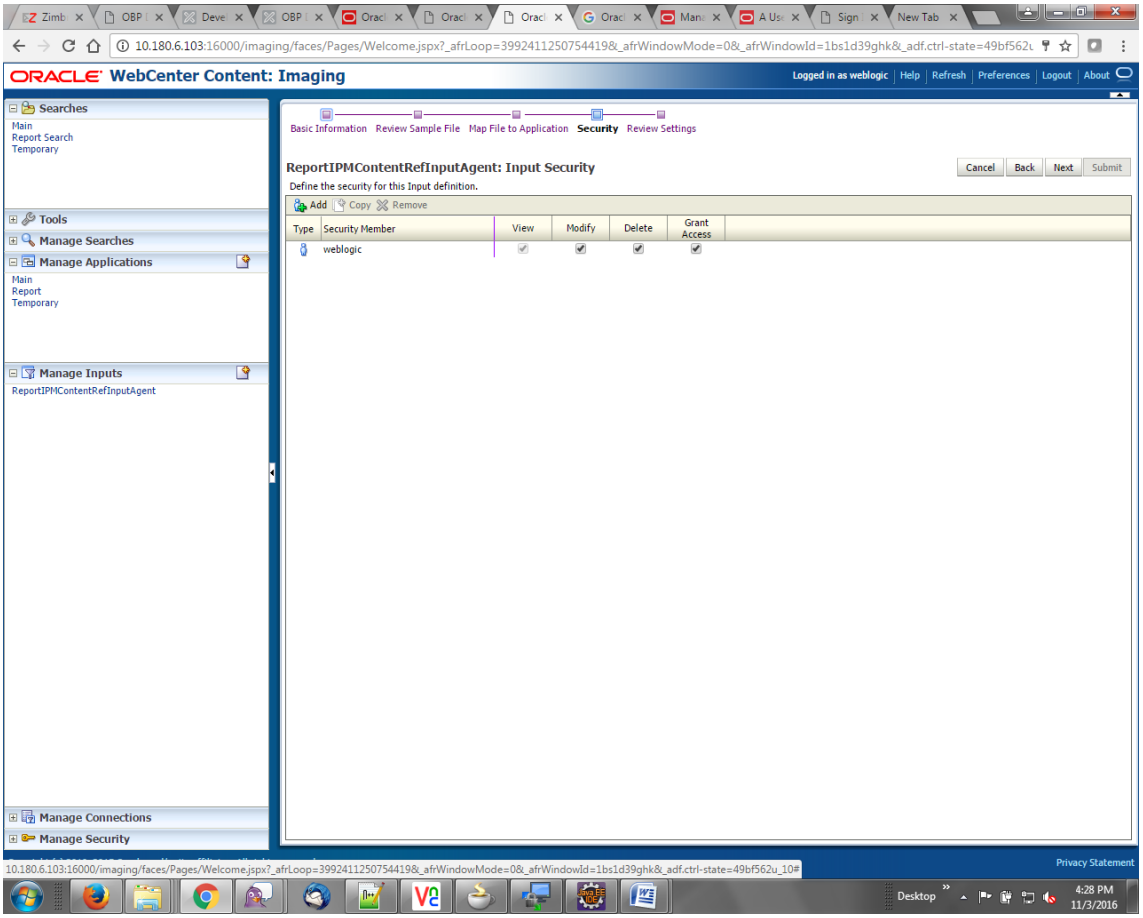
7. In the **Delimeter** field, enter the delimiter value as | (vertical bar character).
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 6–54 Input Agent Details: Field Mapping



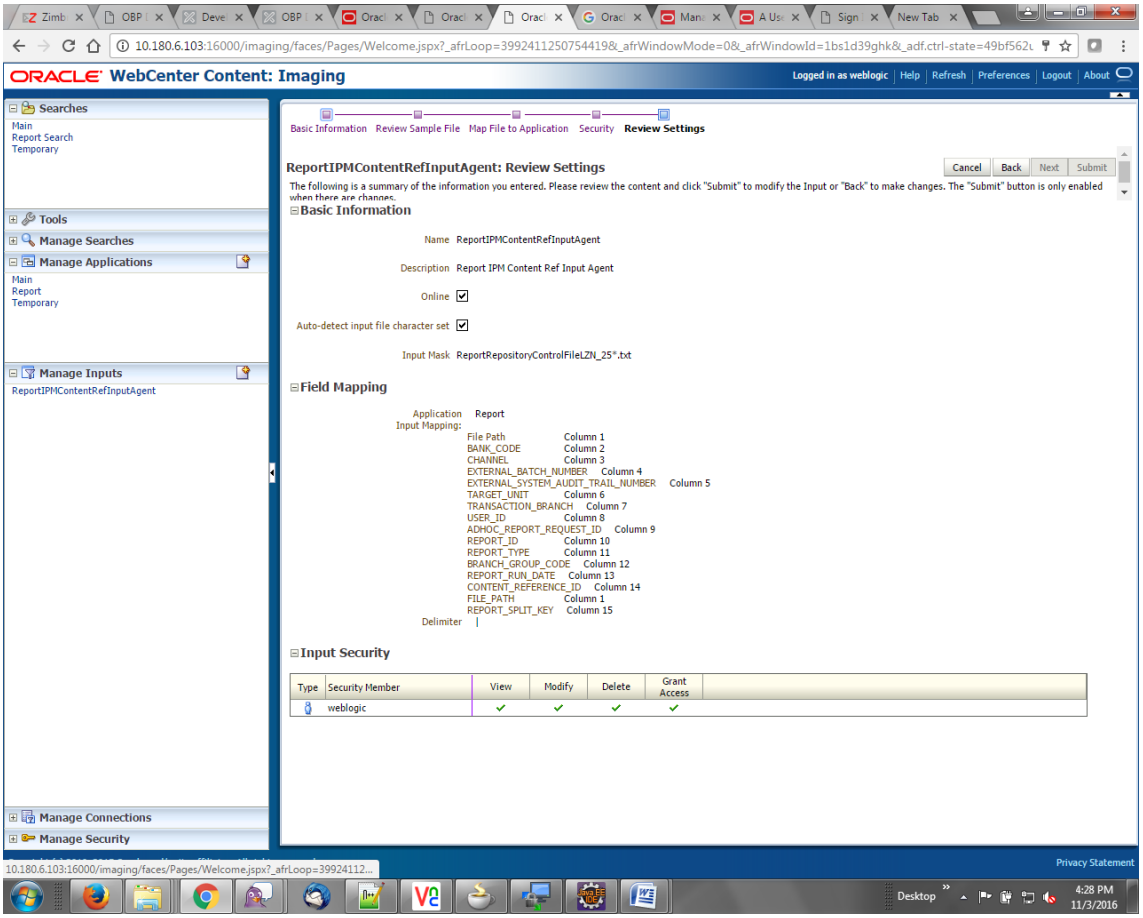
9. Select the access rights for user in the Security section and click **Next.**

