Oracle® Banking Enterprise Default Management

US Localization Installation Guide - Silent Installation

Release 2.10.0.0.0

F29509-01

April 2020

ORACLE®

Oracle Banking Enterprise Default Management US Localization Installation Guide - Silent Installation, Release 2.10.0.0.0

F29509-01

Copyright © 2017, 2020, Oracle and/or its affiliates.

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

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

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

Contents

Preface **16**
Audience 16
Documentation Accessibility 16
Organization of the Guide 16
Related Documents 17
Conventions 18
1 Getting Started **20**
1.1 About Oracle Banking Enterprise Default Management 20
1.2 About This Document 20
1.3 Assumptions 20
1.4 Limitations 21
1.5 Exclusions 21
2 Pre-Installation Configuration **22**
2.1 Setup Prerequisites 22
2.1.1 Hardware Environment 22
2.1.2 Software Environment 22
2.1.2.1 Certification Details 22
2.2 Installation Process Overview 25
2.3 Installation Checklist 26
2.3.1 Updating installobp***.properties 27
2.3.2 Database and WebLogic Domain Configuration 57
2.4 OID Schema Setup – Custom OBEDM Schema 58
2.4.1 Prerequisite – OID setup 58
2.4.2 Verify the OID installation 58

2.4.2.1 Start and Verify the OID processes 58
2.4.2.2 OPSS/OID Performance Tuning 59
2.4.2.3 Import OBEDM Specific LDIF files 65
2.4.2.4 Verify the import using ODSM or JXplorer 67
3 OBEDM US Localization SOA Media Pack Installation 70
3.1 Installation and Configuration Procedure 70
3.1.1 Preparatory Steps 70
3.1.2 Pre-Installation Steps 70
3.1.3 Installation Steps 71
3.2 Post Installation Configuration 75
4 OBEDM US Localization Host Media Pack Installation 80
4.1 Installation and Configuration Procedure 80
4.1.1 Preparatory Steps 80
4.1.2 Pre-Installation Steps 80
4.1.3 Installation Steps 81
4.2 Post Installation Configuration 91
5 OBEDM US Localization Presentation Media Pack Installation 100
5.1 Installation and Configuration Procedure 100
5.1.1 Preparatory Steps 100
5.1.2 Pre-Installation Steps 100
5.1.3 Installation Steps 101
5.2 Post Installation Configuration 108
6 Standalone Database Setup 116
6.1 Pre-Installation Steps 116
6.2 OBEDM Database Setup – RCU Installation 116
6.3 OBEDM Database Installation 117

6.3.1 Host DB Schema Creation and Verification 117
6.3.2 HOST DB schema ddl execution 117
6.3.3 HOST DB Schema Seeding 118
6.3.4 System Configuration DB Update Script Execution 118
7 OBEDM and IPM Integration 120
7.1 IPM Application Setup for OBEDM Content Management 120
7.1.1 UCM Connection 120
7.1.2 Main Application Configuration 127
7.1.2.1 Manage Application Configuration 127
7.1.2.2 Manage Searches 133
7.1.3 Temp Application Configuration 140
7.1.3.1 Manage Application Configuration 140
7.1.3.2 Manage Searches 146
7.2 IPM Configuration for Bulk Upload Process Setup 154
7.2.1 Prerequisites 154
7.2.2 Setting up the Connection Name 154
7.2.3 Setting up Input Agent Path 160
7.2.4 Create SOA Connection 162
7.2.5 Manage Workflow Configuration 167
7.2.6 Manage Inputs for Input Agents 174
7.2.7 Additional Steps 179
7.2.8 SSL Handshake Resolution 180
7.3 IPM Report Upload Setup 181
7.3.1 Prerequisites 181
7.3.2 Setting up the Connection Name 182
7.3.3 Setting up Input Agent Path 187

7.3.4 Create SOA Connection 189
7.3.5 Manage Application Configuration 194
7.3.6 Manage Inputs for Input Agents 203
7.3.7 Manage Searches 208
7.3.8 Additional Steps 215
8 ODI Configuration 218
8.1 Configuration Procedure 218
9 Monitoring Servers Using Oracle Enterprise Manager 220
10 Post Installation Verification 222
10.1 UI Domain Verification 222
10.2 Host Domain Verification 225
10.3 SOA Domain Verification 229
10.4 BPM Worklist Window Setting 231
11 Errors and Remedies 234
11.1 OBEDM Domain Installation 234
11.2 OBEDM Security Policy Seeding 234
11.3 OBEDM Domain Post Installation 234
11.4 Error on First Log in 235
11.5 Login Issues 236
11.6 SOA Setup in Cluster 236
11.6.1 "COMPONENTTYPE": invalid identifier error 236
11.7 BPM Worklist Task Issue 237
11.8 Artifacts Issue for SM500 page 238
11.9 ra/FCRJConnectorSOA connector issue 239
11.10 Humantask Startup Issue 240
12 Uninstalling the Application 242

12.1 Manual Uninstall 242

List of Figures

Figure 2–1 Installation Overview 26
Figure 2–2 JXplorer 68
Figure 3–1 Steps in installobpsoa.sh script 72
Figure 3–2 Verification of Properties 72
Figure 3–3 Verification of Properties 73
Figure 3–4 Confirmation to Proceed Domain Installation (cont.) 73
Figure 3–5 Copying and Extraction of obpinstall-ui-soa.zip 74
Figure 3–6 Copying and Extraction of obpinstall-ui-soa.zip 74
Figure 3–7 Copying and Extraction of obpinstall-ui-soa.zip 75
Figure 3–8 Domain Creation Confirmation 75
Figure 3–9 Starting Post Installation 77
Figure 3–10 Starting Post Installation (contd) 77
Figure 3–11 SOA Post Installation Completion 78
Figure 3–12 Go to Web Services Configuration 79
Figure 3–13 Attach Policy 79
Figure 4–1 Steps in installobphost.sh script 82
Figure 4–2 Verification of Properties 83
Figure 4–3 Verification of Properties (contd) 83
Figure 4–4 Verification of Properties (contd) 84
Figure 4–5 Verification of Properties (contd) 84
Figure 4–6 Confirmation and Copying of Installables to Target Machine 85
Figure 4–7 Confirmation and Copying of Installables to Target Machine (contd) 86
Figure 4–8 Confirmation and Copying of Installables to Target Machine (contd) 86
Figure 4–9 Domain Installation Confirmation 87

Figure 4–10 Untar the policyStoreSetup and Copy on destination location 87
Figure 4–11 Untar the policyStoreSetup and Copy on destination location (contd) .. 88
Figure 4–12 Untar the policyStoreSetup and Copy on destination location (contd) .. 89
Figure 4–13 Policy Seeding 90
Figure 4–14 Policy Seeding (contd) 91
Figure 4–15 Host Domain Admin Server Credentials 92
Figure 4–16 Host Domain Post Installation Script Execution 93
Figure 4–17 Host Domain Post Installation Script Execution (contd) 94
Figure 4–18 Host Domain Post Installation Script Execution (contd) 95
Figure 4–19 Host Domain Post Installation Script Execution (contd) 96
Figure 4–20 Host Domain Post Installation Script Execution Summary 97
Figure 5–1 Steps in installobpui.sh script 102
Figure 5–2 Confirmation to Proceed Domain Installation 103
Figure 5–3 Confirmation to Proceed Domain Installation (contd) 104
Figure 5–4 Confirmation to Proceed Domain Installation (contd) 105
Figure 5–5 Copying and Extraction of obpinstall-ui-soa.zip 106
Figure 5–6 Copying and Extraction of obpinstall-ui-soa.zip (contd) 107
Figure 5–7 Domain Creation Confirmation 108
Figure 5–8 UI Admin Server Credentials 109
Figure 5–9 UI Admin Server Running 109
Figure 5–10 UI Admin Server Running (contd) 110
Figure 5–11 Starting Post Installation 111
Figure 5–12 Starting Post Installation (contd) 112
Figure 5–13 Continuation of Post-Installation 113
Figure 5–14 Continuation of Post-Installation (contd) 114
Figure 7–1 IPM Imaging Console - Login page 121

Figure 7–2 IPM - Welcome page 122
Figure 7–3 Create Content Server Connection 123
Figure 7–4 UCM: Basic information 124
Figure 7–5 UCM: Connection Settings 125
Figure 7–6 UCM: Connection Security 126
Figure 7–7 UCM: Review Settings 127
Figure 7–8 Main: General Properties 128
Figure 7–9 Main: Field Definitions 129
Figure 7–10 Field Definitions (cont.) 129
Figure 7–11 Main: Application Security 130
Figure 7–12 Main: Document Security 131
Figure 7–13 Main: Storage Policy 132
Figure 7–14 Main: Review Settings 133
Figure 7–15 Main: Properties 134
Figure 7–16 Main: Results Formatting 135
Figure 7–17 Main: Conditions 136
Figure 7–18 Main: Parameters 137
Figure 7–19 Main: Search Security 138
Figure 7–20 Main: Preview and Test 139
Figure 7–21 Main: Review Settings 140
Figure 7–22 Temporary: General Properties 141
Figure 7–23 Temporary: Field Definitions 142
Figure 7–24 Temporary: Application Security 143
Figure 7–25 Temporary: Document Security 144
Figure 7–26 Temporary: Storage Policy 145
Figure 7–27 Temporary: Review Settings 146

Figure 7–28 Temporary: Properties 147
Figure 7–29 Temporary: Results Formatting 148
Figure 7–30 Temporary: Conditions 149
Figure 7–31 Temporary: Parameters 150
Figure 7–32 Temporary: Search Security 151
Figure 7–33 Temporary: Preview and Test 152
Figure 7–34 Temporary: Review Settings 153
Figure 7–35 EM Console Login 155
Figure 7–36 Click Weblogic Domain: ipm domain 156
Figure 7–37 Navigate to Weblogic Domain --> Security --> Credentials 157
Figure 7–38 Create Map oracle.wsm.security 158
Figure 7–39 Create Key basic.credentials 159
Figure 7–40 ipm_domain: Credentials Created 160
Figure 7–41 Navigate to Weblogic Domain --> System MBean Browser 161
Figure 7–42 InputDirectories: Enter Input Agent Path 162
Figure 7–43 Manage Connections: Create Workflow Connection 163
Figure 7–44 IUTSOA: Basic Information 164
Figure 7–45 IUTSOA: Workflow Settings 165
Figure 7–46 IUTSOA: Connection Security 166
Figure 7–47 IUTSOA: Review Settings 167
Figure 7–48 Main: Application Summary 168
Figure 7–49 Manage Applications - Server Properties 169
Figure 7–50 Manage Applications - Component Properties 170
Figure 7–51 Manage Applications - Payload Properties 171
Figure 7–52 Manage Applications - Workflow Configuration 172
Figure 7–53 Field Definitions 173

Figure 7–54 Main: Application Summary 174
Figure 7–55 Input Agent: Basic Information 175
Figure 7–56 Input Agent: Input Mask 176
Figure 7–57 Input Agent: File Parameters 177
Figure 7–58 Input Agent: Fields Mapping 178
Figure 7–59 Input Agent: Summary 179
Figure 7–60 flx_fw_config_all_b table 180
Figure 7–61 SSL Handshake Resolution 181
Figure 7–62 Log in to Enterprise Manager (EM) console 182
Figure 7–63 Click Weblogic Domain: ipm domain 183
Figure 7–64 Navigate to Weblogic Domain --> Security --> Credentials 184
Figure 7–65 Create Map oracle.wsm.security 185
Figure 7–66 Create Key: basic.credentials 186
Figure 7–67 ipm_domain: Credentials Created 187
Figure 7–68 Navigate to Weblogic Domain --> System MBean Browser 188
Figure 7–69 InputDirectories: Enter Input Agent Path 189
Figure 7–70 Manage Connections: Create Workflow Connection 190
Figure 7–71 IUTSOA: Basic Information 191
Figure 7–72 IUTSOA: Workflow Settings 192
Figure 7–73 IUTSOA: Connection Security 193
Figure 7–74 IUTSOA: Review Settings 194
Figure 7–75 Create Application: General Properties 195
Figure 7–76 Report: Field Definitions 196
Figure 7–77 Create Application: Applications Security 197
Figure 7–78 Create Application: Document Security 198
Figure 7–79 Create Application: Storage Policy 199

Figure 7–80 Report: Workflow Configuration - Server Properties 200
Figure 7–81 Report: Workflow Configuration - Component Properties 201
Figure 7–82 Report: Application Summary 202
Figure 7–83 Create Application: Review Settings 203
Figure 7–84 Manage Inputs 204
Figure 7–85 Input Agent Details: Input Mask 205
Figure 7–86 Input Agent Details: Field Mapping 206
Figure 7–87 Input Agent Details: Security 207
Figure 7–88 Input Agent Details: Review Settings 208
Figure 7–89 Create Search: Properties 209
Figure 7–90 Create Search: Results Formatting 210
Figure 7–91 Create Search: Conditions 211
Figure 7–92 Create Search: Parameters 212
Figure 7–93 Create Search: Security 213
Figure 7–94 Create Search: Preview and Test 214
Figure 7–95 Create Search: Review Settings 215
Figure 7–96 Component Properties 217
Figure 10–1 UI Weblogic Console 223
Figure 10–2 UI Weblogic Console 224
Figure 10–3 UI EM Console Status Check 224
Figure 10–4 UI Admin wsm-pm Validator 225
Figure 10–5 UI managed wsm-pm validator 225
Figure 10–6 Host WebLogic Console 227
Figure 10–7 Host WebLogic Console 227
Figure 10–8 Host WebLogic Console 228
Figure 10–9 HOST admin wsm-pm validator 228

Figure 10–10 HOST managed wsm-pm validator 229
Figure 10–11 SOA WebLogic Console 231
Figure 10–12 SOA WebLogic Console 231
Figure 10–13 BPM Worklist Window Settings 232
Figure 11–1 SOA Domain Error 234
Figure 11–2 Error on First Log In 236
Figure 11–3 BPM Worklist Task issue 238
Figure 11–4 Artifacts Issue for SM500 page 239
Figure 11–5 Settings for javax.resource.cci.ConnectionFactory page 240

List of Tables

Table 2–1 Hardware and OS 22

Table 2–2 List of Software 23

Table 2–3 Notes 24

Table 2–4 Values for updating installobp***.properties 27

Table 2–5 Oracle Banking Enterprise Default Management DB and WebLogic Domain Configuration 57

Table 2–6 Parameter Values to be Changed 59

Table 2–7 Suggested values for Tuning and Alter Command 60

Table 2–8 Properties 64

Table 2–9 Order of Execution 66

Table 7–1 PROP ID Values 180

Table 7–2 PROP ID Values 215

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
- Documentation Accessibility
- Organization of the Guide
- Related Documents
- Conventions

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, Oracle OID and Oracle SOA Suite.

Documentation Accessibility

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

Access to Oracle Support:

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

Organization of the Guide

This document contains:

Chapter 1 Getting Started

This chapter presents an overview of Oracle Banking 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 SOA 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 SOA (Integration Server) Media pack.

Chapter 4 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 5 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 6 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 7 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 8 ODI Configuration

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

Chapter 9 Monitoring Servers Using Oracle Enterprise Manager

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

Chapter 10 Post Installation Verification

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

Chapter 11 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 12 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
ODI	Oracle Data Integrator
OEL	Oracle Enterprise Linux
OEM	Oracle Enterprise Manager
OID	Oracle Internet Directory
OIM	Oracle Identity Manager
RCU	Repository Creation Utility
sh	Unix Shell file
SOA	Service Oriented Architecture Tier
SVN	Source Code Version Repository
UI	User Interface, that is Presentation Tier
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)
- Integration Server (Oracle Banking Enterprise Default Management Integration and Approval Processes hosted on Oracle SOA)
- Security Configuration (Seeding security to OID)
- Seed Data Configuration (Seeding data to Core banking OLTP Database Server)

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

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

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

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

1.3 Assumptions

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

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

- The 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
6	4	32	200	As per SOA certification matrix.	Oracle SOA 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 (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
2	SOA	Banking App	Oracle SOA Suite 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
3	OBEDM HOST	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
4	OID	Security	Oracle Internet Directory 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
5	IPM	Document	Oracle WebCenter - Content 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
6	ODI	Integration	Oracle Data Integrator 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
7	OIM	Security	Oracle Identity Manager 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
8	OAM	Security	Oracle Access Manager 12.2.1.3.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.3.0) Java Version jdk1.8.0_xx (jdk1.8.0_172) Oracle Linux 7.5 64-bit
9	OEM	Management	Oracle Enterprise Manager 13.2.0.0.0 As per certification matrix of Oracle Enterprise Manager 13.2.0.0.0
10	EM Agent Installation	Management	Push from OEM Console
11	OBEDM Database	Database	Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 Oracle Linux 7.5 64-bit
12	HTTP Server	Web Server	Oracle HTTP Server 12.2.1.3.0

The following are some notes related to the software.

Table 2–3 Notes

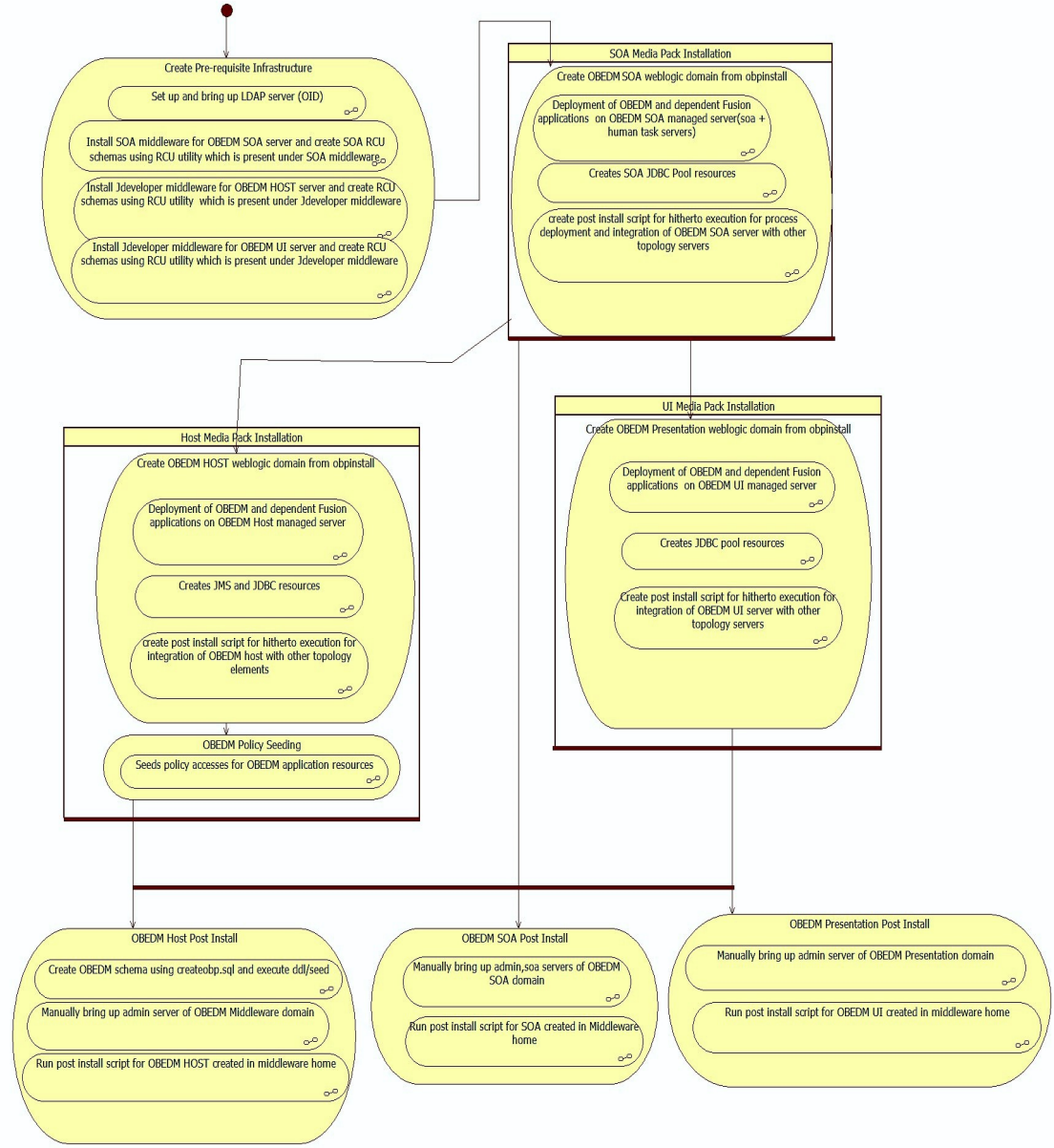
Serial Number	Description
1	OBEDM release has been certified with OEL version 7.5 during the release cycle. It is strongly recommended to use the versions on which the release is certified.
2	ODI_OUTBOUND_USERNAME and ODI_OUTBOUND_PASSWORD The OBEDM installer will not abort the installation if this component is not present. It can be installed later. However, it is strongly recommended to use the actual property values instead of default property values during the installation. Else, the actual values for ODI_OUTBOUND_USERNAME and ODI_OUTBOUND_PASSWORD once available have to be manually updated in the 'ra/FCRJConnectorODI' jndi property of com.ofss.fc.app.connector.ear application inside middleware host server after the entire installation completes.
3	The OBEDM installer will not abort the installation if this component is not present. It can be installed later. It is strongly recommended to use the actual property values instead of default property values during the installation. Else, these properties have to be manually updated in Host Database after the entire installation completes.
4	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.
5	Oracle Access Manager can be installed later.
6	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.
7	It is mandatory for machine nodes on which OBEDM UI, Host, and SOA Media pack installation is planned, to install the Java Cryptography Extensions Unlimited Strength Jurisdiction Policy Files, to enable additional encryption strengths.
8	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/
9	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/html/E82037_01/toc.htm

Serial Number	Description
	The url details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.3.0) products. Changes necessary at a system level for the fusion middleware should be made prior to executing 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/html/E82037_01/toc.htm#GUID-95BCDEF2-F2FC-4E30-A8EF-B966F817B1D4
10	The value of property SOA_SERVER_NAME in installer properties should not be changed. The default value of soa_server1, that is shipped along with media pack, should be retained AS IS. Managed servers, that are required inside the cluster as per the naming onsite conventions, should be added after the media pack installation is complete.
11	Oracle SOA Suite 12.2.1.3.0 patch - p27651368_122130_Generic.zip has to be applied on SOA machine only. This can be downloaded from the following link: http://aru.us.oracle.com:8080/ARU/ViewPatchRequest/process_form?aru=22513715

2.2 Installation Process Overview

The following diagram provides an overview of the steps that need to be followed to install and configure Oracle Banking Enterprise Default Management:

Figure 2–1 Installation Overview



2.3 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/html/E82037_01/toc.htm

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

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

2.3.1 Updating installobp***.properties

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

Table 2–4 Values for updating installobp.properties***

Sr.No	Name	Description	Example Value	Value
1	SILENT_INSTALL	Flag for installing silent or interactive mode	Y	
2	IPM_INSTALLED	Flag to make sure IPM is installed	Y	
3	BIP_INSTALLED	Flag to make sure BIP is installed	N	
4	OID_FARM_AND_POLICY_SEEDING_FLAG	Flag for policy seeding	Y	
5	BIP_REPORTS_UPLOADING_FLAG	Flag for BIP reports uploading	N	
6	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
7	SECURITY_ENABLED	Flag for security enable	Y	
8	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	
9	LOCAL_DISPLAY_VALUE	Value of DISPLAY variable to be	0	

Sr.No	Name	Description	Example Value	Value
		exported to generate installation wizard in local machine		
10	DOMAIN_NAME	Weblogic Domain name	host_domain or ui_domain or base_domain	
11	XD_COMPONENT_NAME	XD Component value	batchhost	This will be always batchhost
12	LOCALIZATION_TYPE	Type of localization	US	Depends on localization type
13	DOMAIN_DIRECTORY_LOCATION	Location where DOMAIN_NAME folder will be created	/scratch/app/product/fmw/user_projects/domains	
14	WEBLOGIC_USERNAME	Username for weblogic domain	weblogic	
15	WEBLOGIC_PASSWORD	Password for weblogic domain	weblogic1	
16	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.110 (Do not use localhost)	
17	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
18	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen port	7002	
19	MANAGED_SERVER_LISTEN_ADDRESS	Managed server listen address	10.180.84.110	
20	MANAGED_SERVER_LISTEN_PORT	Managed server listen port	8001	
21	MANAGED_SERVER_SSL_LISTEN_PORT	SSL listen port for managed server	8002	
22	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
23	OID_IP	I/P address of the OID server.	10.180.84.113	
24	OID_PORT	Port of the OID process instance.	3060	