Figure 6–55 Input Agent Details: Security



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

Figure 6–56 Input Agent Details: Review Settings



Note

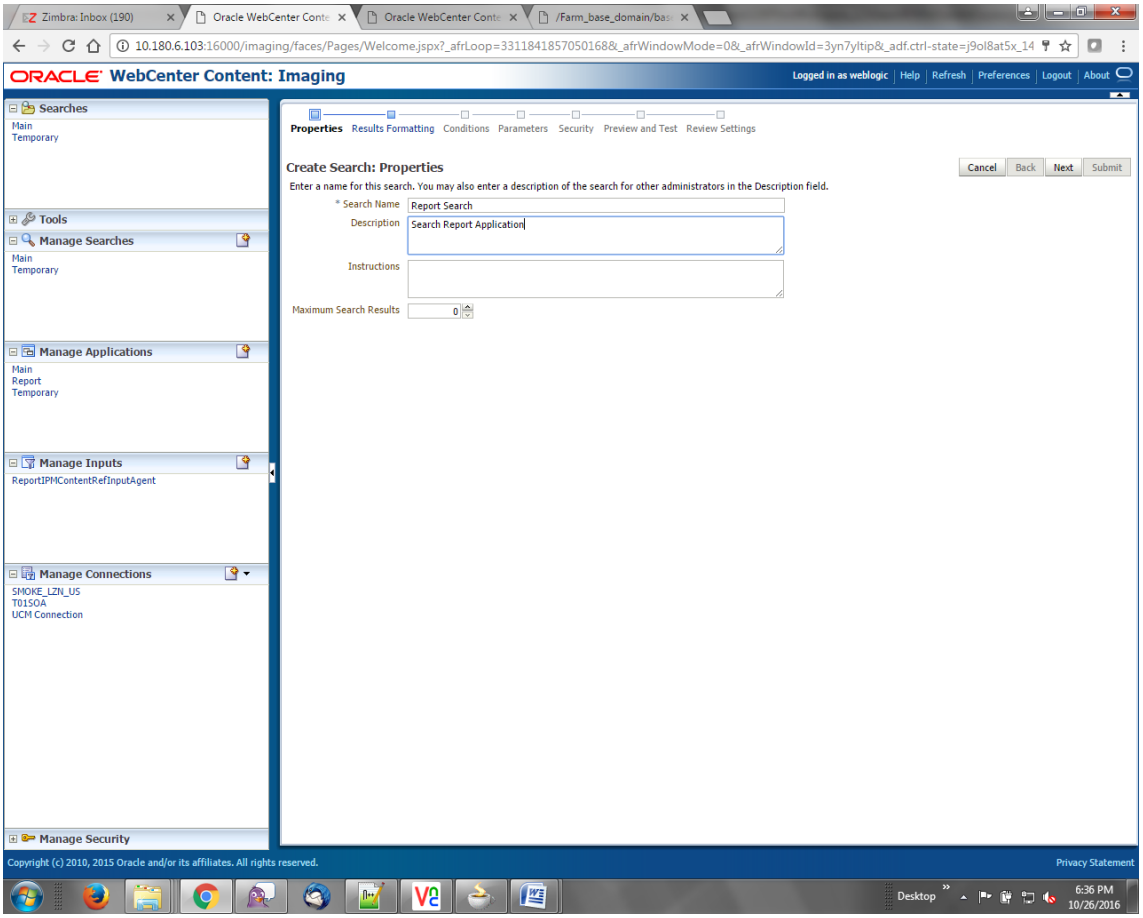
Do not forget to toggle online, else the input agent will not pick up any file for processing.

6.2.6 Manage Searches

To manage searches:

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

Figure 6–57 Create Search: Properties



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

Figure 6–58 Create Search: Results Formatting

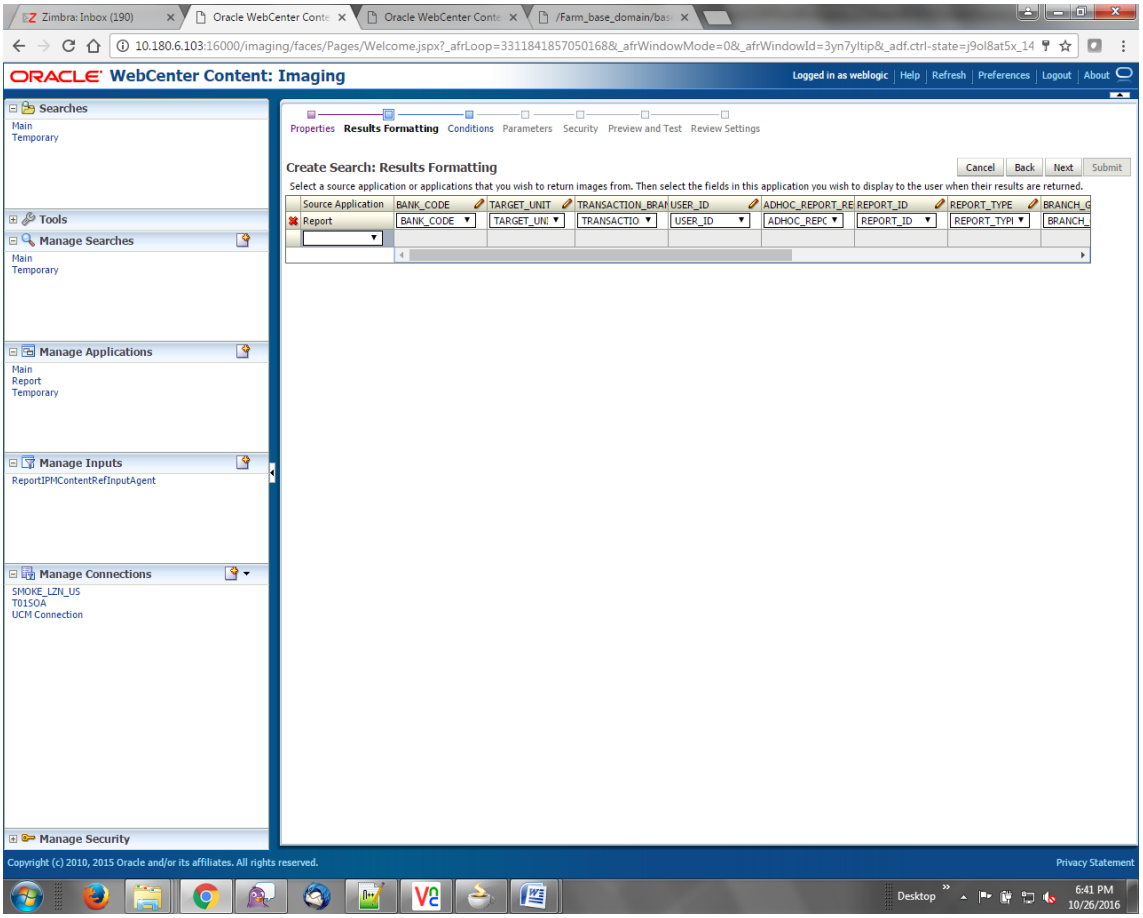


Figure 6–59 Create Search: Conditions

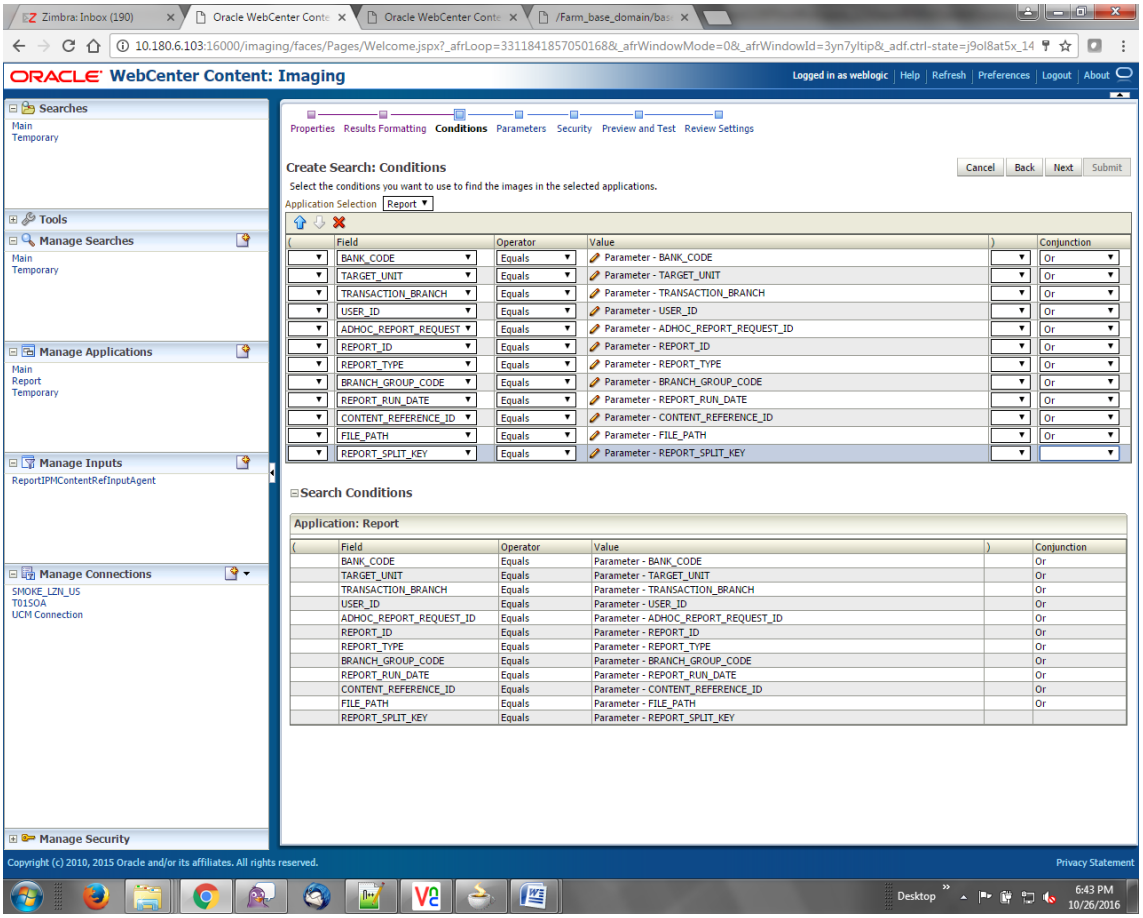
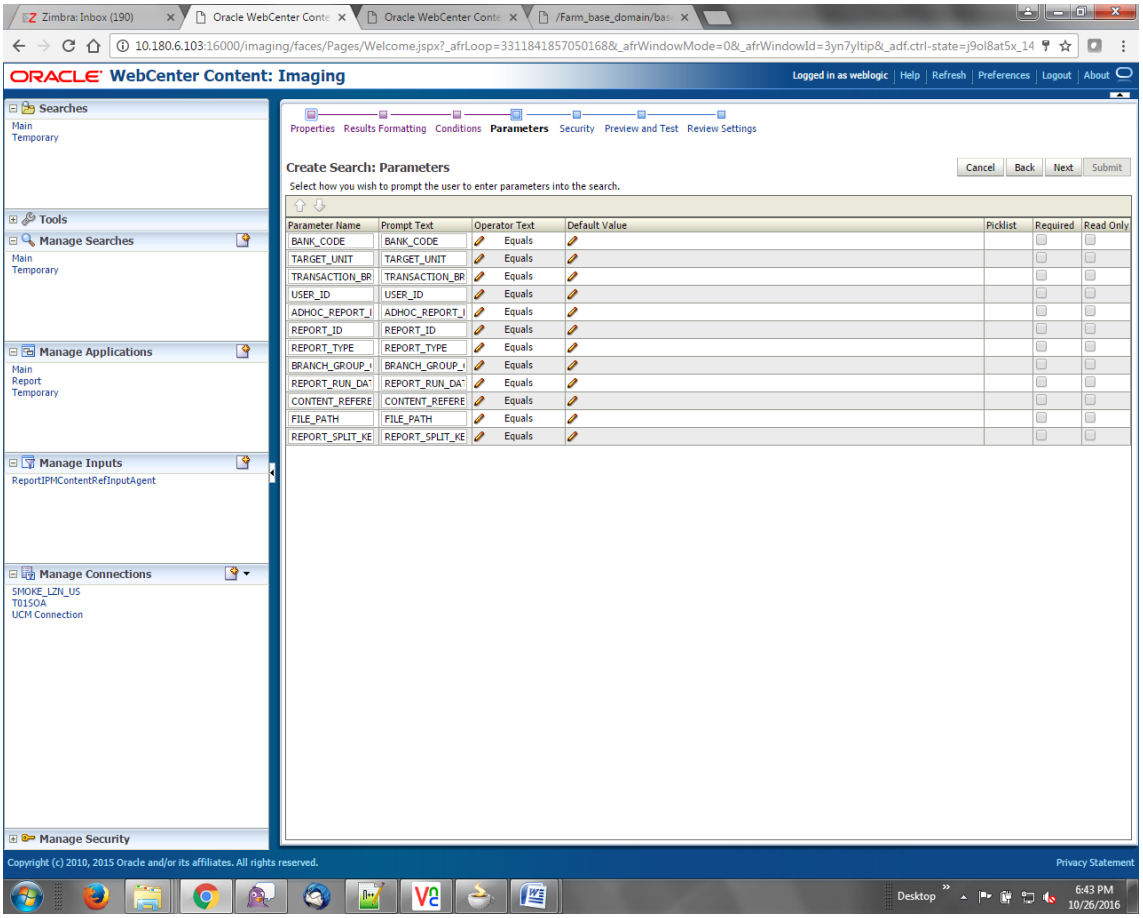
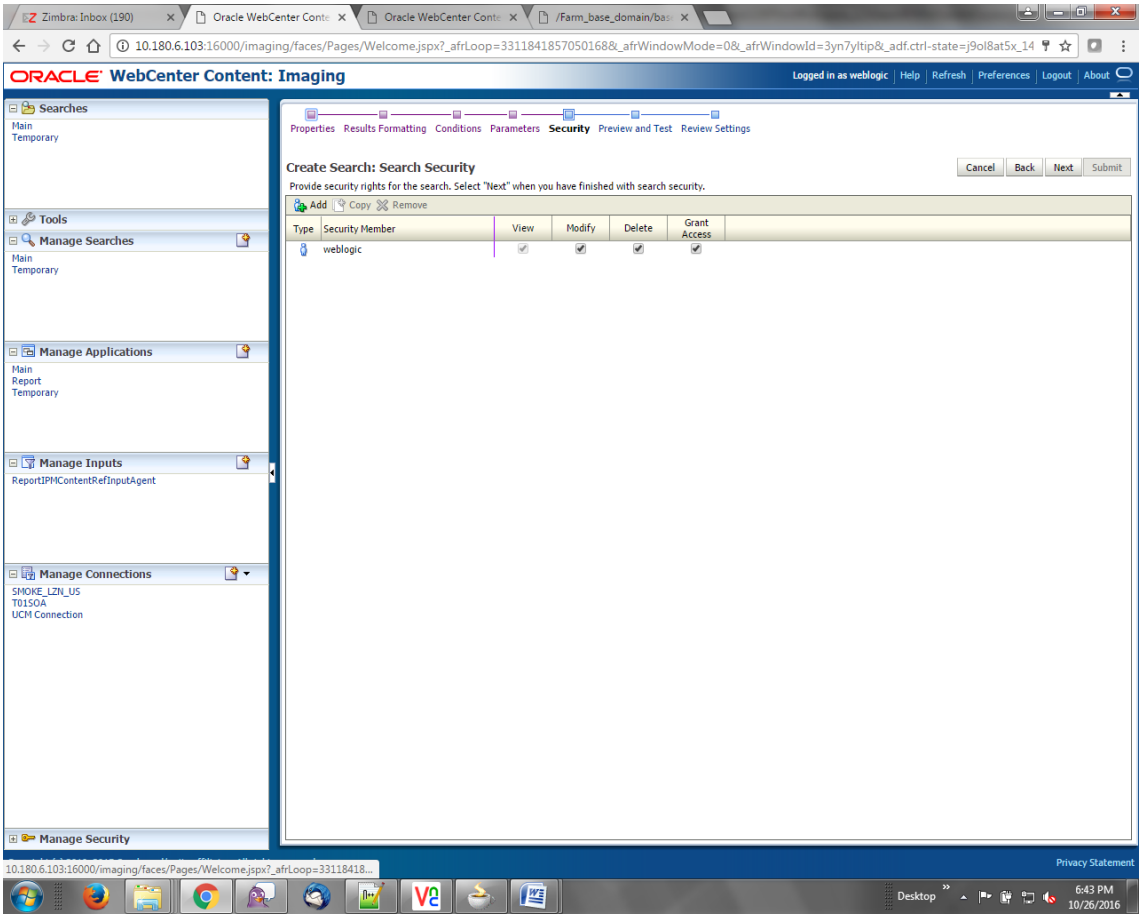