Sr.No	Name	Description	Example Value	Value
25	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn= orcladmin	
26	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
27	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
28	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	cn=Users,dc=in,dc=oracle,dc=com	
29	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	
30	HOST_CLUSTER_NAME	Refers to HOST cluster name	obphost_cluster1	
31	HOST_SERVER_NAME	Refers to HOST server name	obphost_server1	
32	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_101	
33	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	/scratch/app/product/jdk1.8.0_101	

Sr.No	Name	Description	Example Value	Value
		patching.		
34	CENTRAL_INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
35	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)	
36	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	
37	HOST_MW_HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
38	UI_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of UI Admin server	10.180.84.111	
39	UI_ADMIN_SERVER_LISTEN_PORT	Listen port of UI Admin server	7001	
40	UI_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of UI managed server	10.180.84.111	
41	UI_MANAGED_SERVER_LISTEN_PORT	Listen port of UI managed server	8001	
42	UI_MANAGED_SERVER_SSL_LISTEN_PORT	Listen ssl port of UI managed server	8002	
43	SOA_ORACLE_HOME	Name of Oracle SOA which is present in fusion middleware.	soa	
44	SOA_IP	i/p address of SOA machine	10.180.84.112	

Sr.No	Name	Description	Example Value	Value
45	SOA_UNIX_USER	Unix username of SOA machine	ofssobp	
46	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
47	SOA_DOMAIN_NAME	Refers to the middleware home of the weblogic installation on the SOA server.	base_domain	
48	SOA_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
49	SOA_ADMIN_SERVER_LISTEN_PORT	Listen port of SOA Admin server	7001	
50	SOA_MANAGED_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
51	SOA_WEBLOGIC_USERNAME	Username of the server of SOA domain	weblogic	
52	SOA_WEBLOGIC_PASSWORD	Password of the server of SOA domain	weblogic1	
53	UI_IP	I/P address of the server on which the OBP presentation or UI layer should be installed.	10.180.84.111	
54	UI_UNIX_USER	Linux login user id used to install the OBP UI solution.	ofssobp	
55	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	
56	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
57	BIP_SERVER_IP	I/P of the BIP server to host OBP	10.180.84.115	

Sr.No	Name	Description	Example Value	Value
		reports		
58	BIP_SERVER_PORT	Port of the BIP server that hosts OBP reports	9502	
59	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
60	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
61	BIP_INSTANCE_ PATH	Oracle BIP Instance directory on BIP server	/scratch/app/ product/fmw/ user_projects/ domains/bi_domain /bidata/	
62	BIP_SERVER_USER	Oracle BIP server user id	weblogic	
63	BIP_SERVER_PSWD	Oracle BIP server user password	weblogic1	
64	BIP_REPORT_ BASE_PATH	Logical Base Path on Oracle BIP server under which OBP reports would be hosted	OBEDM27/R27INSTALLER	
65	BIP_DATASOURCE_ NAME	OBP Host database user used by OBP report to fetch data for reports	OBEDM27	
66	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
67	IPM_SERVER_IP	IP of Oracle Image and Processing Server for OBP Content Management	10.180.84.114	
68	IPM_SERVER_PORT	Port of Oracle Image and Processing Server for OBP Content Management	16000	
69	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ ECM1	
70	OAAM_SERVER_IP	OAAM server IP for 2FA.	oaam-ofss.com	

Sr.No	Name	Description	Example Value	Value
		OAAM_SERVER_IP refers to the ip address of OAAM Server (i.e. the IP of default server name as oaam_server_server1)		
71	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	
72	OIM_SERVER_IP	Oracle Identity Manager IP	oim-ofss.com	
73	OIM_SERVER_PORT	Oracle Identity Manager Port	16000	
74	OFSAA_SERVER_IP	OFSAA Server IP	ofsaa-ofss.com	
75	OFSAA_SERVER_PORT	OFSAA Server Port	17000	
76	DOCUMAKER_SERVER_IP	i/p address of Documaker server	documaker-ofss.com	
77	DOCUMAKER_SERVER_PORT	Listen port of Documaker server	15000	
78	BAM_SERVER_NAME	Bam sever listen address	bam-ofss.com	
79	BAM_SERVER_PORT	BAM managed server port	9003	
80	ODI_SERVER_NAME	ODI server listen address	odi-ofss.com	
81	ODI_SERVER_PORT	ODI server listen port	8001	
82	OBP_HOST_DB_USER	OBP Host database user	OBEDM27	
83	OBP_HOST_DB_PASSWORD	OBP Host database password	welcome1	
84	OBP_HOST_DB_IP	OBP Host database i/p address	10.180.84.113	

Sr.No	Name	Description	Example Value	Value
85	OBP_HOST_DB_PORT	OBP Host database port	1521	
86	OBP_HOST_DB_SERVICE_NAME	OBP Host database service name	P84113A	
87	ONS_NODE	i/p address of ONS service	10.180.84.113	
88	ONS_PORT	Listen port of ONS service	6250	
89	OPSS_HOST_SCHEMA_USER	OPSS Host schema user	PRDHOST_OPSS	
90	OPSS_HOST_SCHEMA_PASSWORD	OPSS Host schema password	welcome1	
91	OPSS_HOST_DB_IP	OPSS Host DB IP	10.180.84.113	
92	OPSS_HOST_DB_PORT	OPSS Host DB Port	1521	
93	OPSS_HOST_DB_SERVICE_NAME	OPSS Host database service name	P84113A	
94	LOCAL_DATASOURCE	STB datasource schema name	PRDHOST_STB	
95	MDS_HOST_DB_USER	MDS schema user to be used by UI and Host domain	UI27_MDS	
96	MDS_HOST_DB_PASSWORD	MDS schema Password of MDS schema user to be used by UI and Host domain	welcome1	
97	MDS_HOST_DB_IP	MDS DB IP address of MDS schema user to be used by UI and Host domain	10.180.84.113	
98	MDS_HOST_DB_PORT	MDS db port of MDS schema user to be used by UI and Host domain	1521	
99	MDS_HOST_DB_SERVICE_NAME	MDS db service name of MDS schema user to be used by UI and Host domain	P84113A	

Sr.No	Name	Description	Example Value	Value
100	OPSS_SOA_SCHEMA_USER	SOA OPSS schema name	SOA27_OPSS	
101	OPSS_SOA_AUDIT_DBDS	SOA OPSS Audit schema name	SOA27_IAU_APPEND	
102	OPSS_SOA_AUDIT_VIEWDS	SOA OPSS Audit View schema name	SOA27_IAU_VIEWER	
103	OPSS_SOA_SCHEMA_PASSWORD	Password of SOA OPSS schema name	welcome1	
104	OPSS_SOA_DB_IP	IP address of SOA OPSS DB machine	10.180.84.113	
105	OPSS_SOA_DB_PORT	Port of SOA OPSS DB	1521	
106	OPSS_SOA_DB_SERVICE_NAME	Service name of SOA OPSS DB	P84113A	
107	HOST_ADMIN_JVM_PARAMS	Host domain admin JVM startup parameters	-Xms1024m -Xmx4096m	
108	HOST_MANAGED_JVM_PARAMS	Host domain managed JVM startup parameters	Xms8g -Xmx8g -XX:NewSize=2048m -XX:MaxNewSize=4096m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75	
109	KEYSTORE_PASSWORD	Password for generating certificate	welcome1	
110	IPM_OUTBOUND_USERNAME	IPM Username created in connector	weblogic	
111	IPM_OUTBOUND_PASSWORD	Password for the IPM user in connector	weblogic1	
112	BIP_OUTBOUND_USERNAME	BIP Username created in connector	weblogic	
113	BIP_OUTBOUND_PASSWORD	Password for the BIP user in connector	weblogic1	
114	ODI_OUTBOUND_USERNAME	ODI Username created in	weblogic	

Sr.No	Name	Description	Example Value	Value
		connector		
115	ODI_OUTBOUND_PASSWORD	Password for the ODI user in connector	weblogic1	
116	OIM_OUTBOUND_USERNAME	OIM Username created in connector	weblogic	
117	OIM_OUTBOUND_PASSWORD	Password for the OIM user in connector	weblogic1	
118	WCM_OUTBOUND_USERNAME	WCM Username created in connector	weblogic	
119	WCM_OUTBOUND_PASSWORD	Password for the WCM user in connector	weblogic1	
120	OFFLINE_CHANNEL_OUTBOUND_USERNAME	Offline Username created in connector	offlineuser	
121	OFFLINE_CHANNEL_OUTBOUND_PASSWORD	Password for the Offline user in connector	welcome1	
122	SAML_ISSUER_OUTBOUND_USERNAME	SAML ISSUER Username created in connector	weblogic	
123	SAML_ISSUER_OUTBOUND_PASSWORD	Password for the SAML ISSUER user in connector	weblogic1	
124	BPEL_ENCRYPTION_OUTBOUND_USERNAME	BPEL_ENCRYPTION Username created in connector	weblogic	
125	BPEL_ENCRYPTION_OUTBOUND_PASSWORD	Password for the BPEL_ENCRYPTION user in connector	weblogic1	
126	FTP_IPM_OUTBOUND_USERNAME	FTP IPM Username created in connector	weblogic	
127	FTP_IPM_OUTBOUND_PASSWORD	Password for the FTP IPM user in connector	weblogic1	

Sr.No	Name	Description	Example Value	Value
128	FTP_BIP_OUTBOUND_USERNAME	FTP BIP Username created in connector	weblogic	
129	FTP_BIP_OUTBOUND_PASSWORD	Password for the FTP BIP user in connector	weblogic1	
130	BIP_USR_OUTBOUND_USERNAME	BIP Username created in connector	weblogic	
131	BIP_USR_OUTBOUND_PASSWORD	Password for the BIP user in connector	weblogic1	
132	SOA_PURGING_OUTBOUND_USERNAME	SOA Username created in connector	weblogic	
133	SOA_PURGING_OUTBOUND_PASSWORD	Password for the SOA user in connector	weblogic1	
134	SOA_OUTBOUND_USERNAME	SOA Username created in connector	weblogic	
135	SOA_OUTBOUND_PASSWORD	Password for the SOA user in connector	weblogic1	
136	ATMUSER_OUTBOUND_USERNAME	ATM Username created in connector	ATMUser	
137	ATMUSER_OUTBOUND_PASSWORD	Password for the ATM user in connector	welcome1	
138	POSUSER_OUTBOUND_USERNAME	POS Username created in connector	POSUser	
139	POSUSER_OUTBOUND_PASSWORD	Password for the POS user in connector	welcome1	
140	DMSHOST_OUTBOUND_USERNAME	DMS HOST Username created in connector	weblogic	
141	DMSHOST_OUTBOUND_PASSWORD	Password for the DMS HOST user in connector	weblogic1	
142	DMSUI_OUTBOUND_	DMS UI Username created in	weblogic	

Sr.No	Name	Description	Example Value	Value
	USERNAME	connector		
143	DMSUI_OUTBOUND_PASSWORD	Password for the DMS UI user in connector	weblogic1	
144	OCH_OUTBOUND_USERNAME	OCH Username created in connector	weblogic	
145	OCH_OUTBOUND_PASSWORD	Password for the OCH user in connector	weblogic1	
146	WS_MFT_OUTBOUND_USERNAME	WS_MFT Username created in connector	weblogic	
147	WS_MFT_OUTBOUND_PASSWORD	Password for the WS_MFT user in connector	weblogic1	
148	OP_OUTBOUND_USERNAME	OP Username created in connector	weblogic	
149	OP_OUTBOUND_PASSWORD	Password for the OP user in connector	weblogic1	
150	ICS_OUTBOUND_USERNAME	Username for ICS connector	weblogic	
151	ICS_OUTBOUND_PASSWORD	Password for ICS connector	Weblogic1	
152	OBDX_OUTBOUND_USERNAME	Username for OBDX connector	1518675030085dean.white@test.com	
153	OBDX_OUTBOUND_PASSWORD	Password for OBDX connector	Welcome@1	
154	CARD_USERNAME	Username of Card connector	orakey	
155	CARD_PASSWORD	Password of Card connector	welcome1	
156	RULE_USERNAME	Username of Rule connector	orakey	
157	RULE_PASSWORD	Password of Rule connector	welcome1	
158	BAM_USERNAME	Username of BAM connector	weblogic	
159	BAM_PASSWORD	Password of BAM connector	weblogic1	

Sr.No	Name	Description	Example Value	Value
160	COMMON_OUTBOUND_USERNAME	Username for common connector	Weblogic1	
161	COMMON_OUTBOUND_PASSWORD	Password for common connector	Weblogic1	
162	PM_OUTBOUND_USERNAME	Username for PM connector	weblogic	
163	PM_OUTBOUND_PASSWORD	Password for PM connector	weblogic1	
164	LENDING_OUTBOUND_USERNAME	Username for lending connector	weblogic	
165	LENDING_OUTBOUND_PASSWORD	Password for lending connector	weblogic1	
166	DEPOSITS_OUTBOUND_USERNAME	Username for deposits connector	weblogic	
167	DEPOSITS_OUTBOUND_PASSWORD	Password for deposits connector	weblogic1	
168	FW_OUTBOUND_USERNAME	Username for FW connector	weblogic	
169	FW_OUTBOUND_PASSWORD	Password for fw connector	weblogic1	
170	COLLECTION_OUTBOUND_USERNAME	Username for collection connector	weblogic	
171	COLLECTION_OUTBOUND_PASSWORD	Password for collection Connector	weblogic1	
172	OR_OUTBOUND_USERNAME	Username for OR connector	weblogic	
173	OR_OUTBOUND_PASSWORD	Password for OR connector	weblogic1	
174	PARTY_OUTBOUND_USERNAME	Username for Party connector	weblogic	
175	PARTY_OUTBOUND_PASSWORD	Password for Party connector	weblogic1	
176	PRODPROC_	Username for	weblogic	

Sr.No	Name	Description	Example Value	Value
	OUTBOUND_USERNAME	PRODPROC connector		
177	PRODPROC_OUTBOUND_PASSWORD	Password for PRODPROC connector	weblogic1	
178	RECOVERY_OUTBOUND_USERNAME	Username for Recovery connector	weblogic	
179	RECOVERY_OUTBOUND_PASSWORD	Password for Recovery connector	weblogic1	
180	PRICING_OUTBOUND_USERNAME	Username for Pricing connector	weblogic	
181	PRICING_OUTBOUND_PASSWORD	Password for Pricing connector	weblogic1	
182	LCM_OUTBOUND_USERNAME	Username for LCM connector	weblogic	
183	LCM_OUTBOUND_PASSWORD	Password for LCM connector	weblogic1	
184	MDM_OUTBOUND_USERNAME	Username for MDM connector	weblogic	
185	MDM_OUTBOUND_PASSWORD	Password for MDM connector	weblogic1	
186	COMMUNICATIONS_OUTBOUND_USERNAME	Username for COMMUNICATIONS connector	weblogic	
187	COMMUNICATIONS_OUTBOUND_PASSWORD	Password for COMMUNICATIONS connector	weblogic1	
188	APPCAPTURE_OUTBOUND_USERNAME	Username for APPCAPTURE connector	weblogic	
189	APPCAPTURE_OUTBOUND_PASSWORD	Password for APPCAPTURE connector	weblogic1	
190	USER_TIMEZONE	Time zone entry	+5:30	
191	HOST_SSL_PASSWORD	Password for configuring SSL in HOST domain	welcome1	
192	SILENT_INSTALL	Flag for executing installer remotely	Y	

Sr.No	Name	Description	Example Value	Value
193	SECURITY_ ENABLED	Flag for security enable	Y	
194	IPM_INSTALLED	Flag for if IPM is installed	Y	
195	BIP_INSTALLED	Flag for if BIP is installed	N	This value must be N.
196	LOCAL_IP	I/P address 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.	10.180.84.111	
197	LOCAL_DISPLAY_ VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
198	DOMAIN_NAME	Weblogic Domain name	Host_domain or ui_domain or base_ domain	
199	XD_COMPONENT_ NAME	XD Component value	obpui	This will be always obpui
200	LOCALIZATION_ TYPE	Type of localization	US	Depends on localizatio n type
201	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
202	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
203	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
204	LOCAL_ DATASOURCE	Username of LOCAL_ DATASOURCE	PRDUI_STB	
205	OPSS_UI_SCHEMA_	OPSS UI schema	PRDUI_OPSS	

Sr.No	Name	Description	Example Value	Value
	USER	name		
206	OPSS_UI_SCHEMA_PASSWORD	OPSS UI schema password	Welcome1	
207	OPSS_UI_DB_IP	OPSS UI DB IP	10.180.84.113	
208	OPSS_UI_DB_PORT	OPSS UI DB PORT	1521	
209	OPSS_UI_DB_SERVICE_NAME	OPSS UI DB SERIVICE NAME	P84113A	
210	MDS_SCHEMA_USER	MDS schema name	PRDUI _MDS	
211	MDS_SCHEMA_PASSWORD	Password of MDS schema	welcome1	
212	MDS_DB_IP	MDS DB IP	10.180.84.113	
213	MDS_DB_PORT	MDS DB PORT	1521	
214	MDS_DB_SERVICE_NAME	MDS DB SERVIVE NAME	P84113A	
215	OPSS_SOA_SCHEMA_USER	SOA OPSS Schema name	PRDSOA _OPSS	
216	OPSS_SOA_AUDIT_DBDS	SOA OPSS AUDIT schema name	PRDSOA_IAU_APPEND	
217	OPSS_SOA_AUDIT_VIEWDS	SOA OPSS AUDIT VIEWDB Schema name	PRDSOA_IAU_VIEWER	
218	OPSS_SOA_SCHEMA_PASSWORD	SOA OPSS password for above three OPSS schema	welcome1	
219	OPSS_SOA_DB_IP	Service name of UI OPSS DB	10.180.84.113	
220	OPSS_SOA_DB_PORT	SOA OPSS DB PORT	1521	
221	OPSS_SOA_DB_SERVICE_NAME	SOA OPSS DB SERVICE NAME	P84113A	
222	HOST_SCHEMA_USER	OBP Host Database username	OBEDM27	
223	HOST_SCHEMA_PASSWORD	OBP Host Database password	welcome1	
224	HOST_DB_IP	OBP Host	10.180.84.113	

Sr.No	Name	Description	Example Value	Value
		Database i/p address		
225	HOST_DB_PORT	OBP Host Database listen port	1521	
226	HOST_DB_ SERVICE_NAME	OBP Host Database service name	P84113A	
227	ONS_NODE	i/p address of ONS service	10.180.84.113	
228	ONS_PORT	Listen port of ONS service	6250	
229	ADMIN_SERVER_ LISTEN_ADDRESS	Admin server listen address	10.180.84.111	
230	ADMIN_SERVER_ LISTEN_PORT	Admin server listen port	7001	
231	ADMIN_SERVER_ SSL_LISTEN_PORT	Admin server SSL listen port	7002	
232	MANAGED_ SERVER_LISTEN_ ADDRESS	Managed server listen address	10.180.84.111	
233	MANAGED_ SERVER_LISTEN_ PORT	Managed server listen port	8001	
234	MANAGED_ SERVER_SSL_ LISTEN_PORT	Managed server SSL listen port	8002	
235	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
236	OID_IP	I/P address of the OID server	10.180.84.113	
237	OID_PORT	Port of the OID process instance.	3060	
238	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn=orcladmin	
239	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
240	OID_GROUP_DSN	The DSN used for object class Groups	cn=Groups,dc=in,dc=oracle,dc=com	

Sr.No	Name	Description	Example Value	Value
		in the OID ldap.		
241	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	cn=Users,dc=in,dc=oracle,dc=com	
242	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	
243	UI_IP	I/P address of the server on which the OBP presentation or UI layer should be installed.	10.180.84.111	
244	UI_CLUSTER_NAME	Name of UI Managed Cluster	obpui_cluster1	
245	UI_SERVER_NAME	Name of UI Managed Server	obpui_server1	
246	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	
247	UI_MW_HOME	Refers to the middleware home of the weblogic installation on the UI server.	/scratch/app/product/fmw	
248	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	/scratch/app/product/jdk1.8.0_101	

Sr.No	Name	Description	Example Value	Value
		the OBP security policies policy seeding utility at the end of the installation.		
249	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_101	
250	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
251	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
252	IPM_UNIX_USER	Linux login user id of IPM server	ofssobp	
253	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
254	IPM_SERVER_PORT	Listen port of IPM server	16000	
255	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ ECM1	
256	BIP_SERVER_IP	i/p address of BIP server	10.180.84.115	
257	BIP_SERVER_PORT	Listen port of BIP server	9502	
258	BIP_UNIX_USER	Linux login user id of BIP server	ofssobp	
259	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
260	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	

Sr.No	Name	Description	Example Value	Value
261	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	
262	OIM_SERVER_IP	Oracle Identity Manager i/p address	oim-ofss.com	
263	OIM_SERVER_PORT	Oracle Identity Manager Listen Port	16000	
264	OFSAA_SERVER_IP	OFSAA Server i/p address	ofsaa-ofss.com	
265	OFSAA_SERVER_PORT	OFSAA Server listen port	17000	
266	UI_ADMIN_JVM_PARAMS	UI domain admin JVM startup parameters	-Xms2048m -Xmx4096m	
267	UI_MANAGED_JVM_PARAMS	UI domain managed JVM startup parameters	-Djbo.ampool.doampooling=false -Xms6g -Xmx6g -XX:NewSize=512m -XX:MaxNewSize =2048m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiating OccupancyFraction=75 -Djbo.load.components.lazily=true	
268	HOST_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of HOST admin server	10.180.84.110	
269	HOST_ADMIN_SERVER_LISTEN_PORT	Listen port of HOST admin server	7001	
270	HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of host managed server	10.180.84.110	

Sr.No	Name	Description	Example Value	Value
271	HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of host managed server	8001	
272	SOA_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
273	SOA_MANAGED_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
274	SOA_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of Admin SOA server	10.180.84.112	
275	SOA_ADMIN_SERVER_LISTEN_PORT	Listen port of Admin SOA server	7001	
276	KEYSTORE_PASSWORD	Password for generating certificate	welcome1	
277	UI_SSL_PASSWORD	Password for configuring SSL in UI domain	welcome1	
278	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	

Sr.No	Name	Description	Example Value	Value
279	UCM_IP	UCM_IP the IP address of the UCM WebLogic managed server.	ofss.ucm.com	
280	UCM_PORT	Port of UCM.	4444	
281	OFFLINE_ CHANNEL_ OUTBOUND_ USERNAME	Offline username created in connector	offlineuser	
282	OFFLINE_ CHANNEL_ OUTBOUND_ PASSWORD	Password for the Offlineuser user in connector	welcome1	
283	CARD_USERNAME	Username of Card connector.	orakey	
284	CARD_PASSWORD	Password of Card connector.	welcome1	
285	RULE_USERNAME	Username of Rule connector	orakey	
286	RULE_PASSWORD	Password of Rule connector	welcome1	
287	USER_TIMEZONE	Time zone entry	+5:30	
288	REMOTE_ EXECUTION	Flag for executing installer remotely	Y	
289	IPM_USERNAME	Username of IPM connector	weblogic	
290	IPM_PASSWORD	Password of IPM connector	weblogic1	
291	FTP_IPM_ USERNAME	Username of FTP_ IPM connector	ofssobp	
292	FTP_IPM_ PASSWORD	Password of FTP_ IPM connector	ofssobp123	
293	FTP_IPM_BATCH_ USERNAME	Username of FTP_ IPM_BATCH	ofssobp	
294	FTP_IPM_BATCH_ PASSWORD	Password of FTP_ IPM_BATCH	ofssobp123	
295	HOST_UNIX_USER	Linux login user id for HOST server	ofssobp	
296	HOST_MW_HOME	Refers to the middleware home of the weblogic installation on the	/scratch/app/product/fmw	