Figure 6–60 Create Search: Parameters



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

Figure 6–61 Create Search: Security



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

Figure 6–62 Create Search: Preview and Test

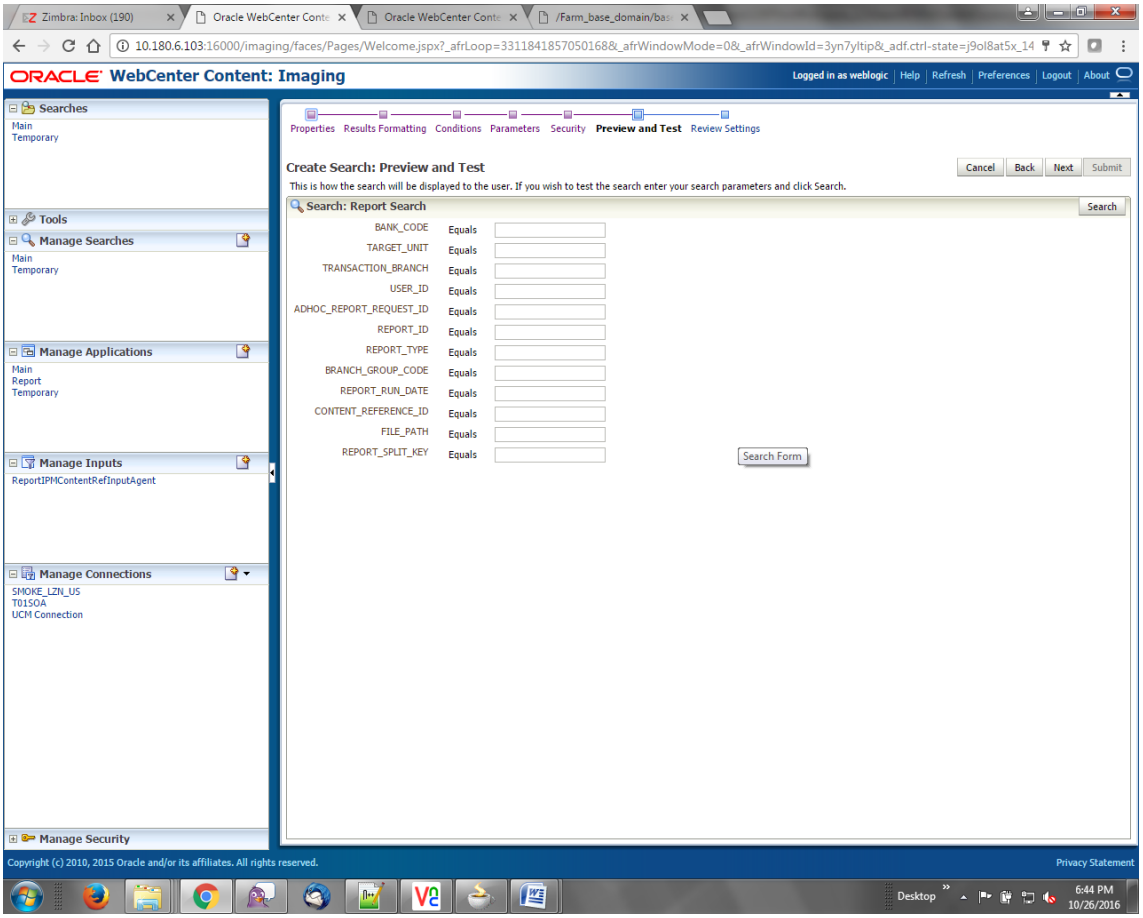
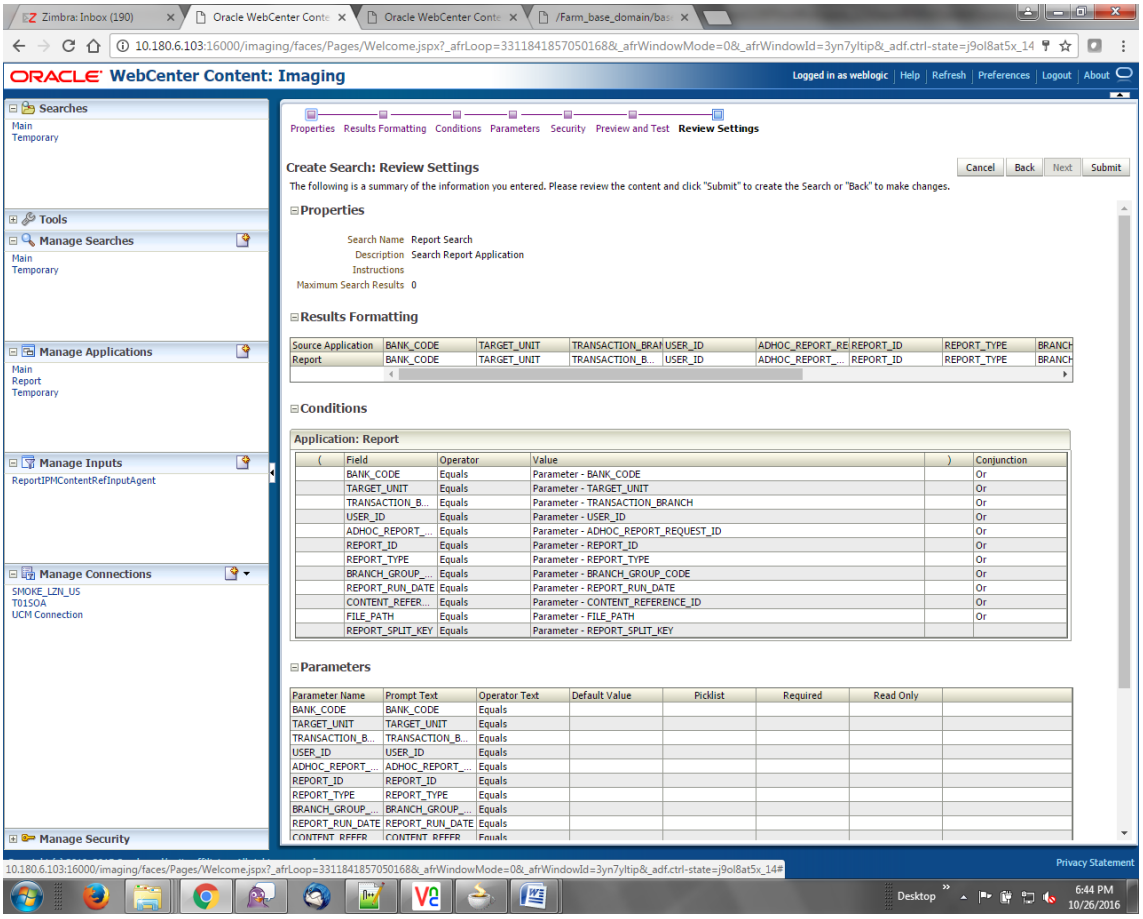


Figure 6–63 Create Search: Review Settings



7 Monitoring Servers Using Oracle Enterprise Manager

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

The OBEDM 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 OBEDM Servers, follow the procedures given in Oracle Banking Enterprise Default Management Management Pack Setup Guide.

8 Post Installation Verification

This chapter lists the steps required to verify the Oracle Banking Enterprise Default Management installation.

8.1 UI Domain Verification

To verify the UI domain installation:

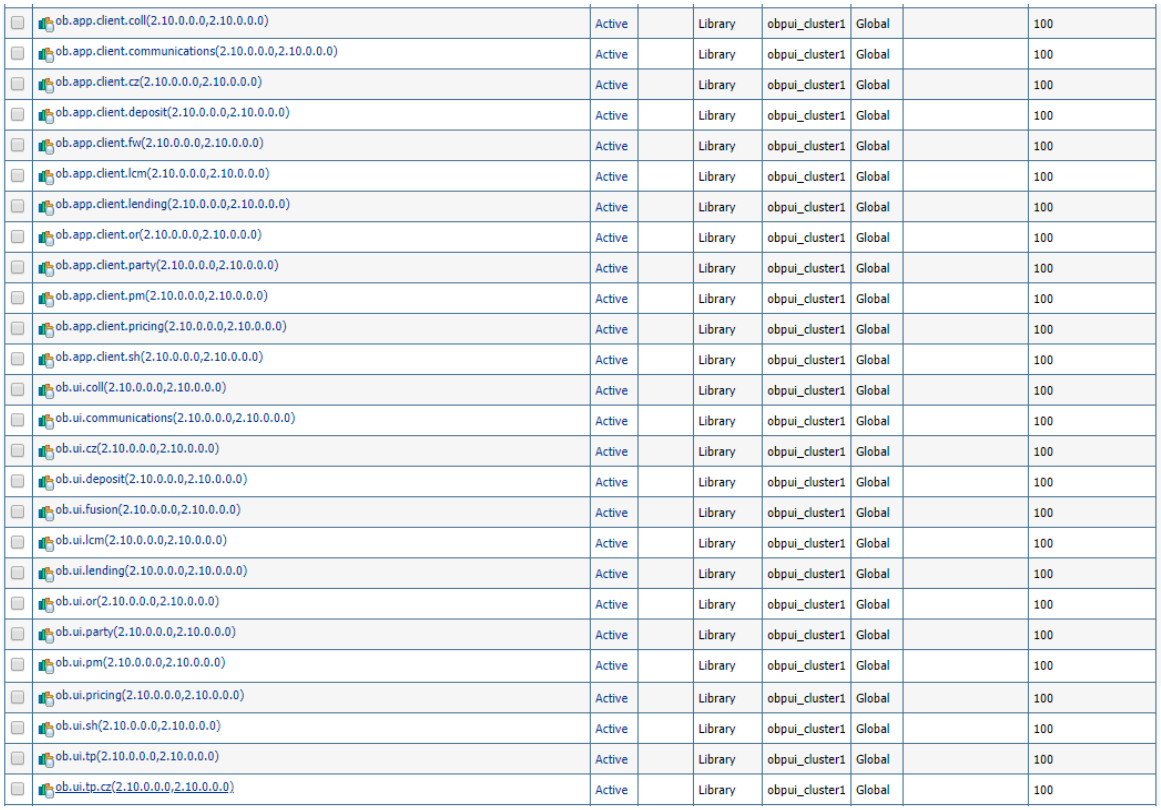
1. Start the UI domain Admin and Managed servers.
2. In the WebLogic console (<UI_IP>:<UI_ADMIN_PORT>/console), navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following OBEDM libraries and applications is *Active*.
    - Shared Libraries
        - ob.app.client.communications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

- ob.ui.pm
- 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.admin
- com.ofss.fc.ui.view.developer
- com.ofss.fc.ui.view.qa
- com.ofss.fc.ui.rest.ops
- com.ofss.fc.ui.view.mds
- com.ofss.fc.ui.view.obec
- com.ofss.fc.ui.view.obepm