Sr.No	Name	Description	Example Value	Value
		Host server.		
297	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
298	SOA_DOMAIN_NAME	SOA Domain Name	base_domain	
299	SILENT_INSTALL	Flag for installing silent or interactive mode	y	
300	SECURITY_ENABLED	Flag for security enable	Y	
301	IPM_INSTALLED	Flag for if IPM is installed	Y	
302	BIP_INSTALLED	Flag for if BIP is installed	N	
303	LOCAL_IP	I/P of the local machine which could be a windows machine on which software like XManager is installed for rendering UI of a utility executing on a remote Linux server.	10.180.84.112	
304	LOCAL_DISPLAY_VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
305	DOMAIN_NAME	Name of the weblogic domain to be created	Host_domain or ui_domain or base_domain	
306	XD_COMPONENT_NAME	XD Component value	obpsoa	This will be always obpsoa
307	LOCALIZATION_TYPE	Type of localization	US	Depends on localization type
308	DOMAIN_DIRECTORY_	Location where DOMAIN_NAME	/scratch/app/product/fmw/user_projects/domains	

Sr.No	Name	Description	Example Value	Value
	LOCATION	folder will be created		
309	WEBLOGIC_USERNAME	Username for weblogic domain	weblogic	
310	WEBLOGIC_PASSWORD	Password for weblogic domain	weblogic1	
311	MDS_SCHEMA_USER	MDS schema user for SOA domain	SOA27_MDS	
312	SOA_INFRASTRUCTURE_SCHEMA_USER	SOA infrastructure schema user for SOA domain	SOA27_SOAINFRA	
313	LOCAL_DATASOURCE	Local schema user for SOA domain	SOA27_STB	
314	UMS_DATASOURCE	UMS schema user for SOA domain	SOA27_UMS	
315	DB_SCHEMA_PASSWORD	Password for MDS schema user	welcome1	
316	DB_IP	i/p address of MDS db machine	10.180.84.113	
317	DB_PORT	Port of MDS db port	1521	
318	DB_SERVICE_NAME	Service Name of MDS user	P84113A	
319	HOST_SCHEMA_USER	OBP Host Database username	OBEDM27	
320	HOST_SCHEMA_PASSWORD	OBP Host Database password	welcome1	
321	HOST_DB_IP	OBP Host Database i/p address	10.180.84.113	
322	HOST_DB_PORT	OBP Host Database port	1521	
323	HOST_DB_SERVICE_NAME	OBP Host Database service name	P84113A	
324	ONS_NODE	i/p address of ONS service	10.180.84.113	
325	ONS_PORT	Port of ONS service	6250	
326	OPSS_SOA_	SOA OPSS	SOA27_OPSS	

Sr.No	Name	Description	Example Value	Value
	SCHEMA_USER	Schema Name		
327	OPSS_SOA_AUDIT_DBDS	SOA OPSS AUDIT Schema name	SOA27_IAU_APPEND	
328	OPSS_SOA_AUDIT_VIEWDS	SOA OPSS AUDIT VIEWDS Schema name	SOA27_IAU_VIEWER	
329	OPSS_SOA_SCHEMA_PASSWORD	Password of OPSS_SOA_SCHEMA_USER	welcome1	
330	OPSS_SOA_DB_IP	i/p address of SOA OPSS DB.	10.180.84.113	
331	OPSS_SOA_DB_PORT	Port of SOA OPSS DB.	1521	
332	OPSS_SOA_DB_SERVICE_NAME	Service name of SOA OPSS DB.	P84113A	
333	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.112	
334	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
335	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen address	7002	
336	SOA_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
337	SOA_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
338	SOA_SERVER_SSL_LISTEN_PORT	SSL Listen port of SOA server	8002	
339	HUMANTASK_SERVER_LISTEN_ADDRESS	Listen address of humantask server	10.180.84.112	
340	HUMANTASK_SERVER_LISTEN_PORT	Listen port of humantask server	9001	
341	HUMANTASK_SERVER_SSL_LISTEN_PORT	SSL listen port of humantask server	9002	
342	BAM_SERVER_LISTEN_ADDRESS	Listen address of BAM server	10.180.84.112	
343	BAM_SERVER_LISTEN_PORT	Listen port of BAM server	9003	
344	BAM_SERVER_SSL_	SSL Listen port of	9004	

Sr.No	Name	Description	Example Value	Value
	LISTEN_PORT	BAM server		
345	HOST_ADMIN_SERVER_LISTEN_ADDRESS	Listen address of HOST admin server	10.180.84.110	
346	HOST_ADMIN_SERVER_LISTEN_PORT	Listen port of HOST admin server	7001	
347	HOST_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of host managed server	10.180.84.110	
348	HOST_MANAGED_SERVER_LISTEN_PORT	Listen port of host managed server	8001	
349	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
350	OID_IP	I/P address of the OID server.	10.180.84.113	
351	OID_PORT	Port of the OID process instance.	389	
352	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn	
353	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
354	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
355	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	cn=Users,dc=in,dc=oracle,dc=com	
356	NODE_MGR_PORT	Refers to the port number to be used for the weblogic node manager. This port should either be free on the UI Presentation server or an existing weblogic node manager should be installed to listen on this port when the same is started	5556	

Sr.No	Name	Description	Example Value	Value
357	SOA_IP	i/p address of SOA server	10.180.84.112	
358	SOA_CLUSTER_NAME	Cluster name of SOA server	obpsoa_cluster1	
359	SOA_SERVER_NAME	Server name of SOA server	soa_server1	
360	HUMAN_TASK_CLUSTER_NAME	Cluster name of Humantask server	obphumantask_cluster1	
361	HUMAN_TASK_SERVER_NAME	Server name of Humantask server	obphumantask_server1	
362	SOA_TARGET	Target folder of SOA machine where files will be copied temporarily during installation	/scratch/install/target	
363	SOA_JAVA_HOME	Refers to the home directory of java installation of the SOA machine. The version of java installed should be 1.8.0 or above. This is used to execute the OBP security policies policy seeding utility at the end of the installation.	/scratch/app/product/jdk1.8.0_101	
364	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_101	
365	CENTRAL_INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory/	
366	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
367	UI_IP	i/p address of UI server	10.180.84.111	
368	UI_UNIX_USER	Linux login user id	ofssobp	

Sr.No	Name	Description	Example Value	Value
		for UI server		
369	UI_DOMAIN_HOME	Full path of UI domain	/scratch/app/ product/fmw/ user_projects/ domains /ui_domain	
370	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
371	SOA_ADMIN_JVM_ PARAMS	SOA domain admin JVM startup parameters	-Xms1024m -Xmx2048m	
372	SOA_ HUMANTASKSERVE R_JVM_PARAMS	SOA domain human task server's JVM startup parameters	-Djbo.ampool. doampooling=false –Xms12g -Xmx12g -XX:NewSize= 512m -XX:MaxNewSize =2048m -XX: +UseParNewGC -XX:+ CMSParallel RemarkEnabled -XX:+UseConcMark SweepGC -XX:CMSInitiating OccupancyFraction=75 -Dobp.http. maxRetryCount=1 -Dobp.http .socketBufferSize=81	
373	SOA_MANAGED_ JVM_PARAMS	SOA domain managed soa server's JVM startup parameters	-XX:NewSize =2048m -XX:MaxNewSize =4096m -XX:+UsePa rNewGC -XX: +CMSPar allelRemarkEnabled -XX:+UseCo ncMarkSweepGC -XX:CMSInit iatingOccupancy Fraction=75 -Xms11g -Xmx11g	
374	KEYSTORE_ PASSWORD	Password for generating certificate	welcome1	
375	UI_MANAGED_ SERVER_LISTEN_	i/p address of UI Managed server	10.180.84.111	

Sr.No	Name	Description	Example Value	Value
	ADDRESS			
376	UI_MANAGED_SERVER_LISTEN_PORT	Listen port of UI Managed server	8001	
377	UI_ADMIN_SERVER_LISTEN_ADDRESS	i/p address of UI Admin server	10.180.84.111	
378	UI_ADMIN_SERVER_LISTEN_PORT	Listen port of UI Admin server	7001	
379	DEFAULT_BANK_CODE	Default bank code will be set while configuring SOA domain	8	
380	DEFAULT_TRANSACTION_BRANCH_CODE	Default branch code will be set while configuring SOA domain	89999	
381	DEFAULT_TARGET_UNIT	Default target unit will be set while configuring SOA domain	OBP_BU	
382	CARD_USERNAME	Username of Card connector.	orakey	
383	CARD_PASSWORD	Password of Card connector	welcome1	
384	RULE_USERNAME	Username of Rule connector	orakey	
385	RULE_PASSWORD	Password of Rule connector	welcome1	
386	USER_TIMEZONE	Time zone entry	+5:30	
387	SOA_SSL_PASSWORD	Password for configuring SSL in SOA domain	welcome1	
388	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
389	BAM_INSTALLATION	During SOA installation value should be ‘N’ During BAM installation value should be Y.	N	
390	IPM_USERNAME	Username of IPM connector	ofssobp	

Sr.No	Name	Description	Example Value	Value
391	IPM_PASSWORD	Password of IPM connector	welcome1	
392	OFFLINE_CHANNEL_OUTBOUND_USERNAME	Username of offline connector	offlineuser	
393	OFFLINE_CHANNEL_OUTBOUND_PASSWORD	Password of offline connector	welcome1	
394	FTP_IPM_USERNAME	Username of FTP_IPM connector	ofssobp	
395	FTP_IPM_PASSWORD	Password of FTP_IPM connector	ofssobp123	
396	FTP_IPM_BATCH_USERNAME	Username of FTP_IPM_BATCH connector	ofssobp	
397	FTP_IPM_BATCH_PASSWORD	Password of FTP_IPM_BATCH connector	ofssobp123	
398	SOA_OUTBOUND_USERNAME	Username of SOA connector	weblogic	
399	SOA_OUTBOUND_PASSWORD	Password of SOA connector	weblogic1	
400	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
401	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
402	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ECM1	
403	BIP_SERVER_IP	I/P of the BIP server to host OBP reports	10.180.84.115	
404	BIP_SERVER_PORT	Port of the BIP server that hosts OBP reports	9502	
405	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
406	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	

2.3.2 Database and WebLogic Domain Configuration

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

Table 2–5 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.	

2.4 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.

2.4.1 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.

2.4.2 Verify the OID installation

This section describes the procedure to verify the OID installation.

2.4.2.1 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.

2.4.2.2 OPSS/OID Performance Tuning

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

Parameters

Change the parameter values as provided below.

Table 2–6 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 2–7 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 2–8 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
```

2.4.2.3 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 2–9 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
   ```

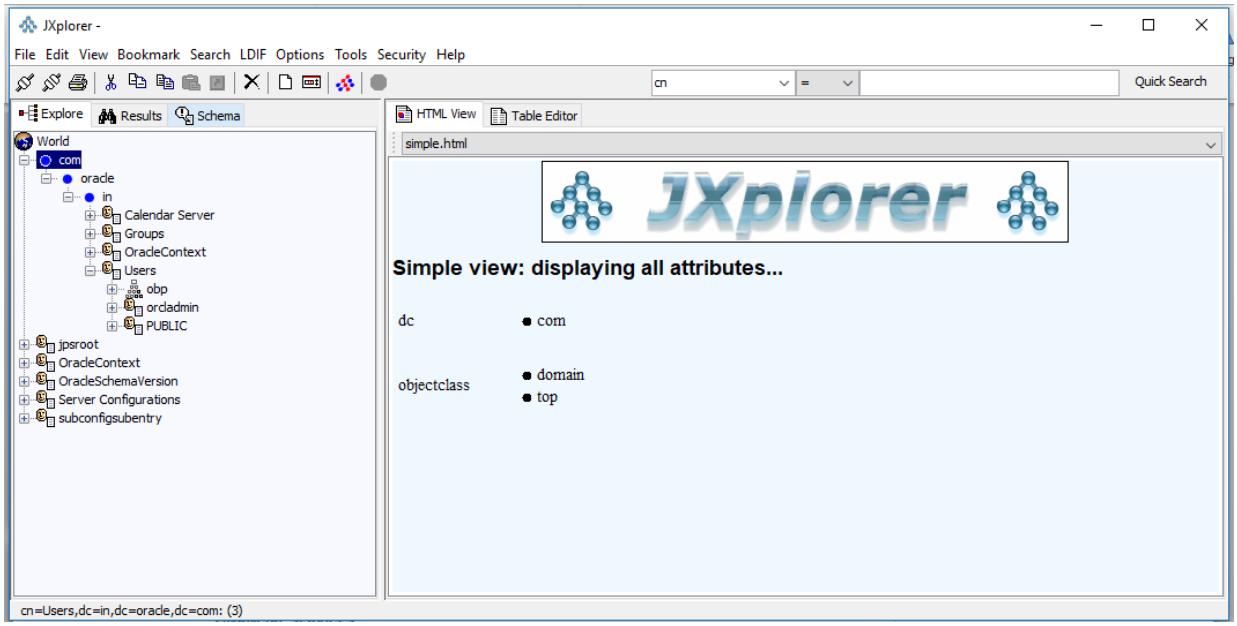
   ldapadd Administrators.ldif

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

2.4.2.4 Verify the import using ODSM or JXplorer

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

Figure 2–2 JXplorer



3 OBEDM US Localization SOA Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Enterprise Default Management US Localization SOA (Integration Server) Media pack. The subsequent section refers to the variable names specified in Section 2.3 Installation Checklist.

3.1 Installation and Configuration Procedure

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

3.1.1 Preparatory Steps

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

Step 1 Procuring Installables

Download the appropriate SOA media pack from the following location:

http://edelivery.oracle.com/

Step 2 Extracting the Installables

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

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

Step 3 Printing Checklists

Take a printout of the installation checklist mentioned in Section 2.3 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 SOA Media Pack installation.

Step 1 Updating installobpsoa.properties

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

Step 2 Checklist for a new setup

Before initiating installation, check the following:

- Make sure required RCU schemas have been created. For more information, see Section 6.1 Pre-Installation Steps and Section 6.2 OBEDM Database Setup – RCU Installation.
- Increase the size of tablespace (at least 4GB and the auto extend mode must be on) for MDS, SOAINFRA and OPSS schema used for SOA domain.
- Node manager must not be running on the target machine.
- Create a dummy folder named target and mention its path against SOA_TARGET property.
- Values given in installobpui.properties must be correct. At run time, no option is given to change the values.
- No processes should be running on the ports given in installobpsoa.properties.
- In case of a re-installation ensure that the directory paths against SOA_TARGET and SOA_MW_HOME specified in installobpsoa.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- Before initiating the installation, ensure that all the values given in installobpsoa.properties are correct. At the time of installation, the values will only be displayed once for verification, and it will not be possible to change the values once the installation begins.

Step 3 OS Level Tuning

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

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

For more information, see Page 12 of the following document:

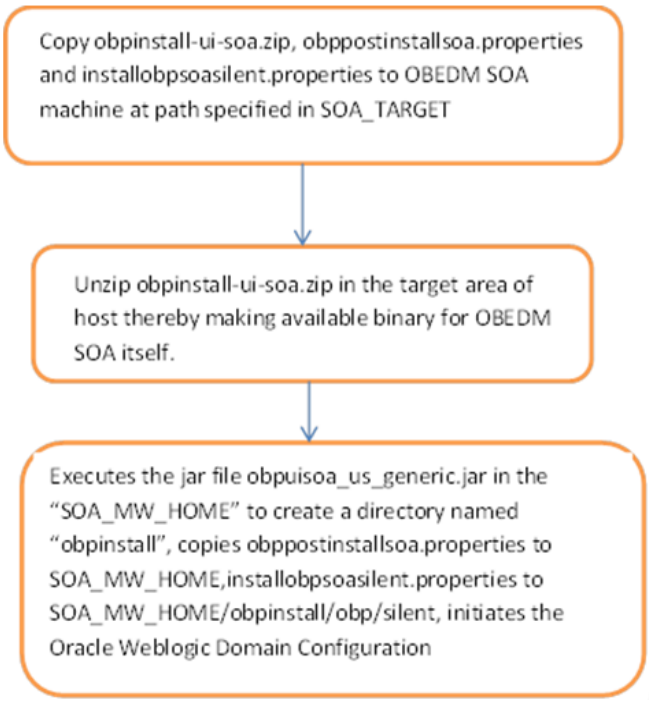
http://www.oracle.com/technetwork/database/availability/maa-fmwsharedstoragebestpractices-402094.pdf

3.1.3 Installation Steps

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

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

Figure 3–1 Steps in installobpsoa.sh script



A sample output is given here.

./installobpsoa.sh

Figure 3–2 Verification of Properties

```
[ofssobp@mum00asl obpus-ui-soa]$ ./installobpsoa.sh
The present working directory is /scratch/install/obpus-ui-soa. It is assumed that all installables are present in this directory.
Printing the information entered above
SILENT_INSTALL                          : y
XD_COMPONENT_NAME                       : obpsoa
LOCALIZATION_TYPE                       : us
LOCAL_IP                                : 10.180.86.238
LOCAL_DISPLAY_VALUE                     : 0.0
DOMAIN_NAME                             : base_domain
DOMAIN_DIRECTORY_LOCATION               : /scratch/app/product/fmw/user_projects/domains
WEBLOGIC_USERNAME                       : weblogic
WEBLOGIC_PASSWORD                       : weblogic1
MDS_SCHEMA_USER                         : OBEDMSOA_MDS
SOA_INFRASTRUCTURE_SCHEMA_USER          : OBEDMSOA_SOAINFRA
DB_SCHEMA_PASSWORD                      : welcome1
DB_IP                                   : mum00bhw.in.oracle.com
DB_PORT                                 : 1521
DB_SERVICE_NAME                         : P3523A
HOST_SCHEMA_USER                        : OBEDMUS210
HOST_SCHEMA_PASSWORD                    : welcome1
HOST_DB_IP                              : mum00bhw.in.oracle.com
HOST_DB_PORT                            : 1521
HOST_DB_SERVICE_NAME                    : P3523A
ADMIN_SERVER_LISTEN_ADDRESS             : 10.180.86.238
ADMIN_SERVER_LISTEN_PORT                : 7001
ADMIN_SERVER_SSL_LISTEN_PORT            : 7002
SOA_SERVER_LISTEN_ADDRESS               : 10.180.86.238
SOA_SERVER_LISTEN_PORT                  : 8001
SOA_SERVER_SSL_LISTEN_PORT              : 8002
HUMANTASK_SERVER_LISTEN_ADDRESS         : 10.180.86.238
HUMANTASK_SERVER_LISTEN_PORT            : 9001
HUMANTASK_SERVER_SSL_LISTEN_PORT        : 9002
BAM_SERVER_LISTEN_ADDRESS               : 10.180.86.238
BAM_SERVER_LISTEN_PORT                  : 9003
BAM_SERVER_SSL_LISTEN_PORT              : 9004
HOST_MANAGED_SERVER_LISTEN_ADDRESS      : 10.180.34.122
HOST_MANAGED_SERVER_LISTEN_PORT         : 8001
LDAP_PROVIDER                           : OID
```

Figure 3–3 Verification of Properties

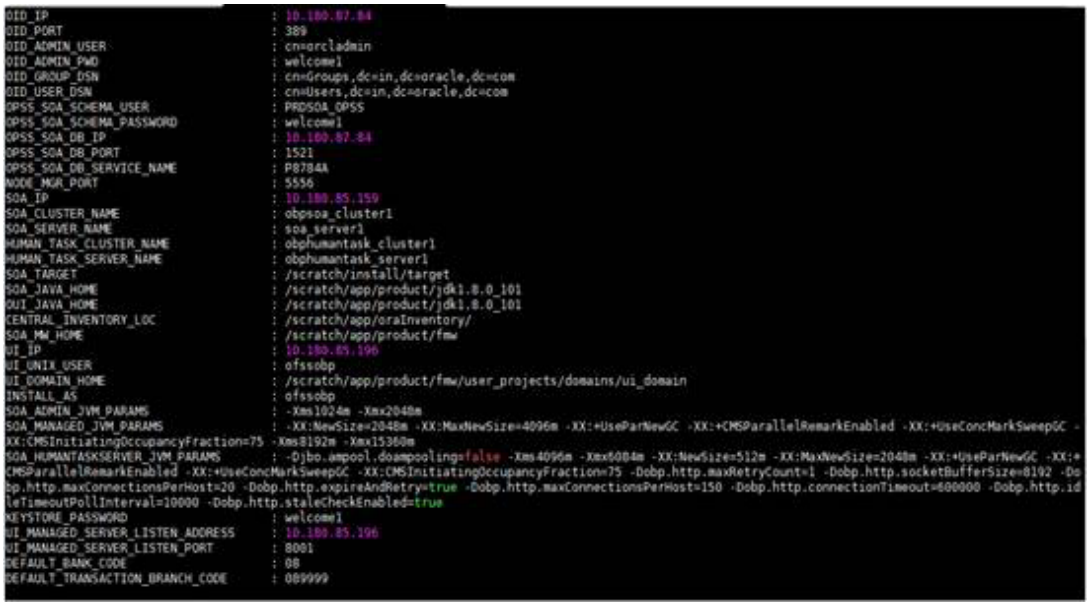
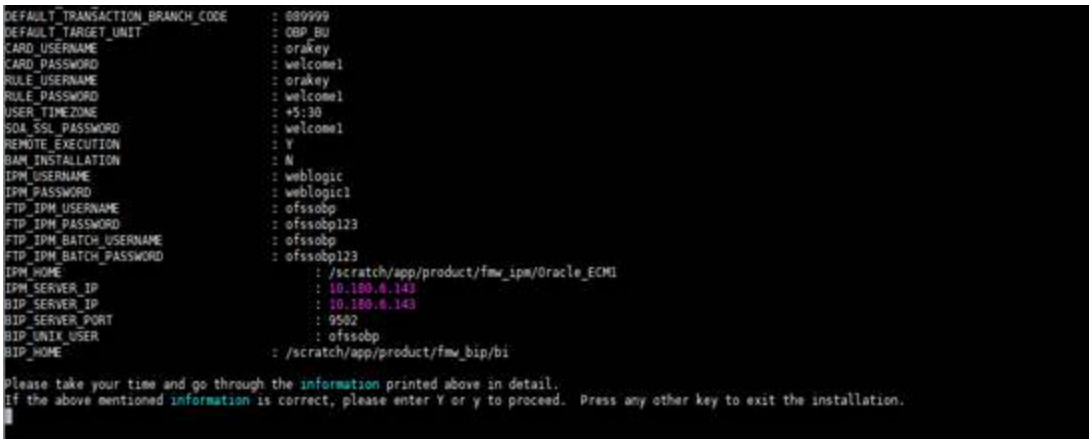


Figure 3–4 Confirmation to Proceed Domain Installation (cont.)