Figure 8–1 UI Weblogic Console



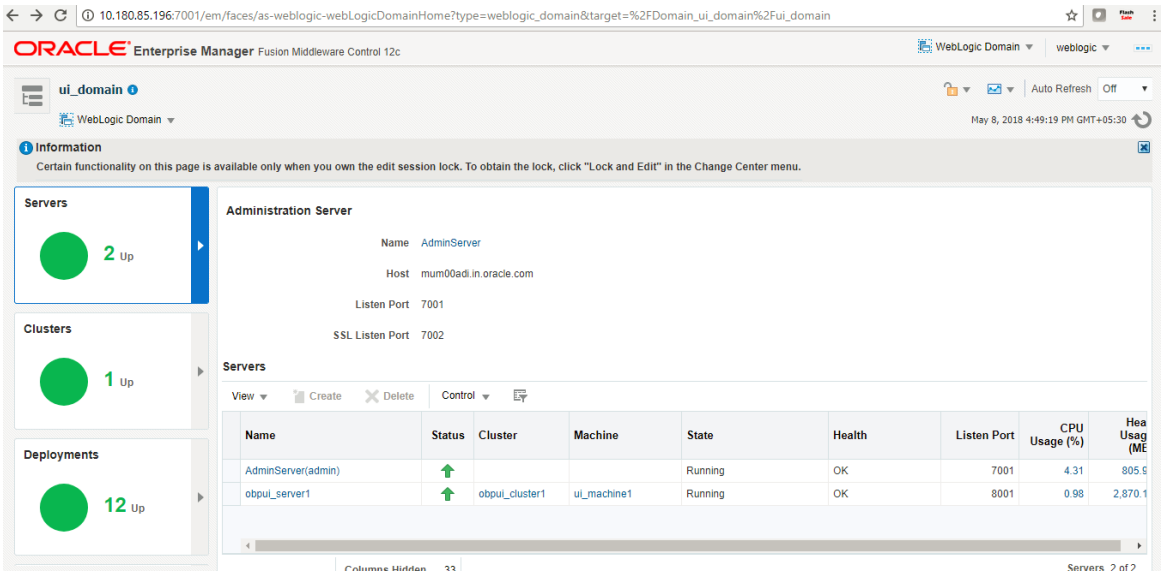
	ob.app.client.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.deposit(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.fw(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.lcm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.lending(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.or(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.app.client.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.deposit(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.fusion(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.lcm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.lending(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.or(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.tp(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
	ob.ui.tp.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100

Figure 8–2 UI Weblogic Console

com.ofss.fc.app.monitoring	Active	OK	Web Application	obpui_cluster1	Global		100
com.ofss.fc.app.ui.connector	Active	OK	Enterprise Application	obpui_cluster1	Global		80
com.ofss.fc.ui.rest.ops	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.admin	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.developer	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.mds	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.obec	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.obepm	Active	OK	Enterprise Application	obpui_cluster1	Global		100
com.ofss.fc.ui.view.qa	Active	OK	Enterprise Application	obpui_cluster1	Global		100

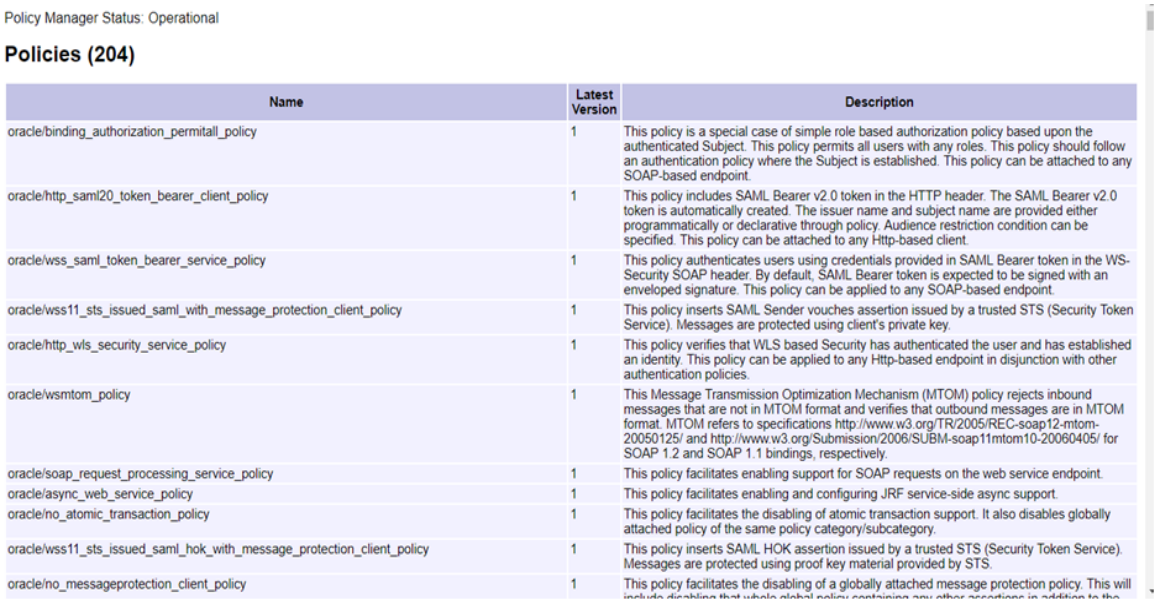
4. In EM console (<UI_IP>:<UI_ADMIN_PORT>/em), check the status of:
   - Cluster
   - Managed Servers
   - Applications

Figure 8–3 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 8–4 UI Admin wsm-pm Validator

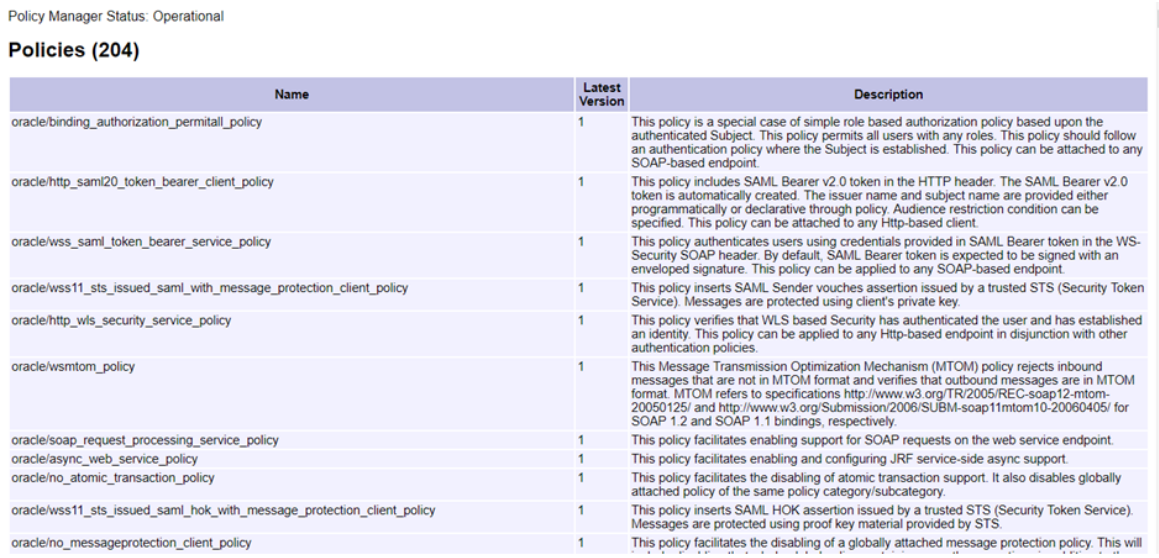


Policy Manager Status: Operational

Policies (204)

Name	Latest Version	Description
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/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/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/async_web_service_policy	1	This policy facilitates enabling and configuring JRF service-side async support.
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/no_messageprotection_client_policy	1	This policy facilitates the disabling of a globally attached message protection policy. This will

Figure 8–5 UI managed wsm-pm validator



Policy Manager Status: Operational

Policies (204)

Name	Latest Version	Description
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/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/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/async_web_service_policy	1	This policy facilitates enabling and configuring JRF service-side async support.
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/no_messageprotection_client_policy	1	This policy facilitates the disabling of a globally attached message protection policy. This will

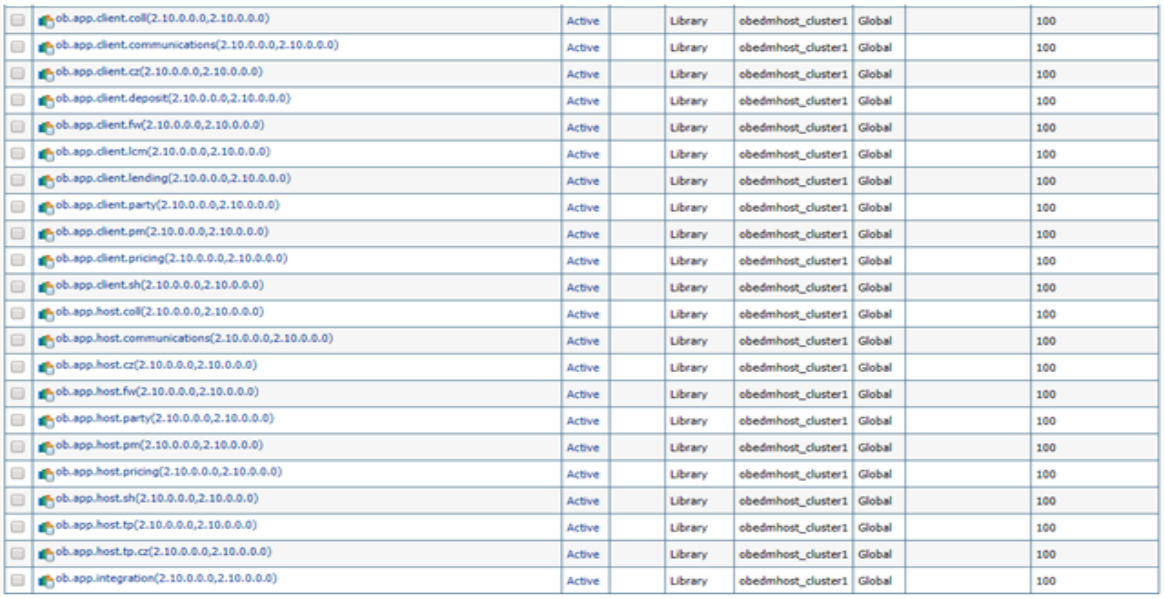
8.2 Host Domain Verification

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 OBEDM libraries and applications is *Active*.

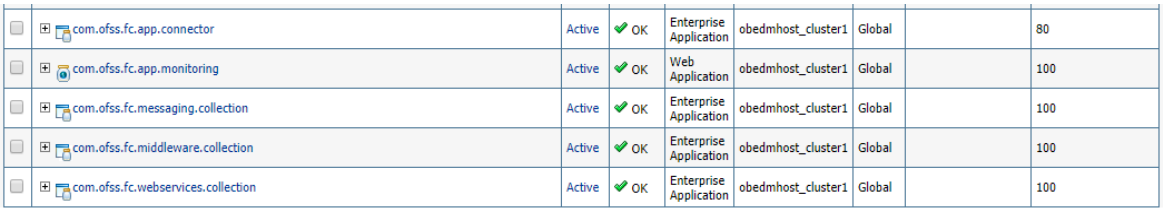
- Shared libraries
  - ob.app.client.communications
  - ob.app.client.coll
  - ob.app.client.cz
  - ob.app.client.deposit
  - ob.app.client.fw
  - ob.app.client.lcm
  - ob.app.client.lending
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.sh
  - ob.app.host.communications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

Figure 8–6 Host WebLogic Console



	ob.app.client.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.deposit(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.fw(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.lcm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.lending(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.client.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.fw(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.tp(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.host.tp.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100
	ob.app.integration(2.10.0.0.0,2.10.0.0.0)	Active		Library	obedmhost_cluster1	Global		100

Figure 8–7 Host WebLogic Console

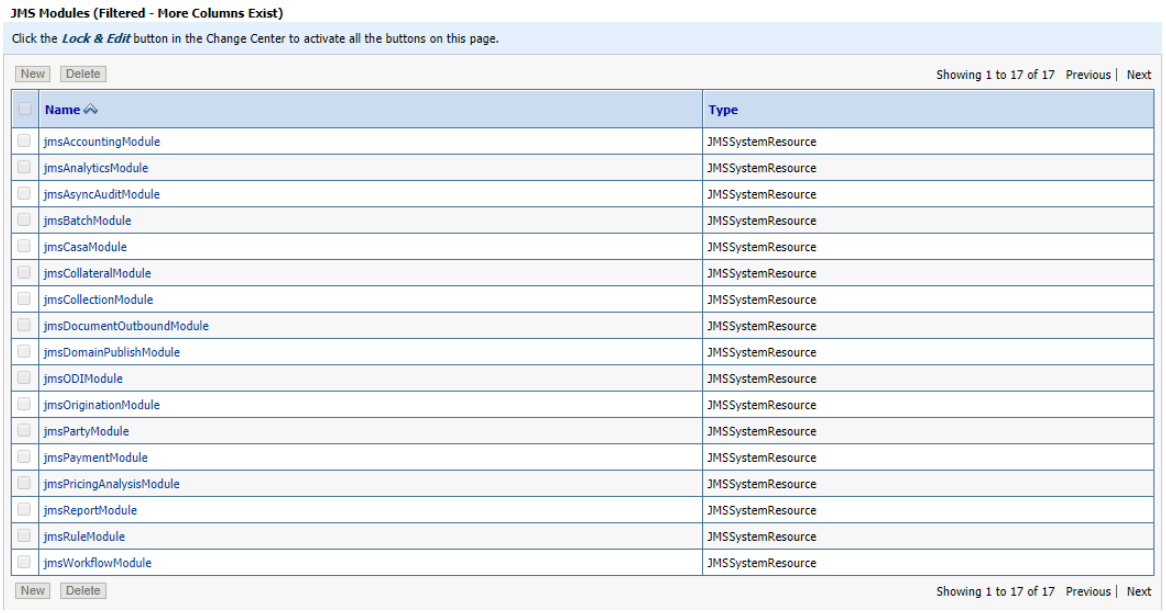


	com.ofss.fc.app.connector	Active	OK	Enterprise Application	obedmhost_cluster1	Global		80
	com.ofss.fc.app.monitoring	Active	OK	Web Application	obedmhost_cluster1	Global		100
	com.ofss.fc.messaging.collection	Active	OK	Enterprise Application	obedmhost_cluster1	Global		100
	com.ofss.fc.middleware.collection	Active	OK	Enterprise Application	obedmhost_cluster1	Global		100
	com.ofss.fc.webservices.collection	Active	OK	Enterprise Application	obedmhost_cluster1	Global		100

JMS Modules

The following JMS Modules are created during host installation:

Figure 8–8 Host WebLogic Console



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 8–9 HOST admin wsm-pm validator

Not secure | 10.180.34.248:7001/wsm-pm/validator

Policy Manager Status: Operational

Policies (204)

Name	Latest Version	Description
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/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/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

Figure 8–10 HOST managed wsm-pm validator

Name	Latest Version	Description
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/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/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

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.