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

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

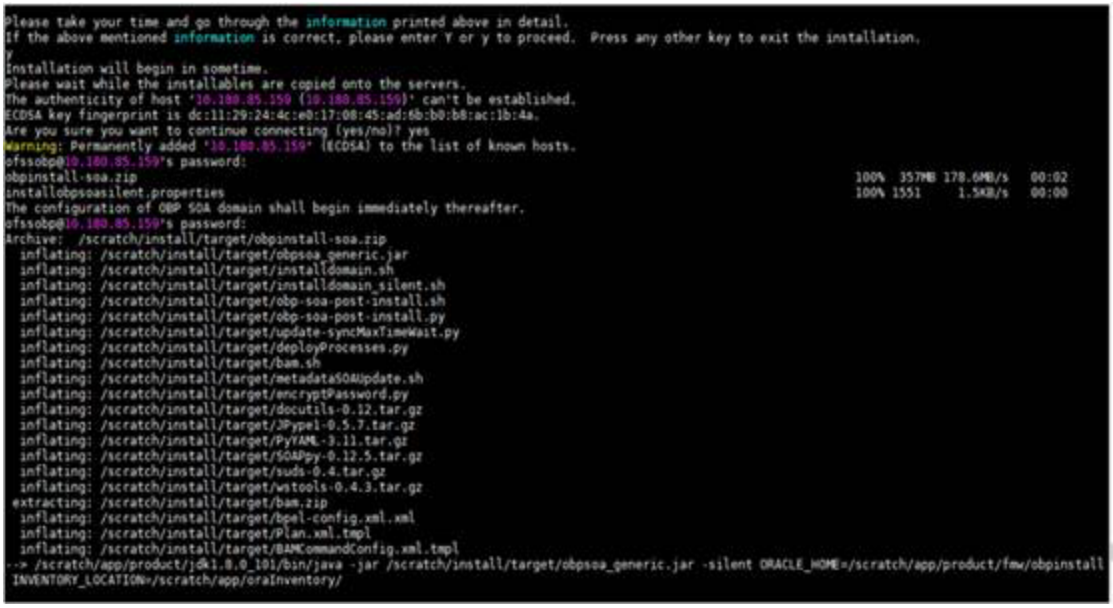


Figure 3–6 Copying and Extraction of obpinstall-ui-soa.zip

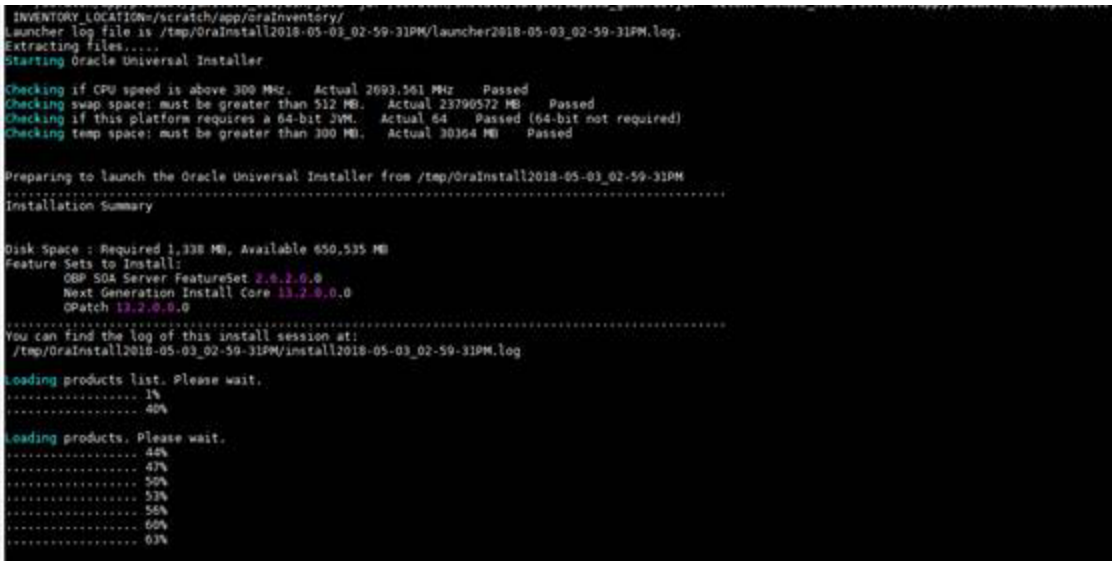


Figure 3–7 Copying and Extraction of obpinstall-ui-soa.zip

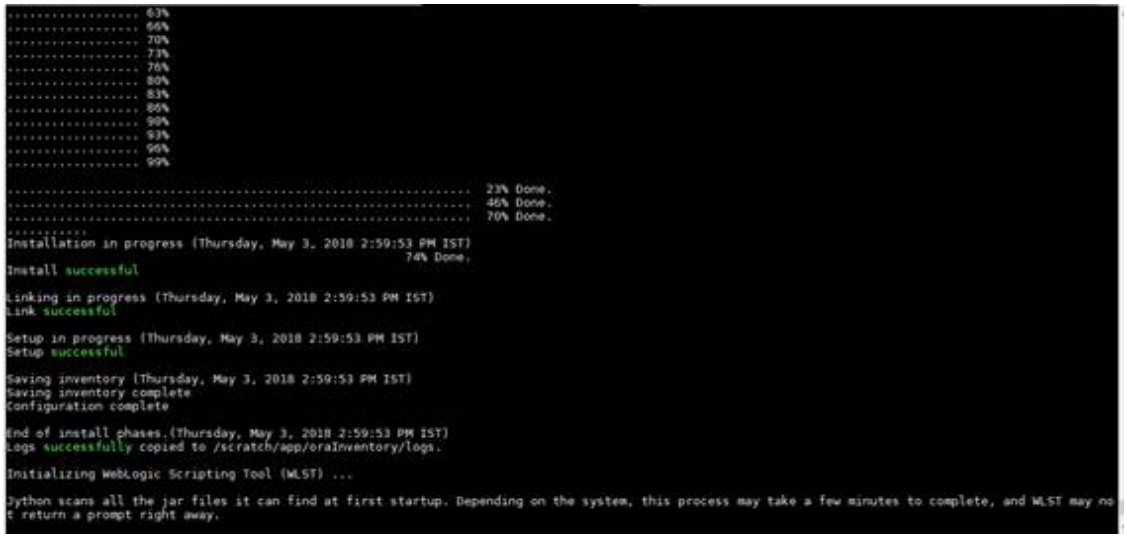


Figure 3–8 Domain Creation Confirmation

3.2 Post Installation Configuration

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

Checklist for Post Installation Procedure

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

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

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

Post Installation Configuration

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

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

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

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

Note

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

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

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

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

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

Then execute following script:

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

A sample output is given here:

Figure 3–9 Starting Post Installation

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

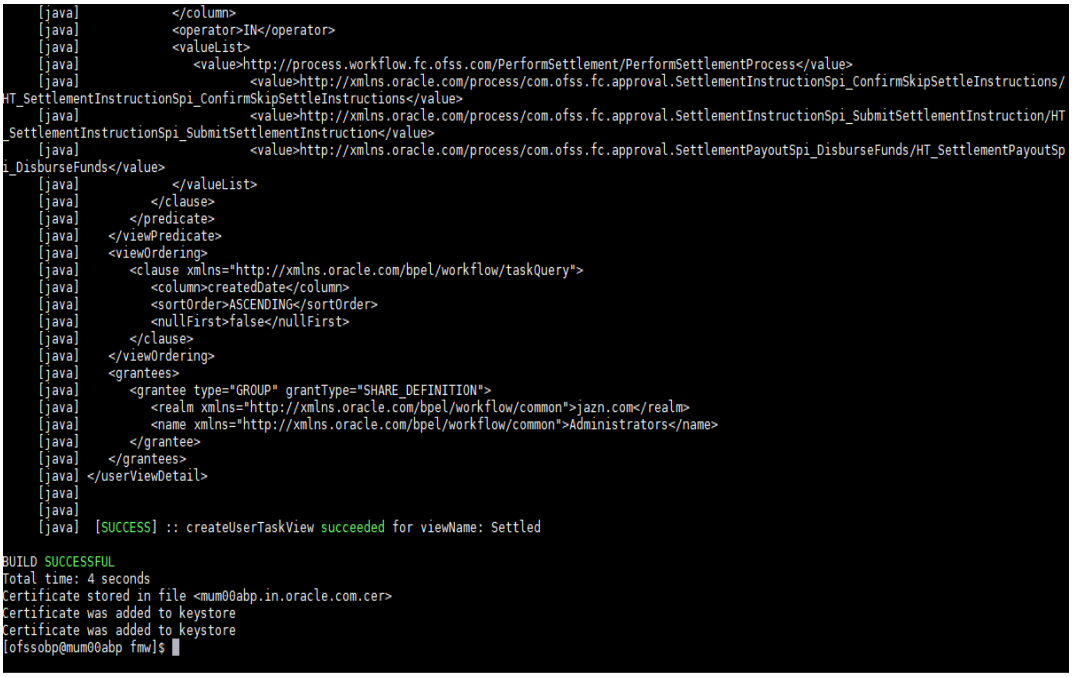
Figure 3–10 Starting Post Installation (contd)

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

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

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

Figure 3–11 SOA Post Installation Completion



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

   deploy-composite-SOA-WLST.log

   post-obp-SOA-WLST.log

   post-soa-GrantAndPolicySet-log.log

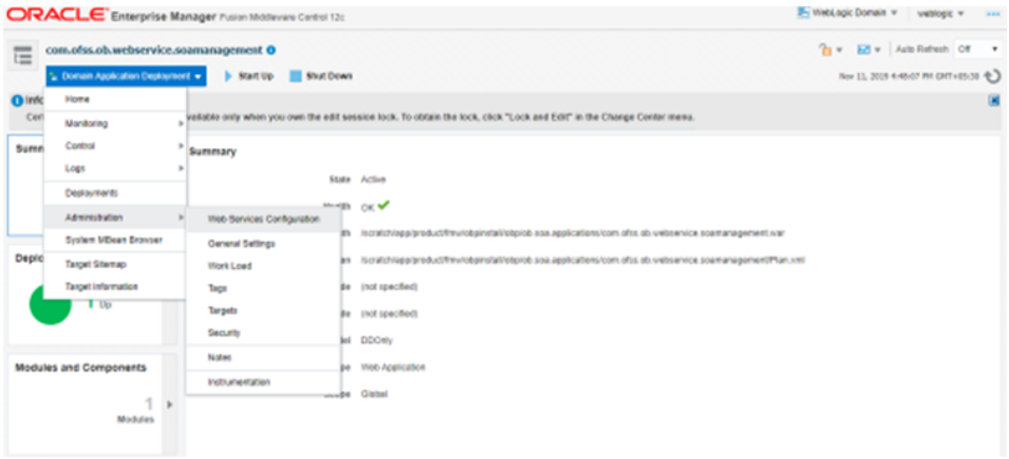
   post-soa-taskflow-grants.log

   update-syncMaxTimeWait.log

   obp-soa-install-log.txt

7. Restart SOA admin and SOA managed server and obphumantask server.
8. After completion of restart, attach the oracle/wss_saml_or_username_token_service_policy in com.ofss.ob.webservice.soamanagement.war. To attach the policy, perform the following steps:
   a. Login to SOA EM.
   b. Click Application Deployments > com.ofss.ob.webservice.soamanagement > Domain Application Deployment > Administration > Web Services Configuration.

Figure 3–12 Go to Web Services Configuration



c. Click Resource Pattern and attach the policy oracle/wss_saml_or_username_token_service_policy for com.ofss.ob.webservice.soamanagement webservice.

Figure 3–13 Attach Policy

4 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 2.3 Installation Checklist.

4.1 Installation and Configuration Procedure

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

4.1.1 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 2.3 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 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 6.1 Pre-Installation Steps and Section 6.2 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.

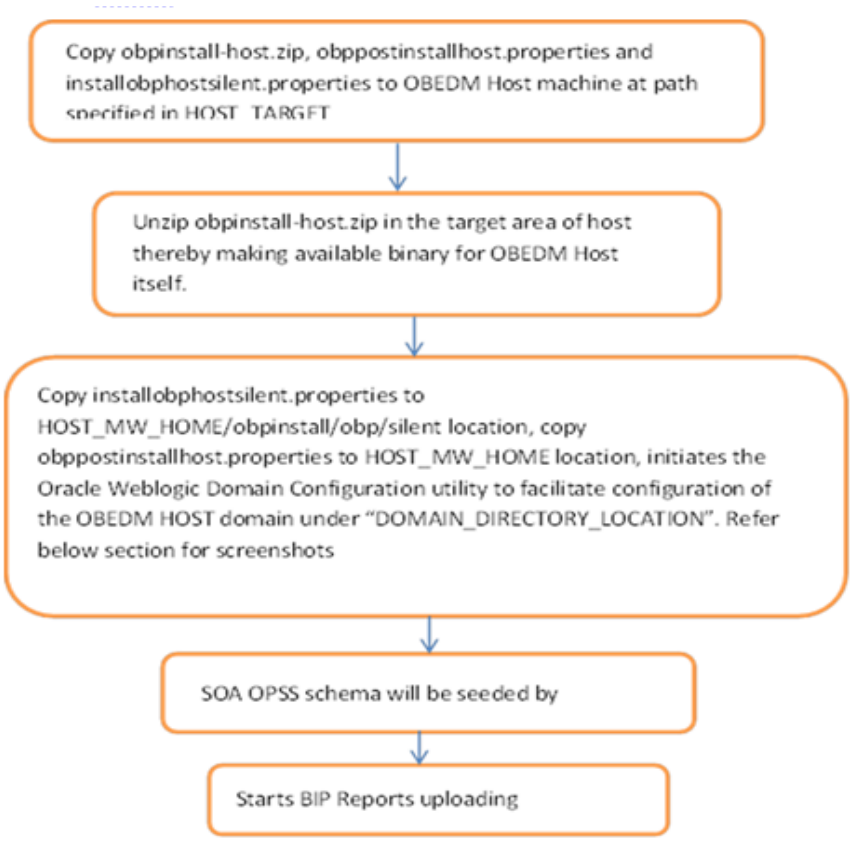
  For example, if HOST_DB_SCHEMA_PREFIX is DEV, then OBP_HOST_DB_USER should be DEV_OBP.
- OID_DOMAIN_NAME in installobphost.properties should match with the OID_DOMAIN_NAME given in installobpui.properties. Any other domain with the same name must not exist in OID. The domain in OID will be created in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

4.1.3 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 4–1 Steps in installobphost.sh script



A sample output is given here.

Figure 4–2 Verification of Properties

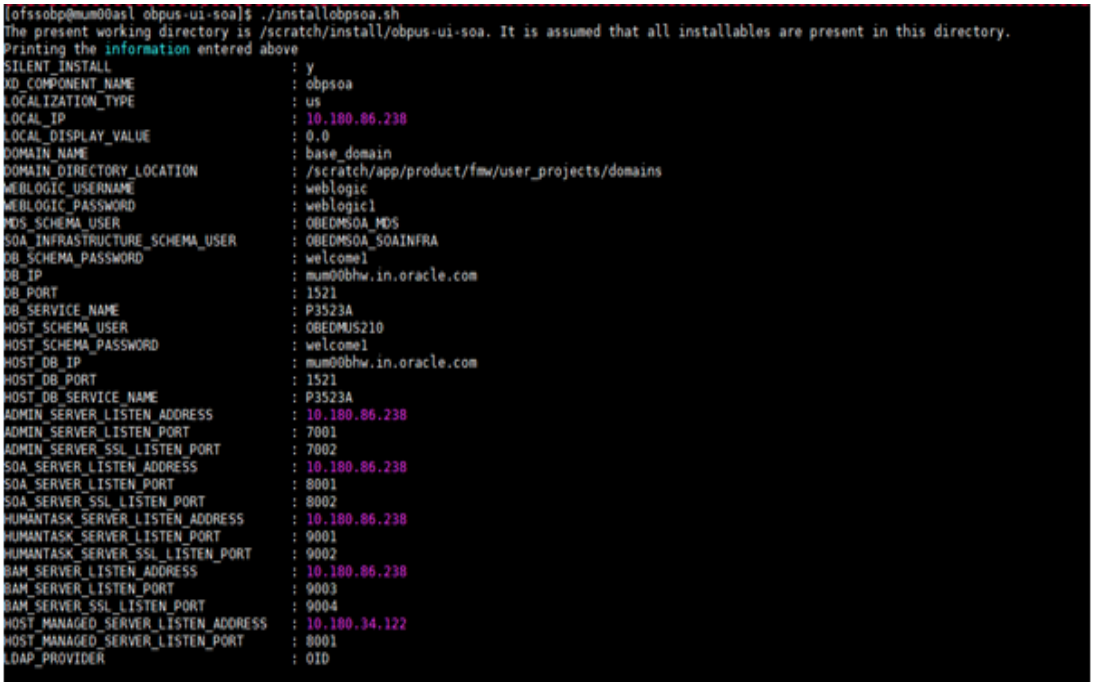


Figure 4–3 Verification of Properties (contd)

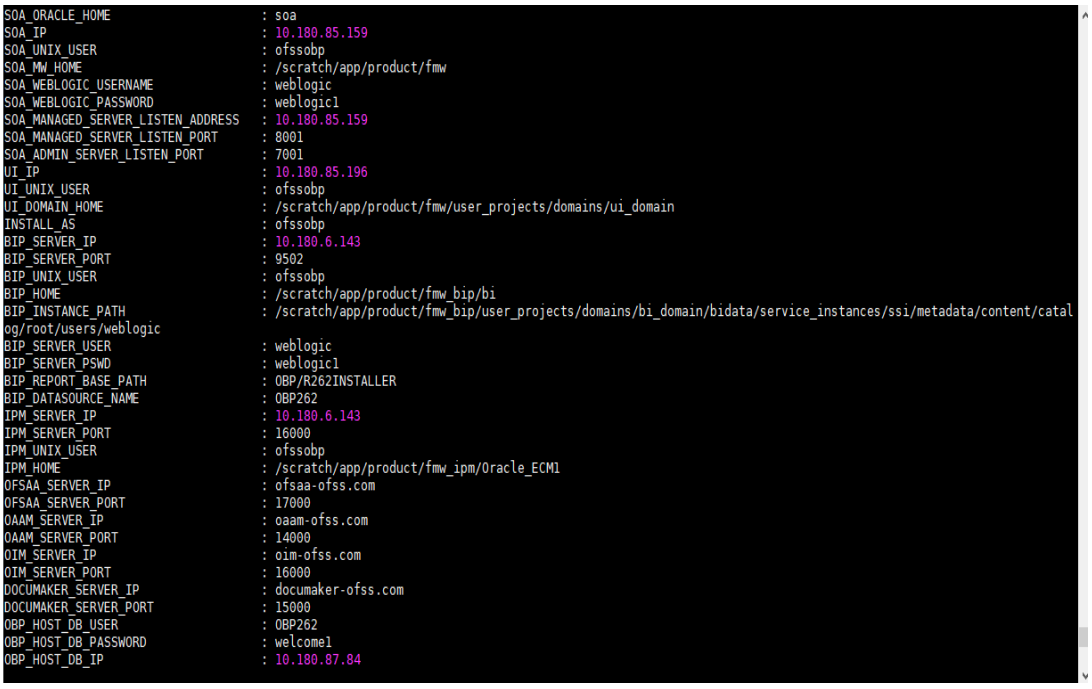


Figure 4–4 Verification of Properties (contd)

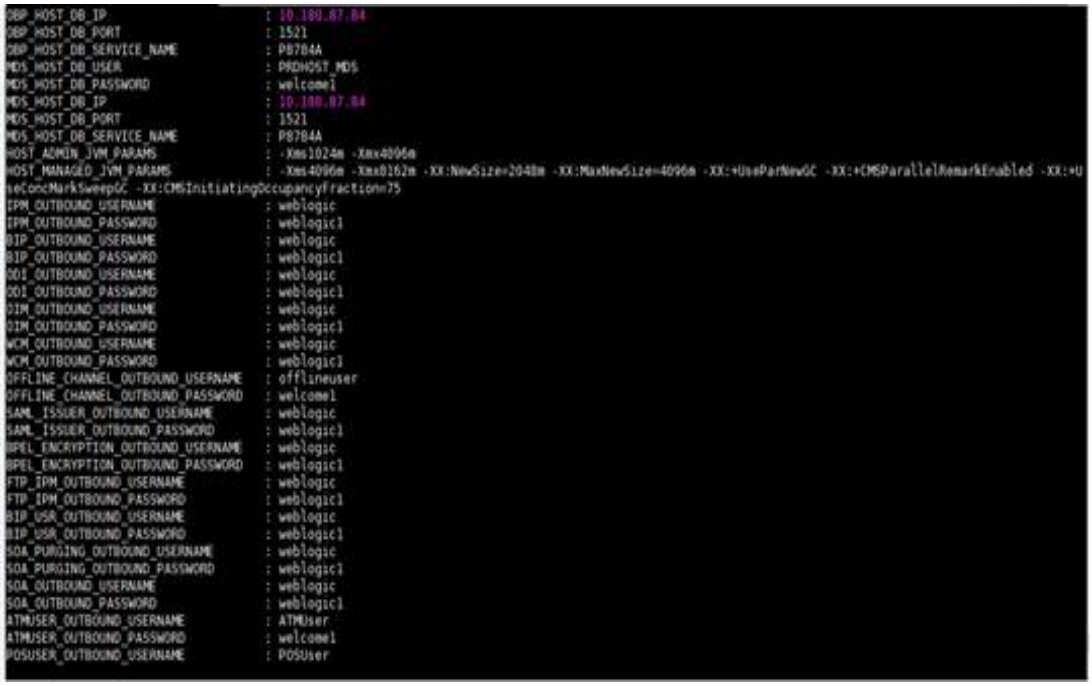
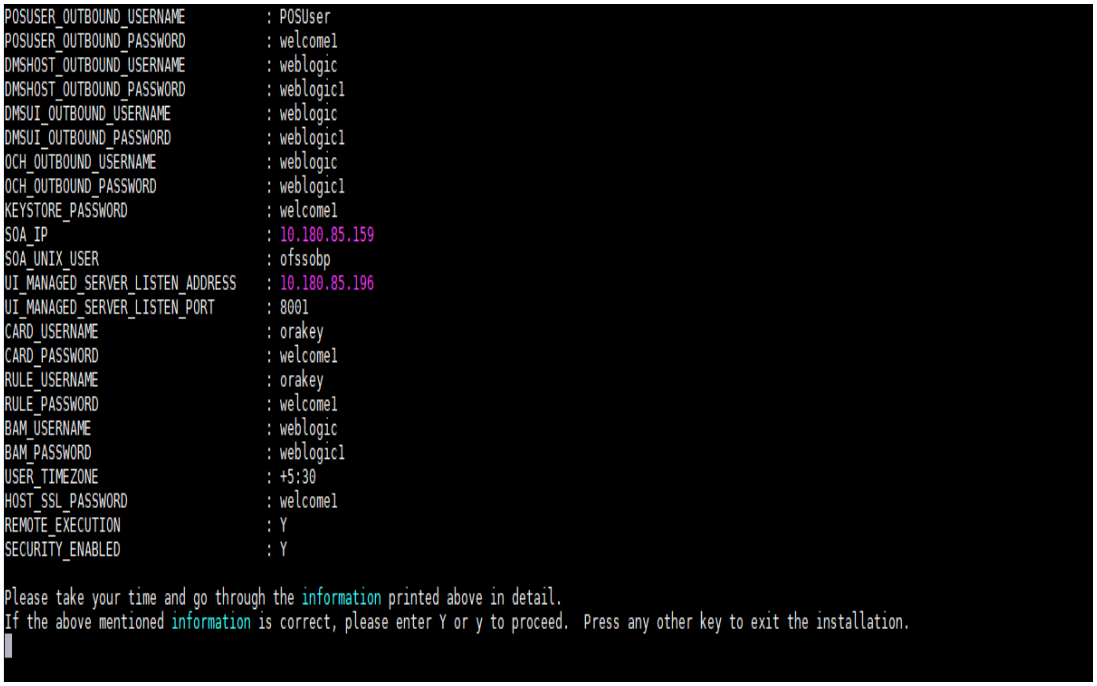


Figure 4–5 Verification of Properties (contd)



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

utility performs the installation and domain is created silently.

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

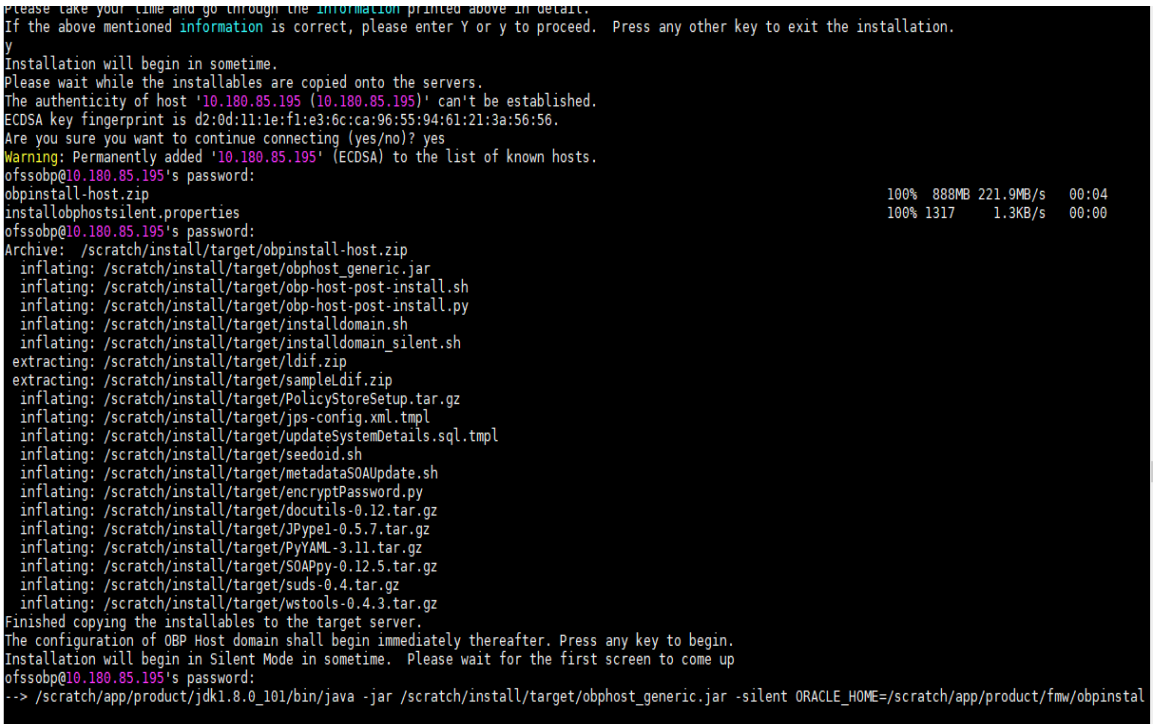


Figure 4–7 Confirmation and Copying of Installables to Target Machine (contd)

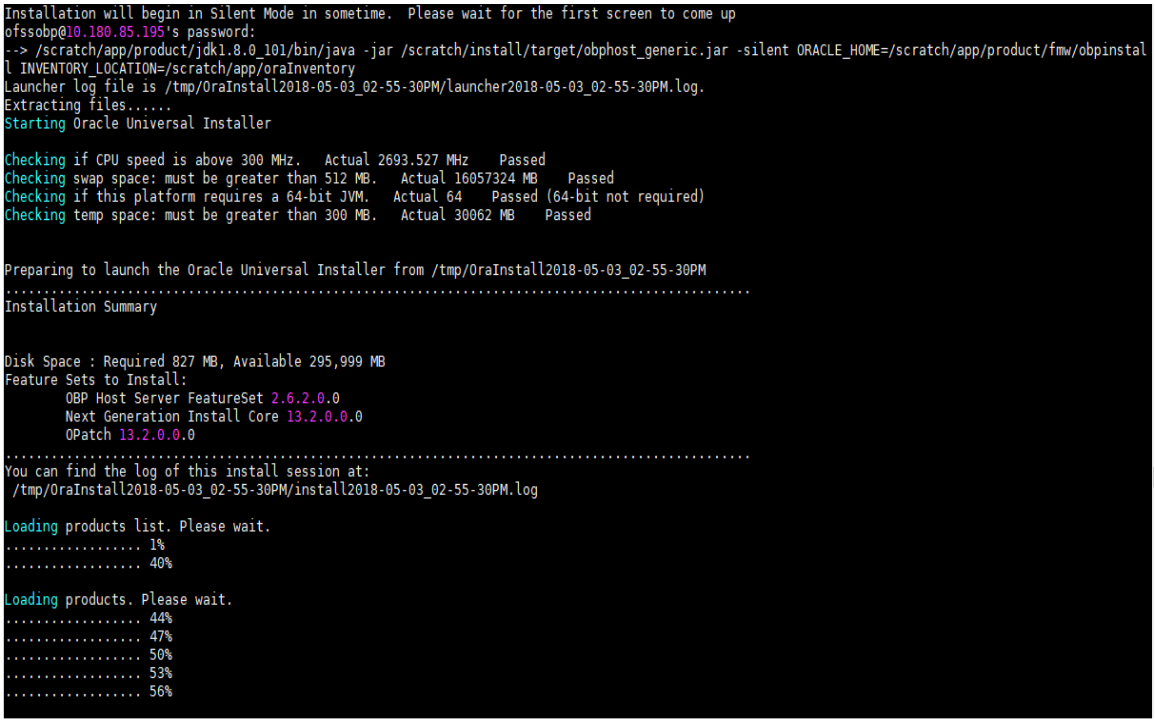
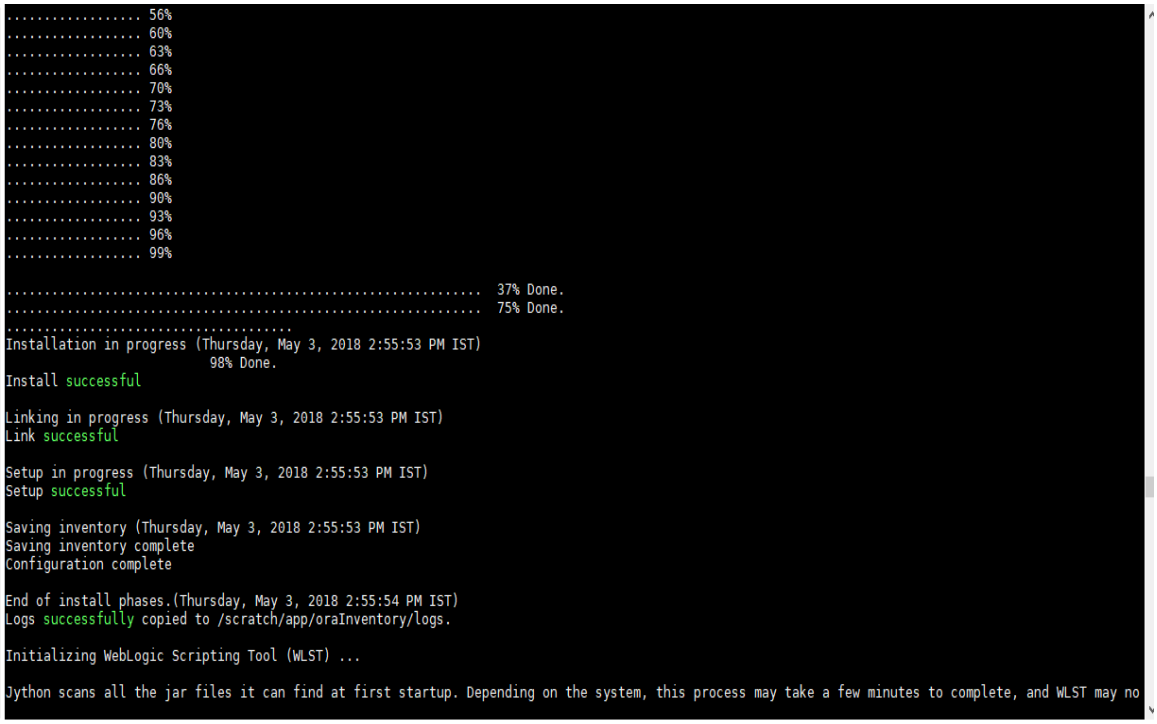
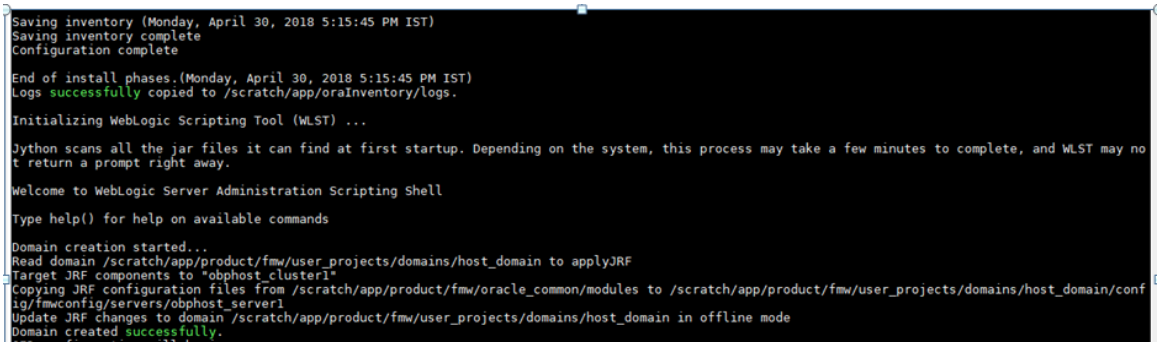


Figure 4–8 Confirmation and Copying of Installables to Target Machine (contd)



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

Figure 4–9 Domain Installation Confirmation



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

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

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

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

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

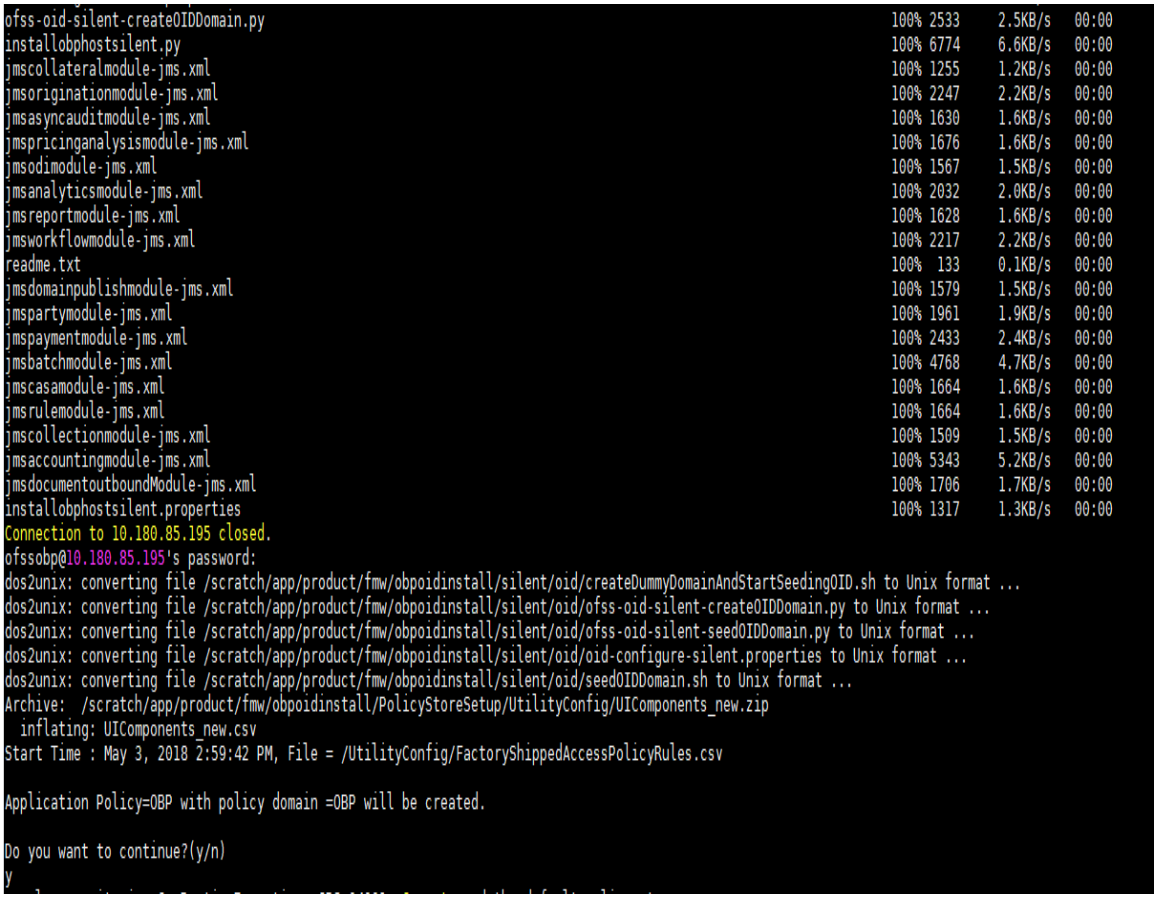
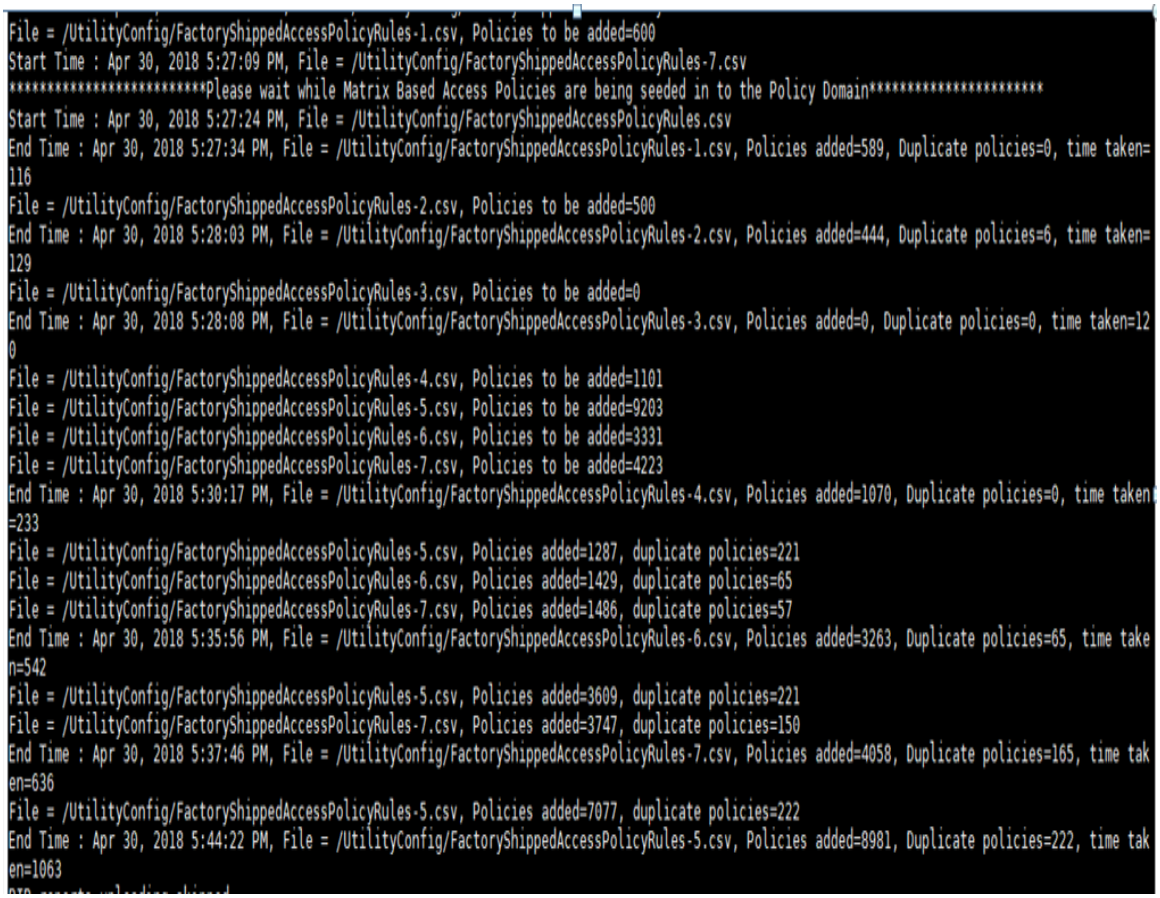


Figure 4–13 Policy Seeding

Figure 4–14 Policy Seeding (contd)



4.2 Post Installation Configuration

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

Checklist for Post Installation Procedure

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

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

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

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

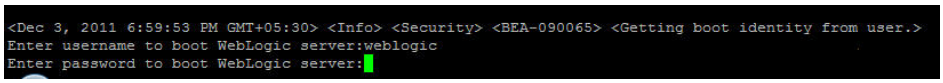
Post Installation Configuration

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

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

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

   Figure 4–15 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 4–16 Host Domain Post Installation Script Execution

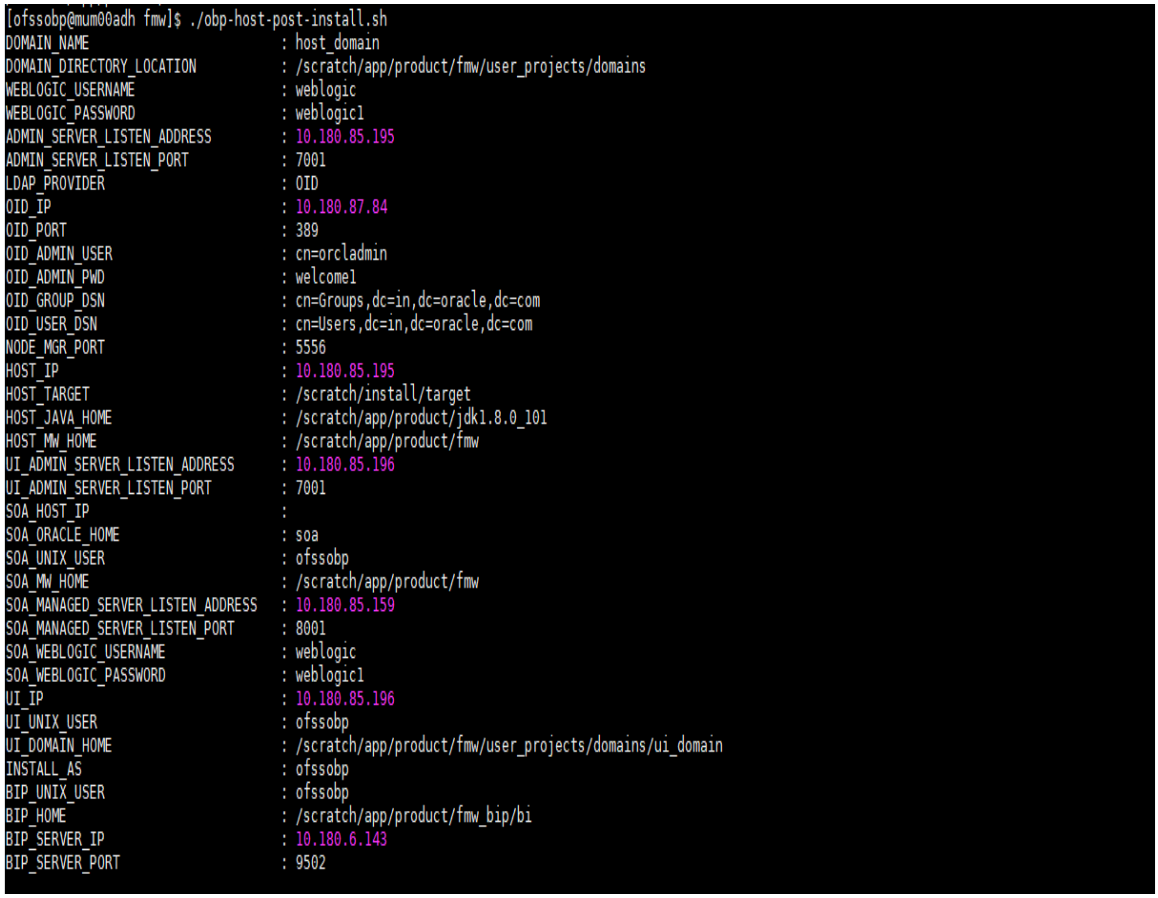


Figure 4–17 Host Domain Post Installation Script Execution (contd)

```
BIP_SERVER_IP                    : 10.180.6.143
BIP_SERVER_PORT                  : 9502
IPM_SERVER_IP                    : 10.180.6.143
IPM_SERVER_PORT                  : 16000
OFSAA_SERVER_IP                  : ofsaa-ofss.com
OFSAA_SERVER_PORT                : 17000
OAAM_SERVER_IP                   : oaam-ofss.com
OAAM_SERVER_PORT                 : 14000
OAAM_SERVER_IP                   : oaam-ofss.com
OAAM_SERVER_PORT                 : 14000
OIM_SERVER_IP                    : oim-ofss.com
OIM_SERVER_PORT                  : 16000
DOCUMAKER_SERVER_IP              : documaker-ofss.com
DOCUMAKER_SERVER_PORT            : 15000
OBP_HOST_DB_USER                 : OBP262
OBP_HOST_DB_PASSWORD             : welcome1
OBP_HOST_DB_IP                   : 10.180.87.84
OBP_HOST_DB_PORT                 : 1521
OBP_HOST_DB_SERVICE_NAME         : P8784A
IPM_OUTBOUND_USERNAME            : weblogic
IPM_OUTBOUND_PASSWORD            : weblogic1
BIP_OUTBOUND_USERNAME            : weblogic
BIP_OUTBOUND_PASSWORD            : weblogic1
ODI_OUTBOUND_USERNAME            : weblogic
ODI_OUTBOUND_PASSWORD            : weblogic1
OIM_OUTBOUND_USERNAME            : weblogic
OIM_OUTBOUND_PASSWORD            : weblogic1
WCM_OUTBOUND_USERNAME            : weblogic
WCM_OUTBOUND_PASSWORD            : weblogic1
OFFLINE_CHANNEL_OUTBOUND_USERNAME  : offlineuser
OFFLINE_CHANNEL_OUTBOUND_PASSWORD  : welcome1
SAML_ISSUER_OUTBOUND_USERNAME    : weblogic
SAML_ISSUER_OUTBOUND_PASSWORD    : weblogic1
BPEL_ENCRYPTION_OUTBOUND_USERNAME  : weblogic
BPEL_ENCRYPTION_OUTBOUND_PASSWORD  : weblogic1
FTP_IPM_OUTBOUND_USERNAME        : weblogic
FTP_IPM_OUTBOUND_PASSWORD        : weblogic1
BIP_USR_OUTBOUND_USERNAME        : weblogic
```

Figure 4–18 Host Domain Post Installation Script Execution (contd)

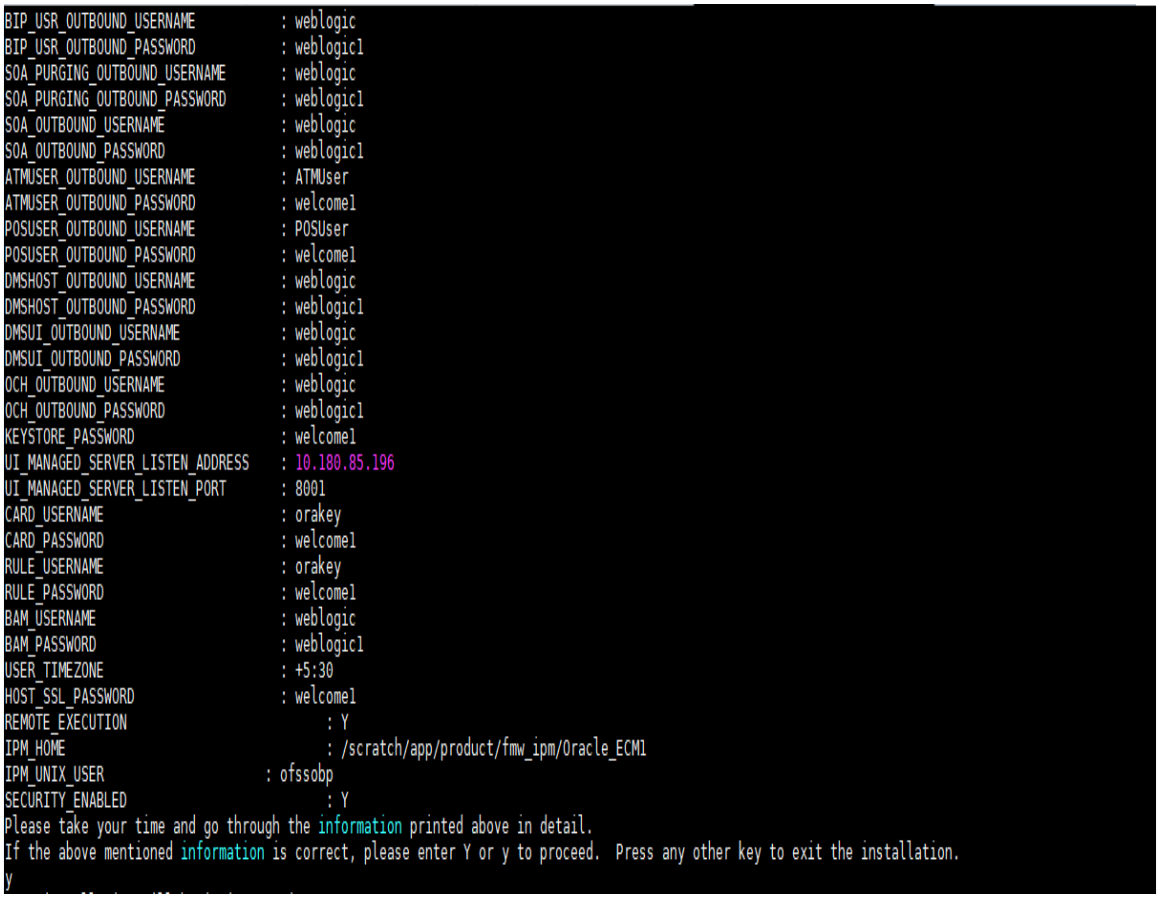


Figure 4–19 Host Domain Post Installation Script Execution (contd)