9 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 Enterprise Default Management.

9.1 OBEDM Security Policy Seeding

For monitoring Oracle Banking Enterprise Default Management application security policy seeding, you can check the logs generated in $HOST_FMW/obpoidinstall/PolicyStoreSetup/logs.

9.2 OBEDM 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 OBEDM 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 OBEDM Host installation in which once the post install script for OBEDM host has secured itself against a LDAP (OID/OVD) it proceeds to restart the OBEDM 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 OBEDM 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

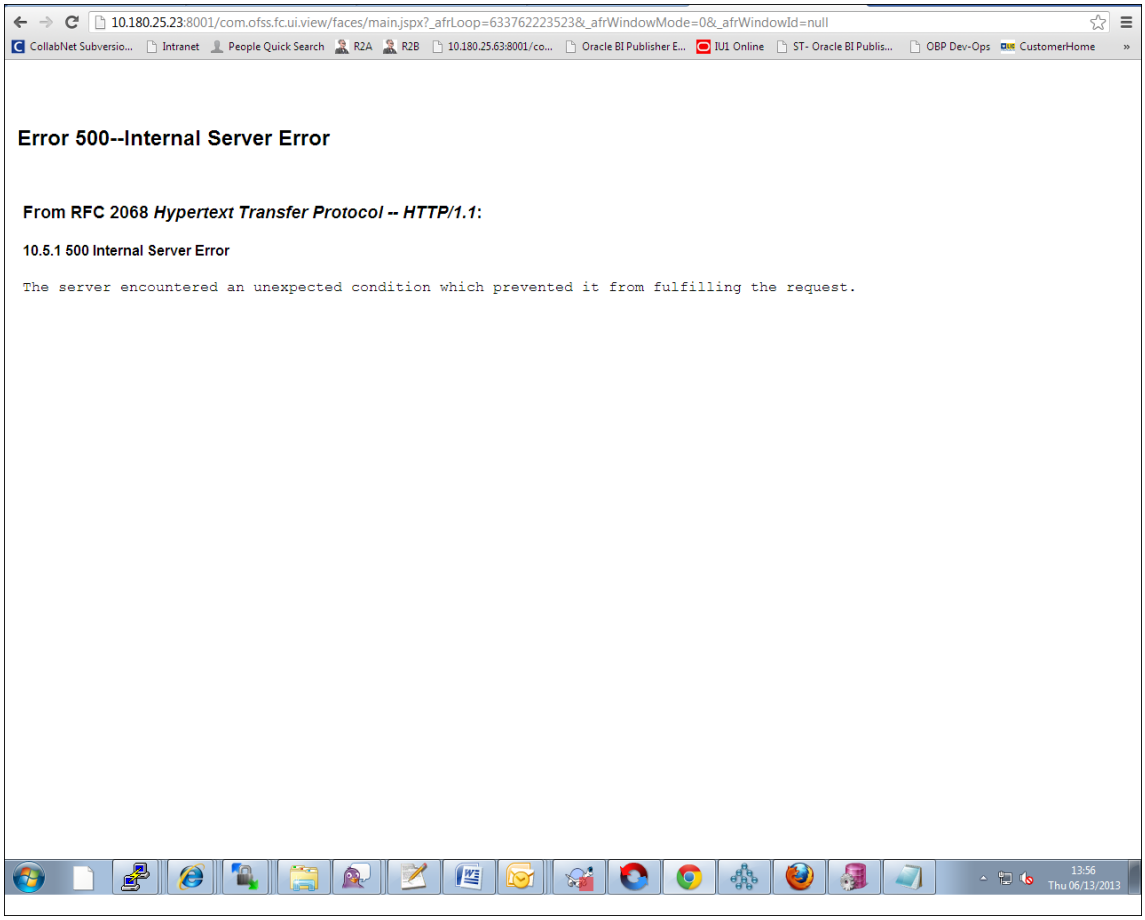
Once the post install script is completed successfully, you can start the domain servers and enter a dummy transaction to check the system correctness. If you face an error you can inspect the stderr log, the WebLogic domain managed server logs as well as the ofss logs under domain directory.

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.

9.3 Error on First Log in

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

Figure 9–1 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.

9.4 Login 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.

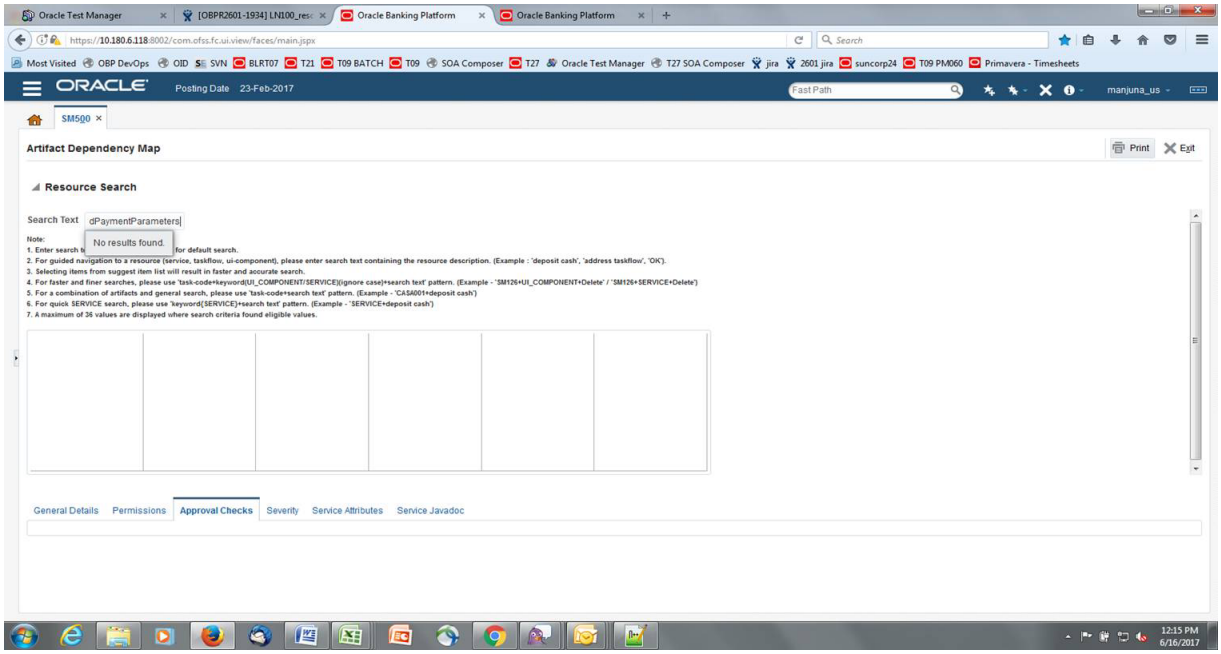
9.5 Artifacts Issue for SM500 page

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 9–2 Artifacts Issue for SM500 page



10 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Enterprise Default Management.

10.1 Manual Uninstall

Currently an installed OBEDM 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 Enterprise Default Management related database schemas run the RCU utility and choose the **Drop** option.