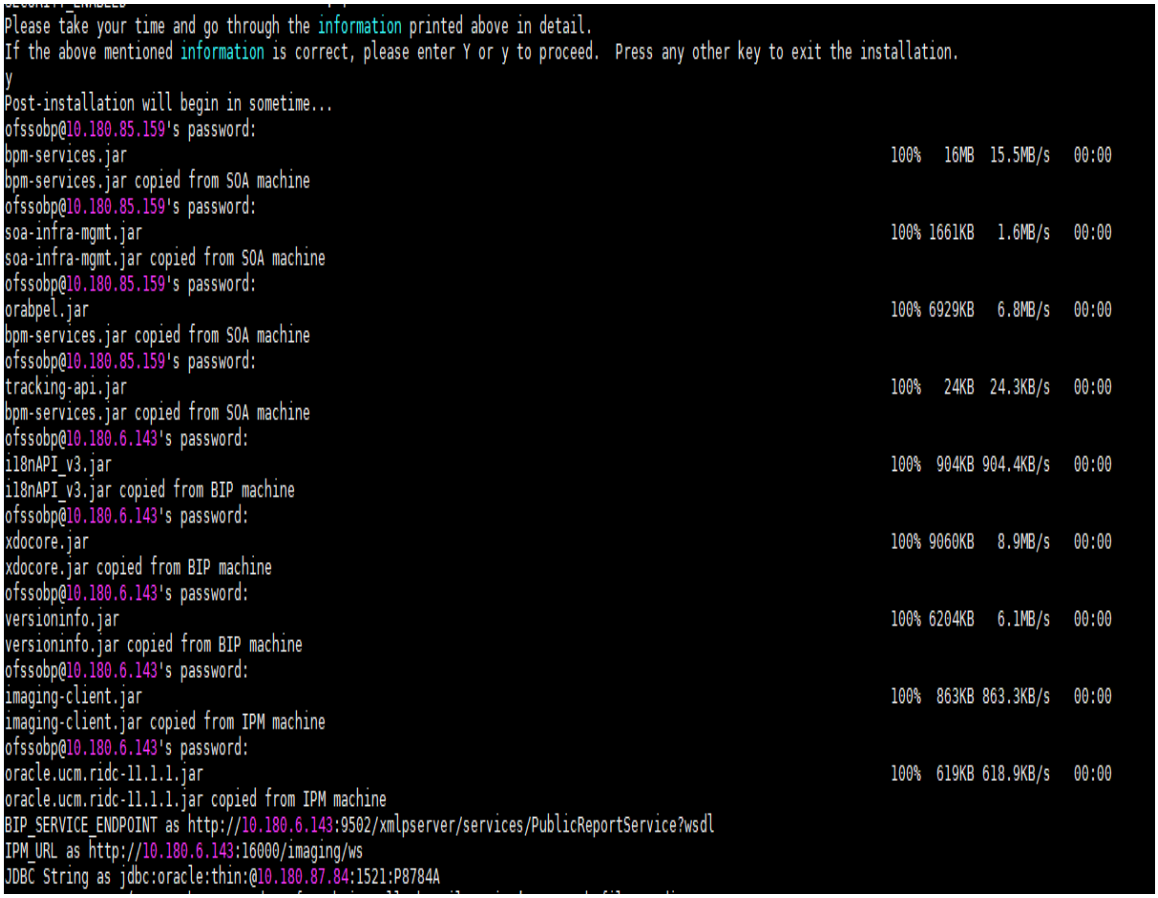
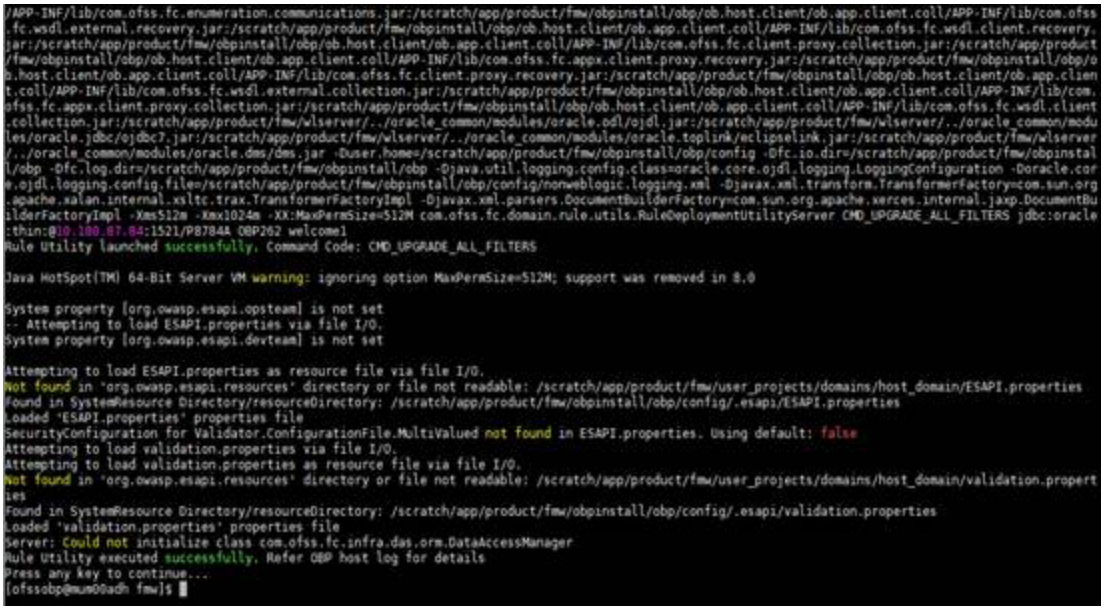


Figure 4–20 Host Domain Post Installation Script Execution Summary



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

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

   within the following xml tag:

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

   add:

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

9. Within the following xml tag:

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

add:

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

10. Then start the admin and managed servers to check the domain configuration status as described in verification part in Section 10.2 Host Domain Verification.

5 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 2.3 Installation Checklist.

5.1 Installation and Configuration Procedure

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

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

- A zip file 'obpinstall-ui-soa.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 2.3 Installation Checklist of this guide and note the values applicable for each point in the last column for 'Value' so that the same is handy during the actual installation.

5.1.2 Pre-Installation Steps

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

Step 1 Updating installobpui.properties

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

Step 2 Checklist for a new setup

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

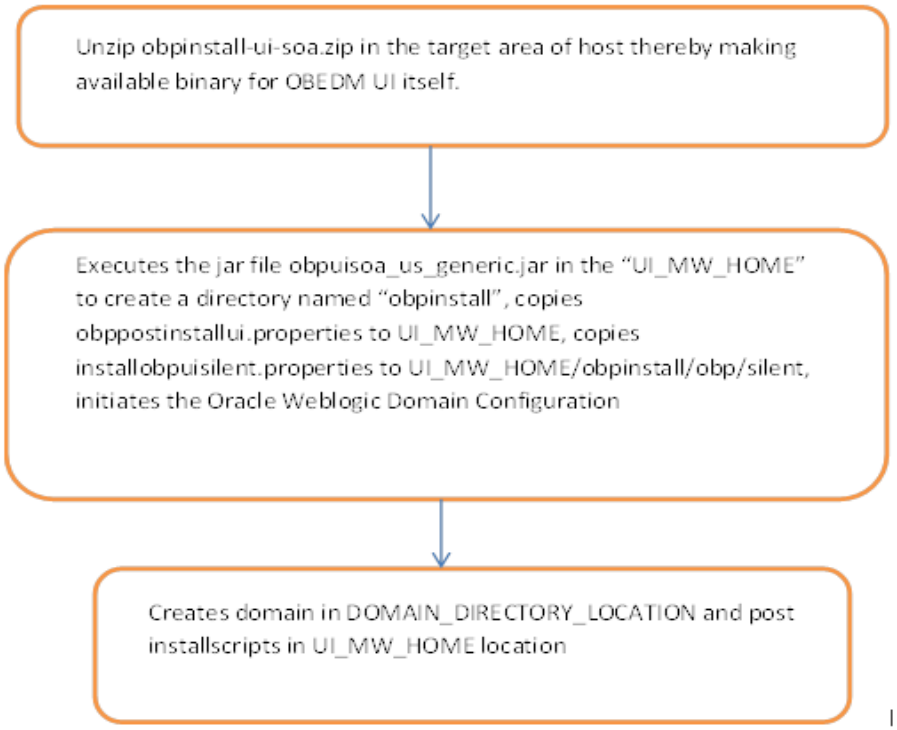
- Make sure required RCU schemas have been created. For more information, see Section 6.1 Pre-Installation Steps and Section 6.2 OBEDM Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against UI_TARGET 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.

5.1.3 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 5–1 Steps in installobpui.sh script



A sample output is given here.

Figure 5–2 Confirmation to Proceed Domain Installation

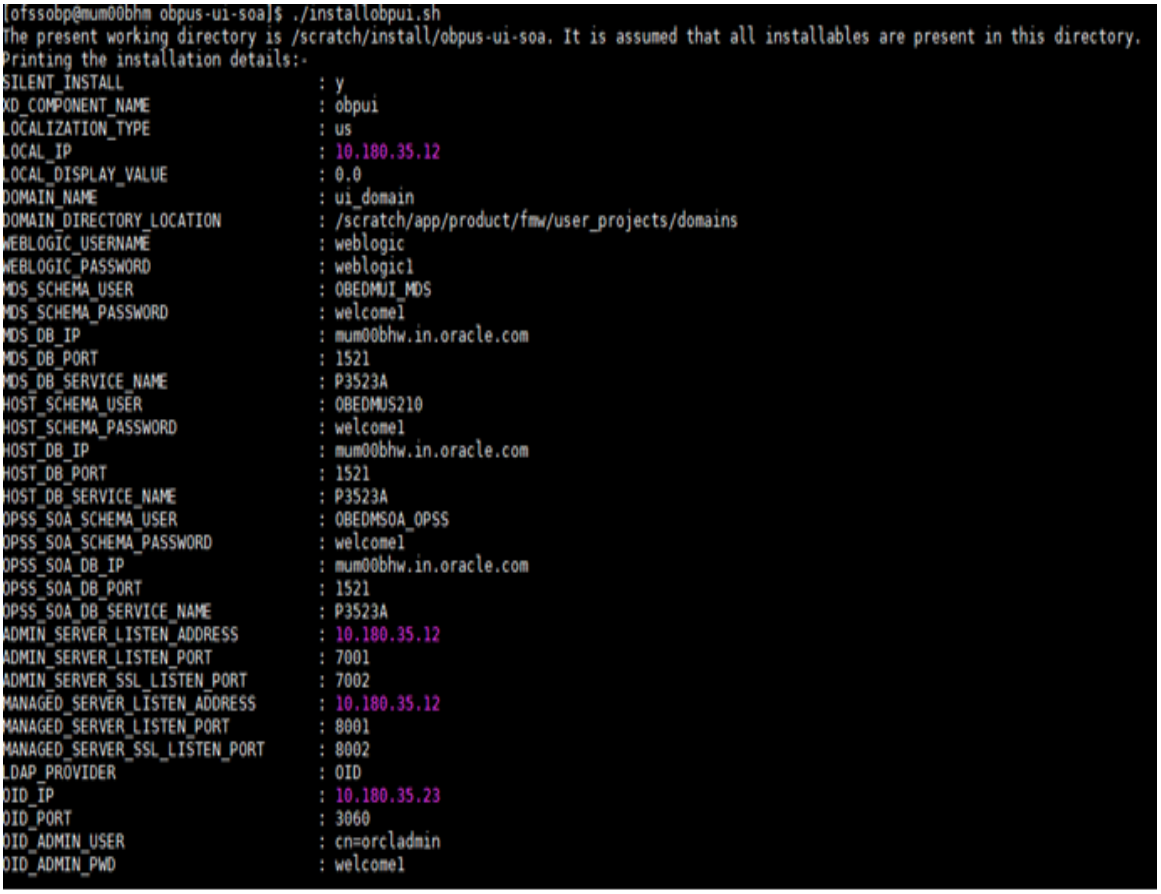


Figure 5–3 Confirmation to Proceed Domain Installation (contd)

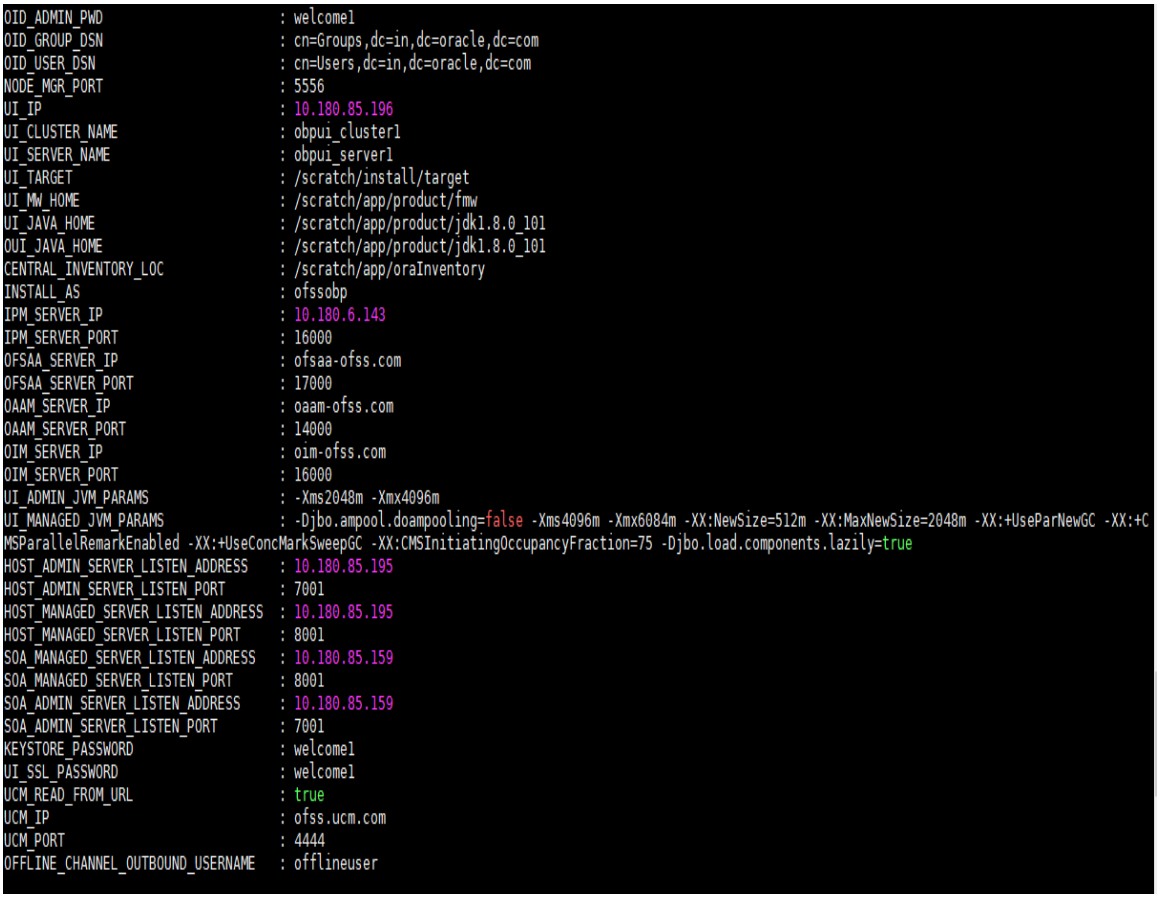


Figure 5–4 Confirmation to Proceed Domain Installation (contd)

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

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

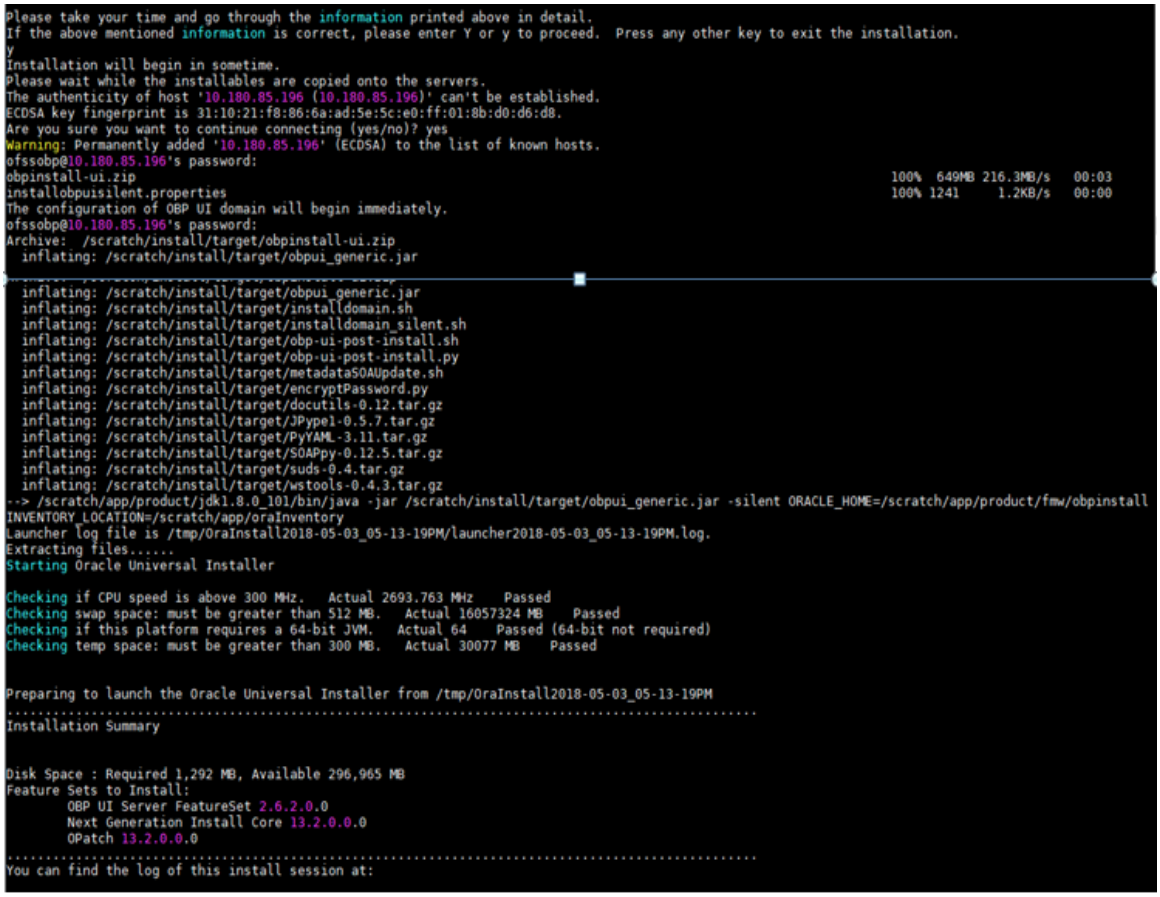


Figure 5–6 Copying and Extraction of obpinstall-ui-soa.zip (contd)

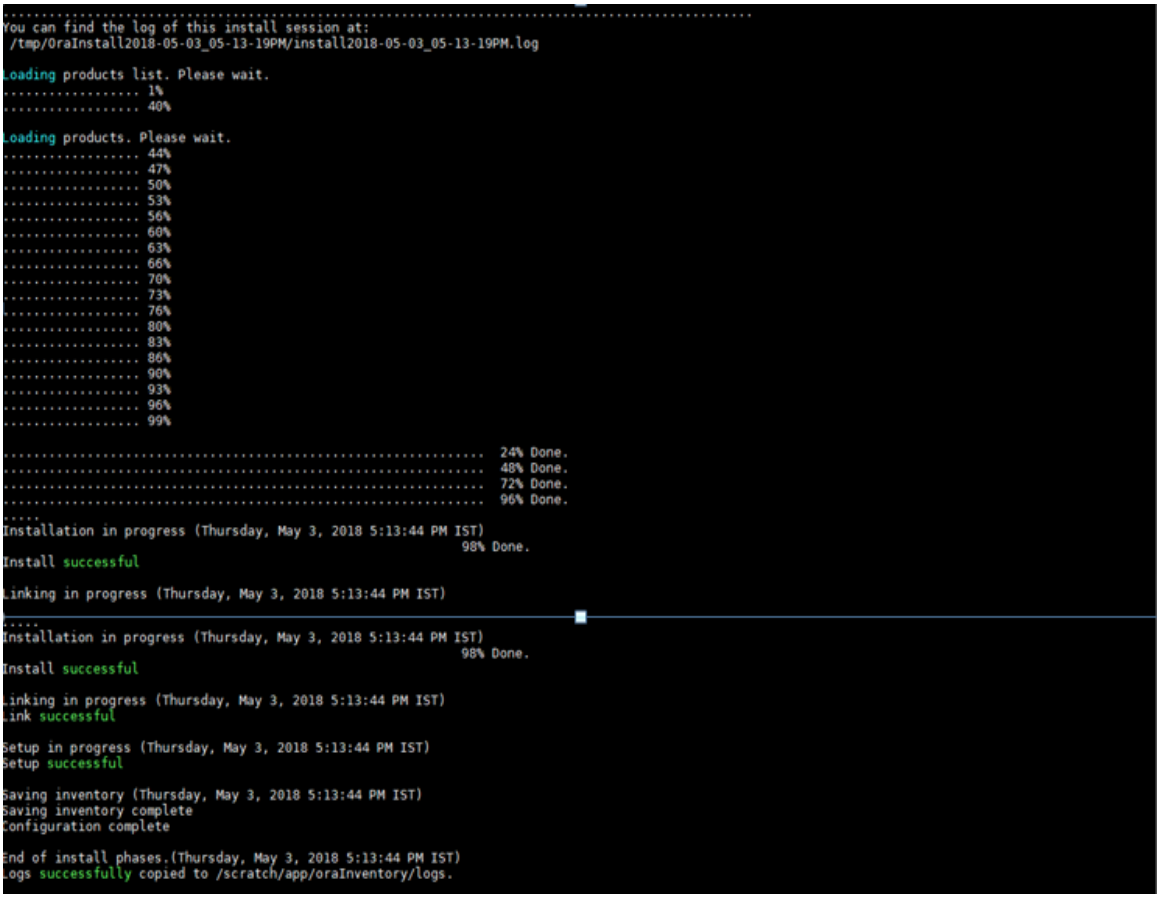
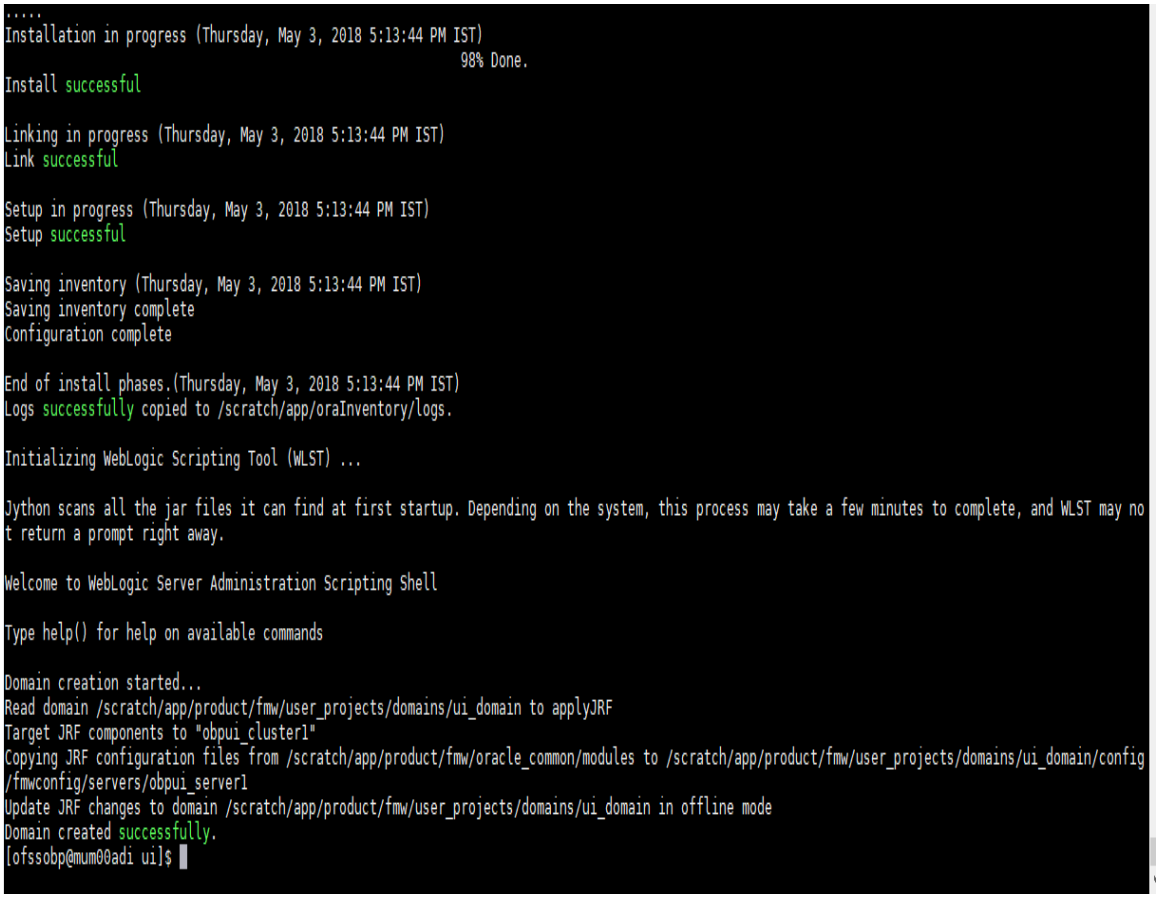


Figure 5–7 Domain Creation Confirmation



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

5.2 Post Installation Configuration

This section describes the post installation configuration procedure for 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 5–8 UI Admin Server Credentials

Figure 5–9 UI Admin Server Running

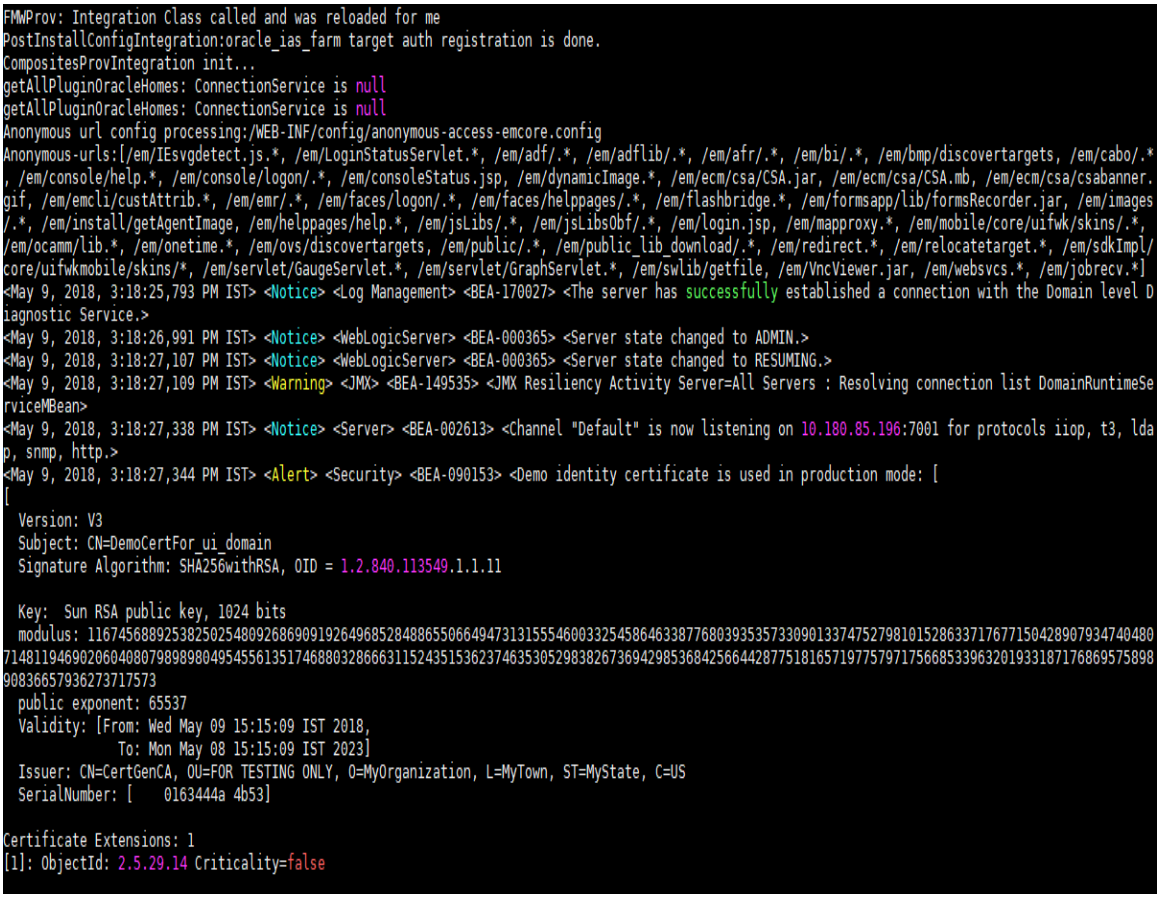


Figure 5–10 UI Admin Server Running (contd)

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

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

6. Execute the script using the following commands:

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

Figure 5–11 Starting Post Installation

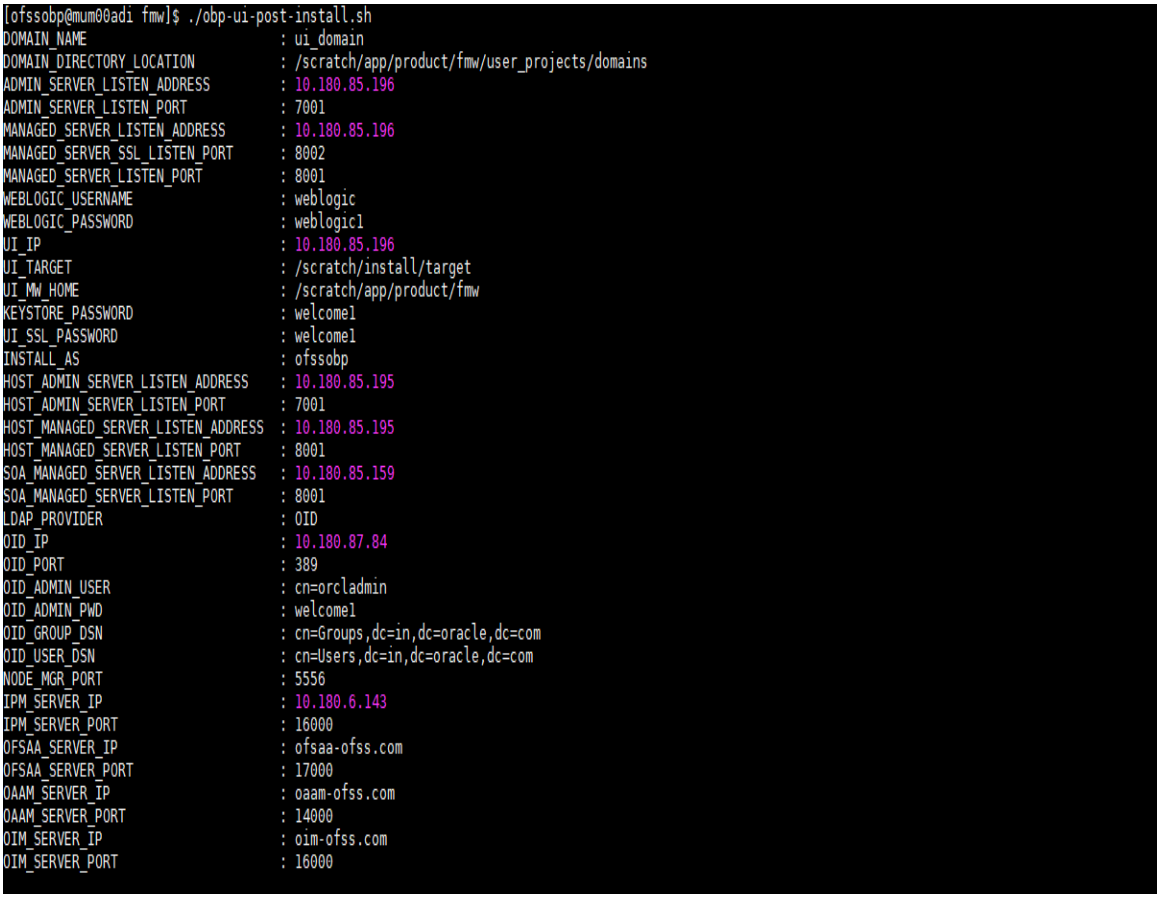


Figure 5–12 Starting Post Installation (contd)

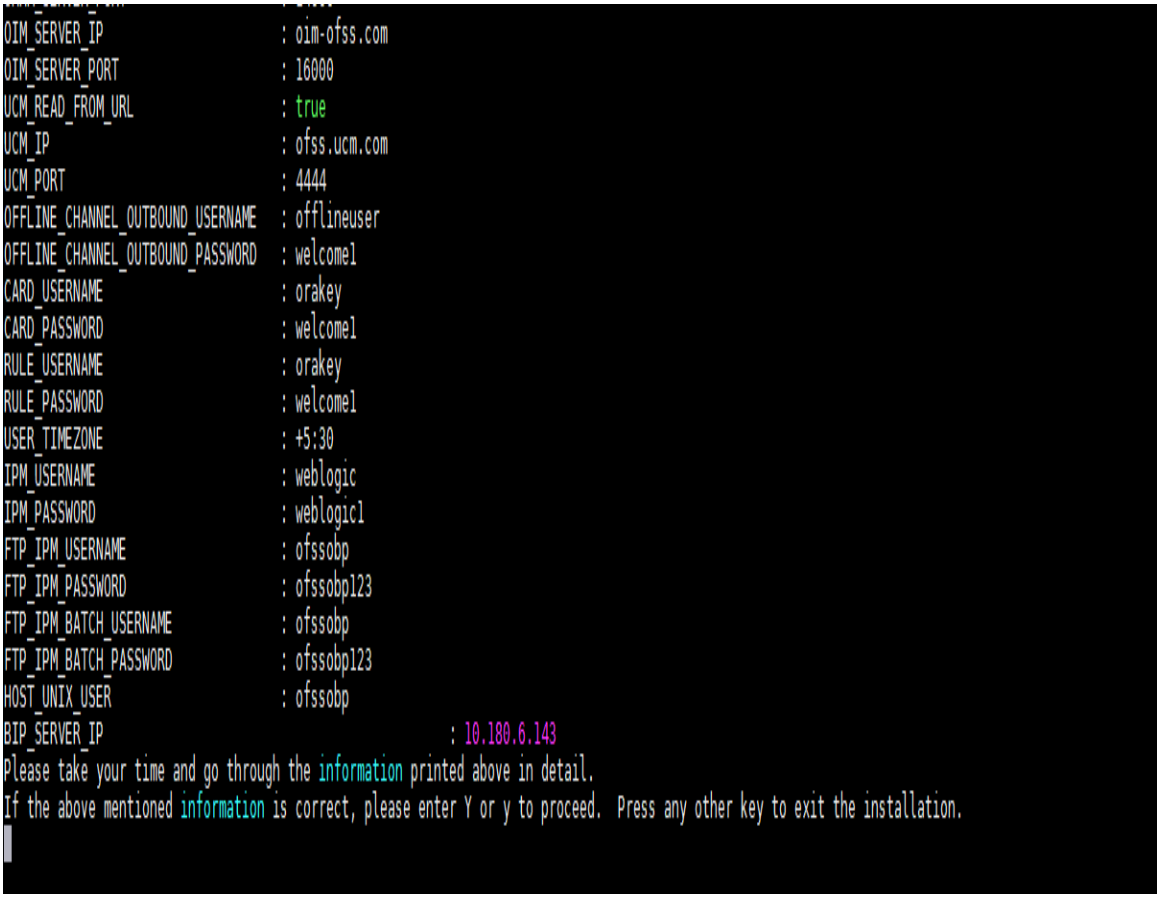


Figure 5–13 Continuation of Post-Installation

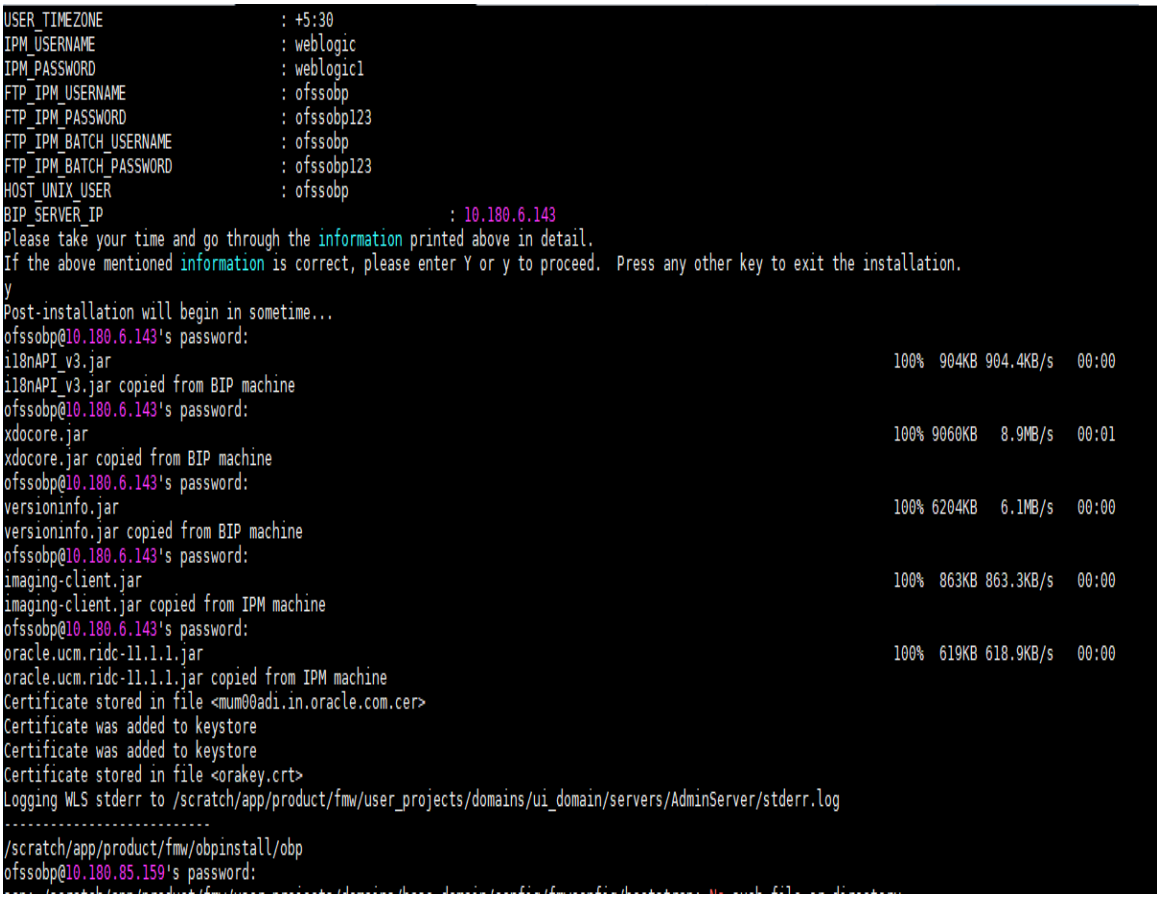
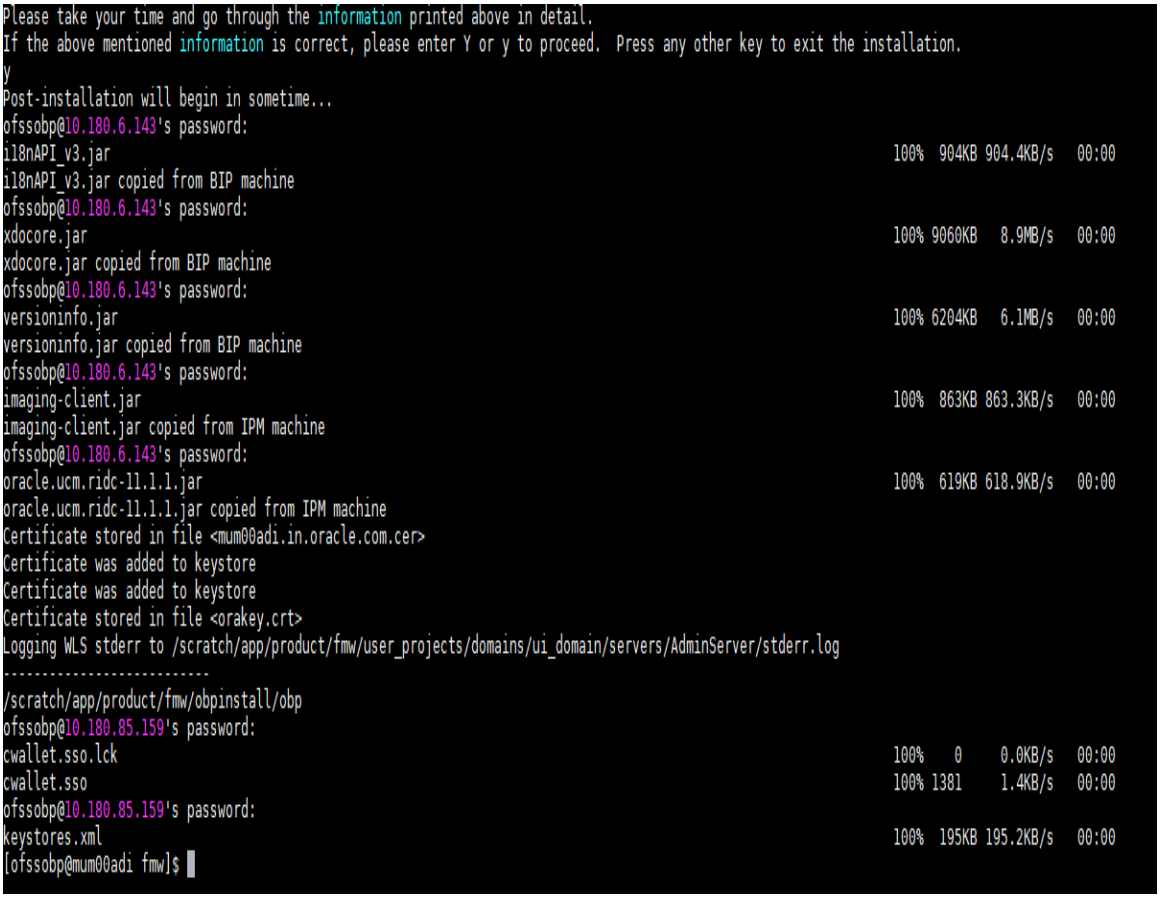


Figure 5–14 Continuation of Post-Installation (contd)



7. For monitoring the script run check the following log files created under the ui domain directory:
   - obp-ui-install-log.txt
   - obp-ui-install-log-py.txt
8. Restart UI admin and UI managed server.

6 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.

6.1 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 6.2 OBEDM Database Setup – RCU Installation:

1. Oracle Database Enterprise Edition 12.2.0.1.0 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.

6.2 OBEDM Database Setup – RCU Installation

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

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

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

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

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

- 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.

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

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

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

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

6.3 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.

6.3.1 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
```

6.3.2 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.

6.3.3 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.

6.3.4 System Configuration DB Update Script Execution

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

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

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

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

```
C:> D:
C:> cd D:\script
D:\seed > sqlplus DEV_OBEDM@welcome1@OBEDMDB
D:\seed >@updateSystemDetails.sql
```

After ddl and seed execution, execute FLX_FW_ARTIFACTS_UICOMP_EXT present under obpus-host.zip.

7 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 7.1 IPM Application Setup for OBEDM Content Management
- Section 7.2 IPM Configuration for Bulk Upload Process Setup
- Section 7.3 IPM Report Upload Setup

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

7.1 IPM Application Setup for 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.

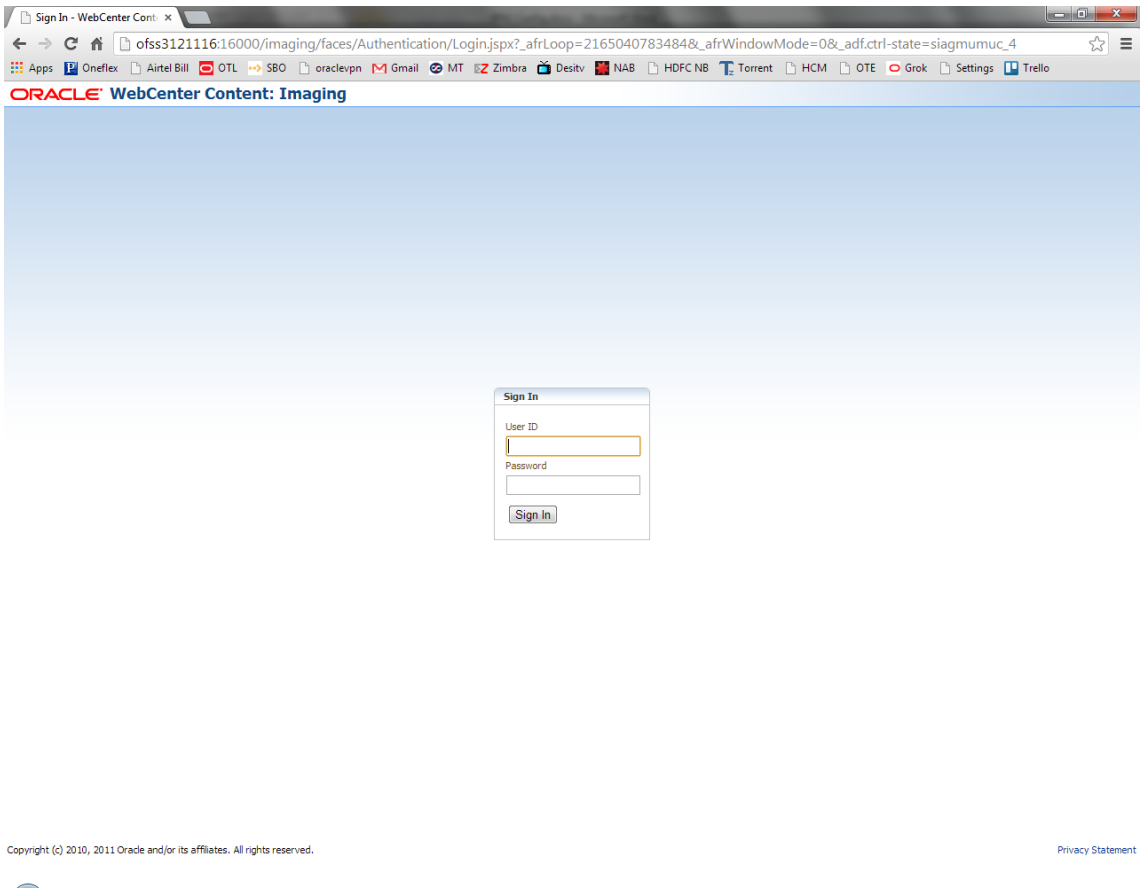
7.1.1 UCM Connection

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

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

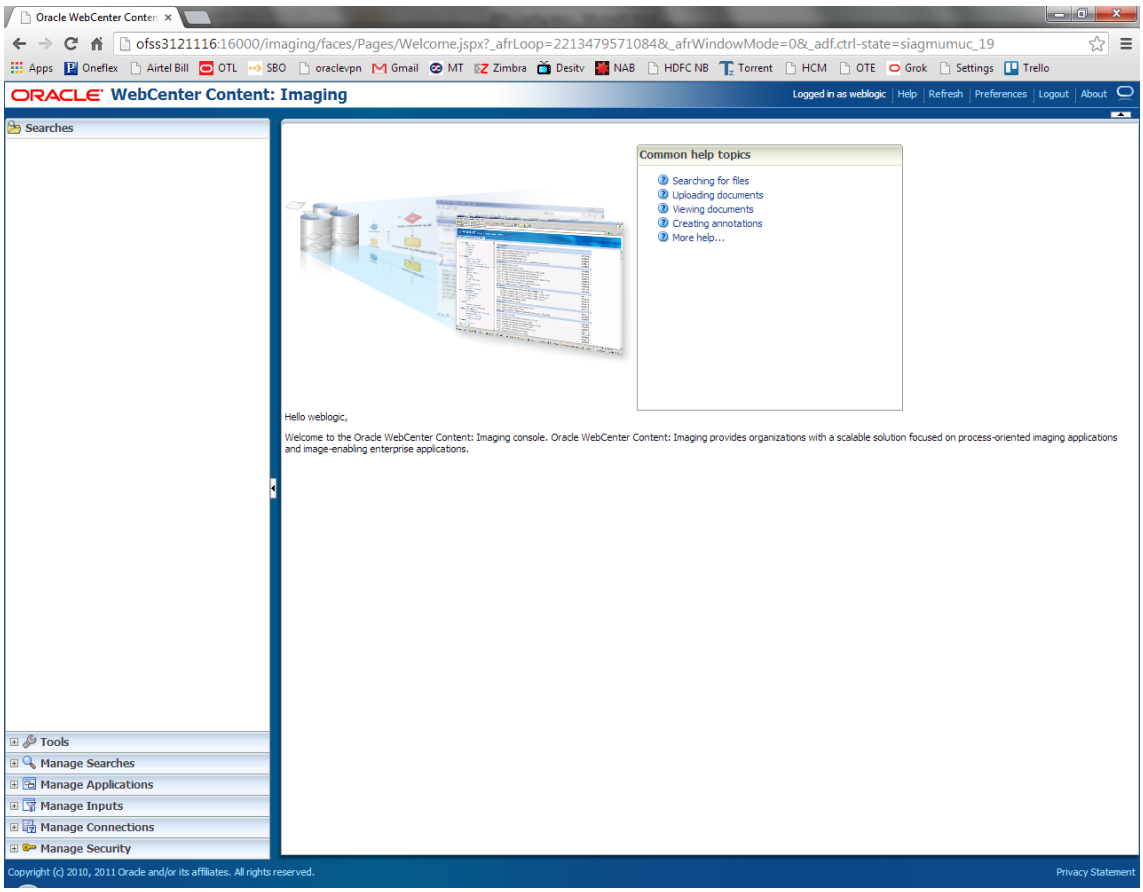
   http:// hostname:16000/imaging

Figure 7–1 IPM Imaging Console - Login page



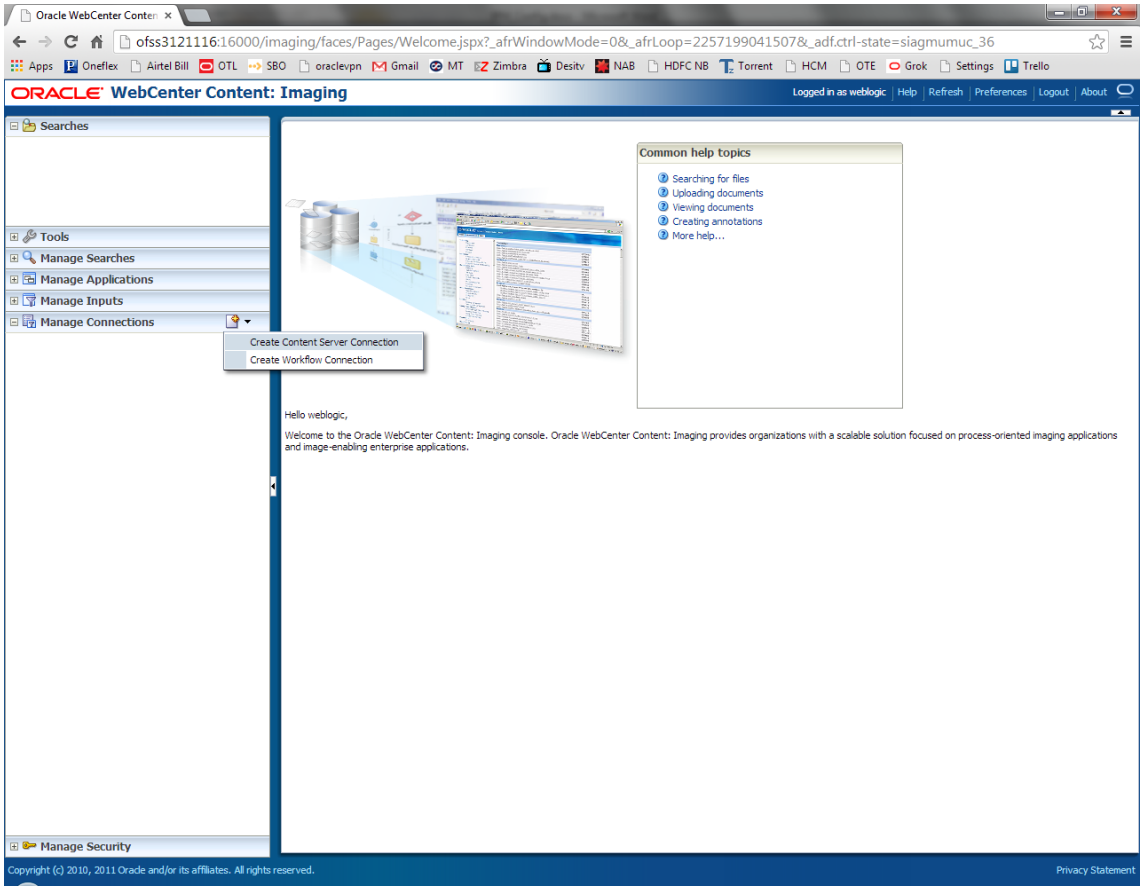
2. Enter the user ID and password set during IPM installation.

Figure 7–2 IPM - Welcome page



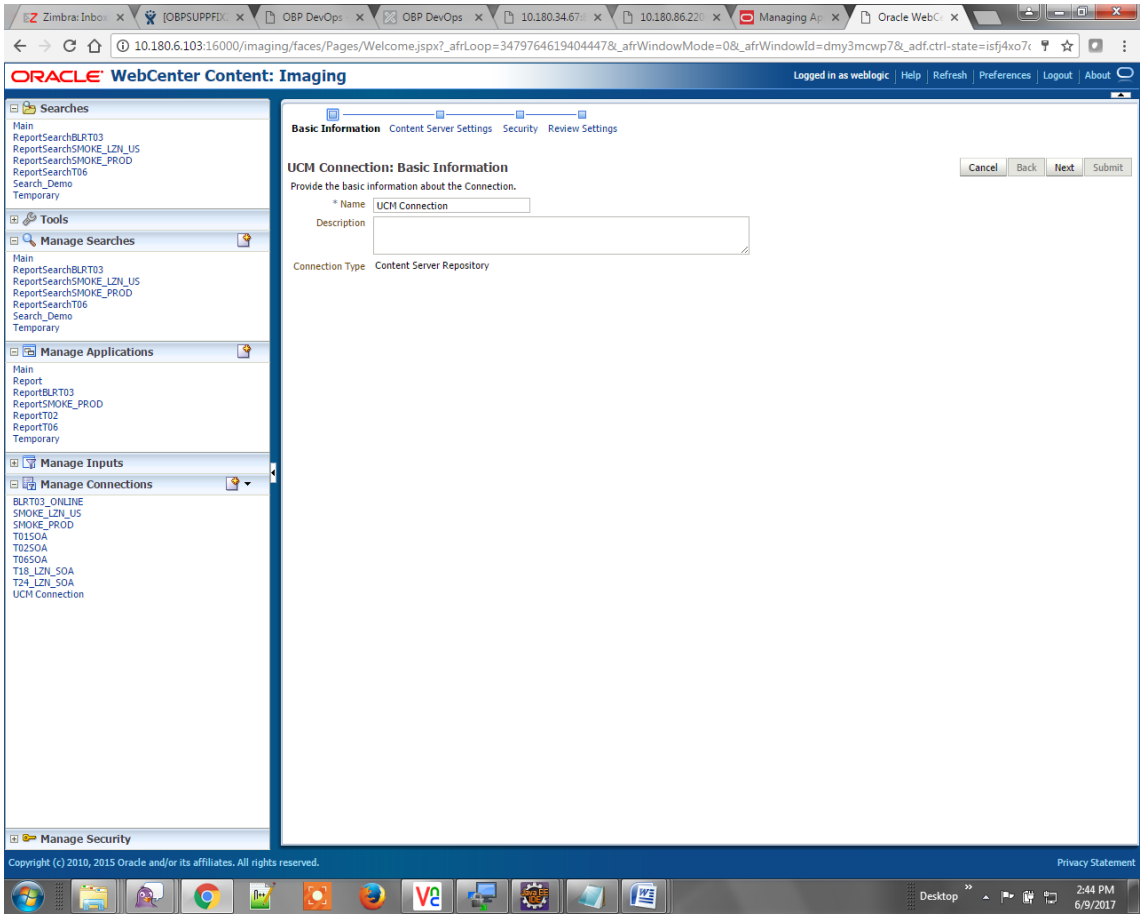
3. Navigate to Manage Connection and select Create Content Server Connection.

Figure 7–3 Create Content Server Connection



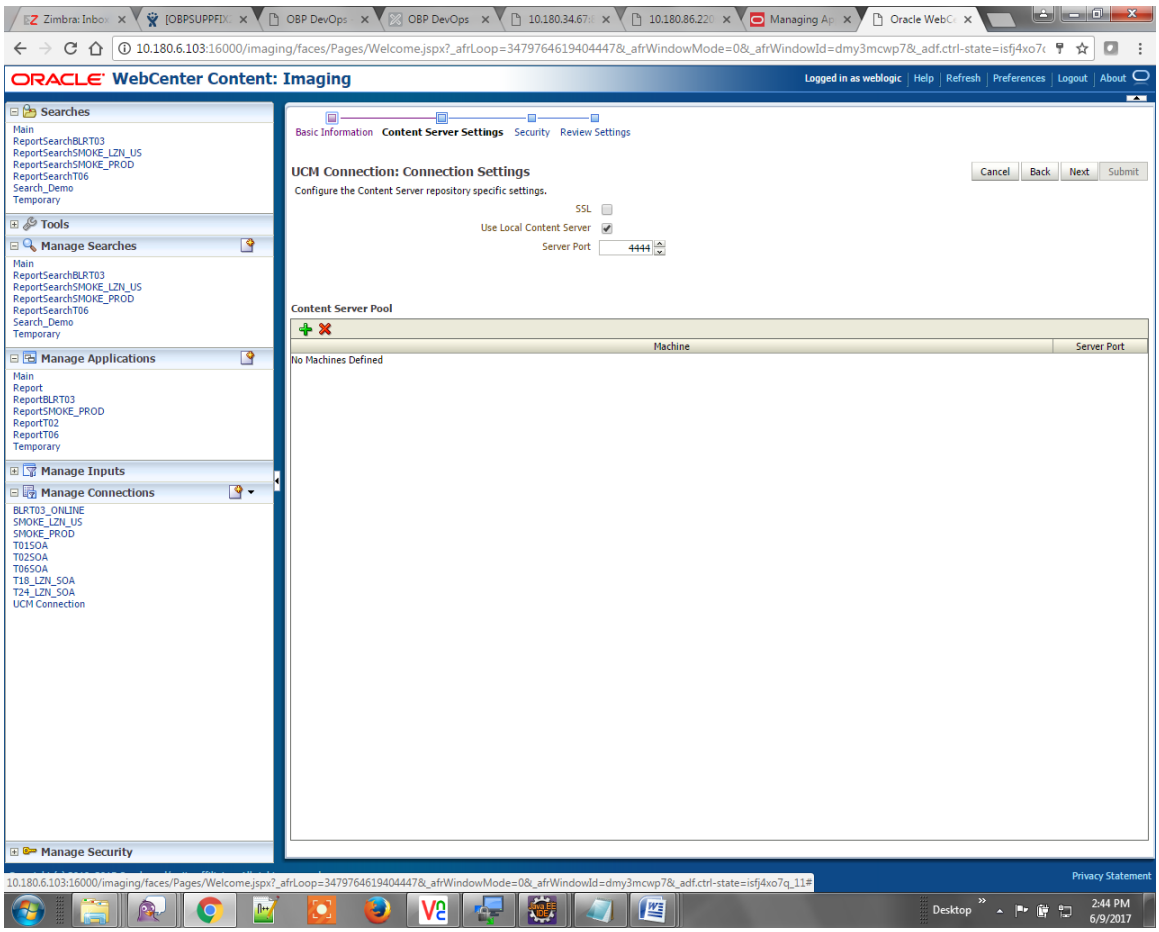
4. In the Basic Information stage, enter the name and description for Content Server Connection as UCM Connection and click Next.

Figure 7–4 UCM: Basic information



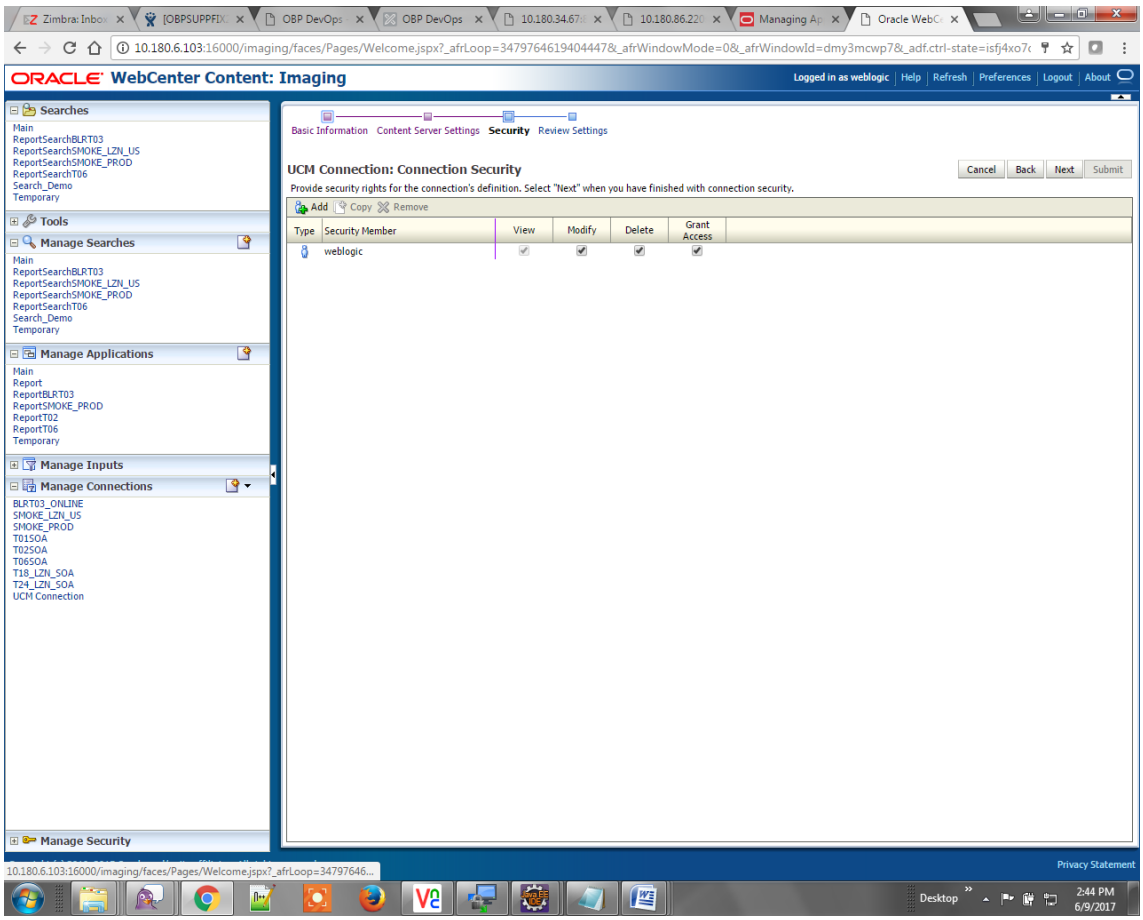
5. In the Content Server Settings page, select the Use Local Content Server check box and select the Server Port as 4444. Click Next.

Figure 7–5 UCM: Connection Settings



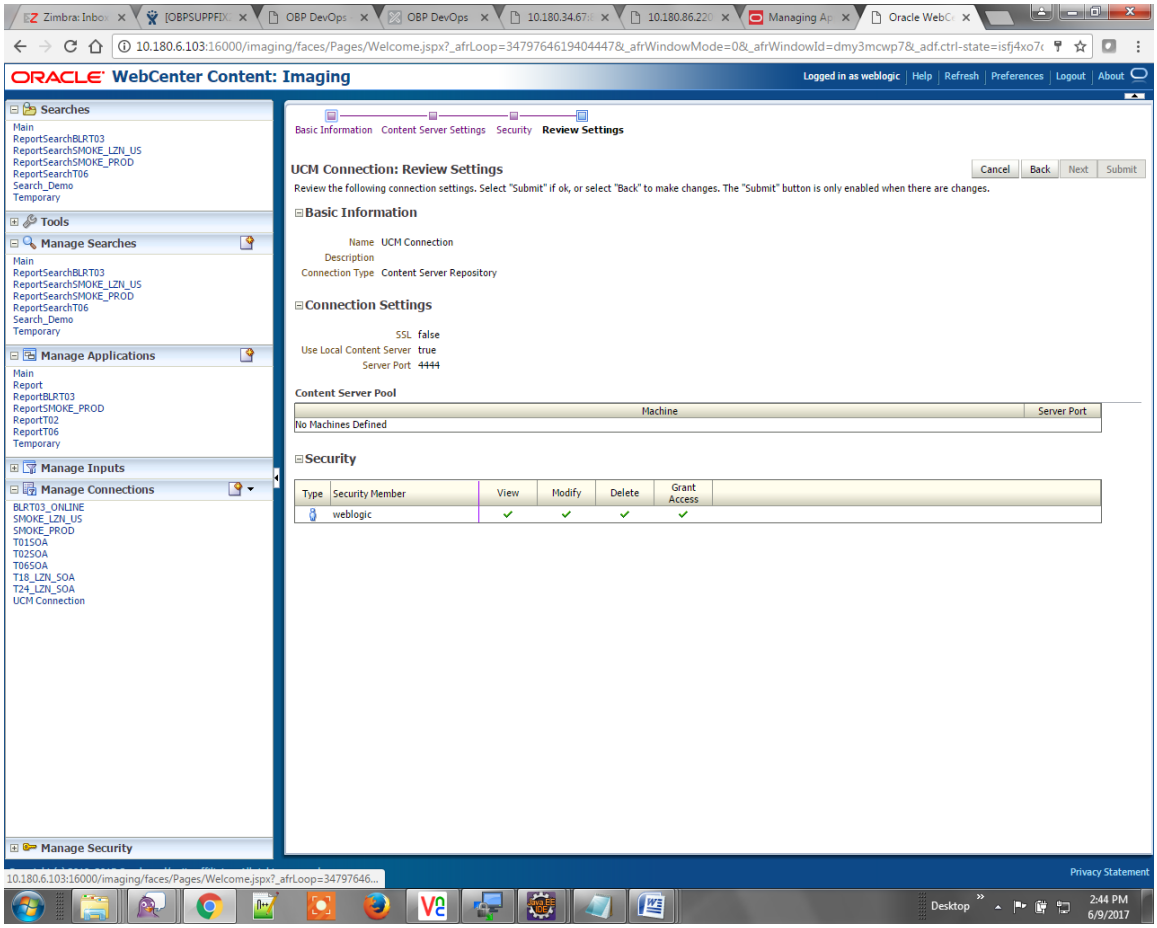
6. In the Security stage, select security rights for connection definition as shown below and click Next. If weblogic security member is not present, create it by clicking Add.

Figure 7–6 UCM: Connection Security



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

Figure 7–7 UCM: Review Settings



7.1.2 Main Application Configuration

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

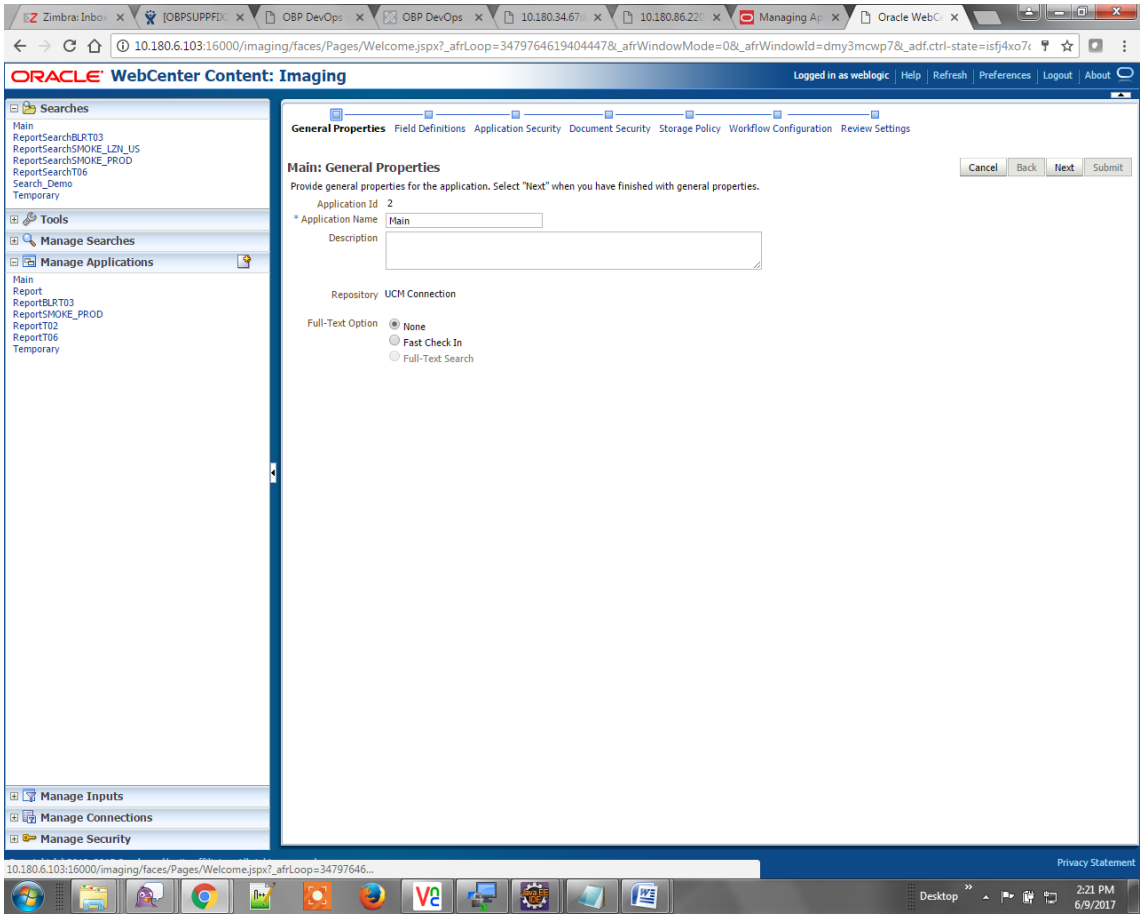
Create a main application and a temporary application in IPM.

7.1.2.1 Manage Application Configuration

To manage application configuration:

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

Figure 7–8 Main: General Properties



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

Figure 7–9 Main: Field Definitions

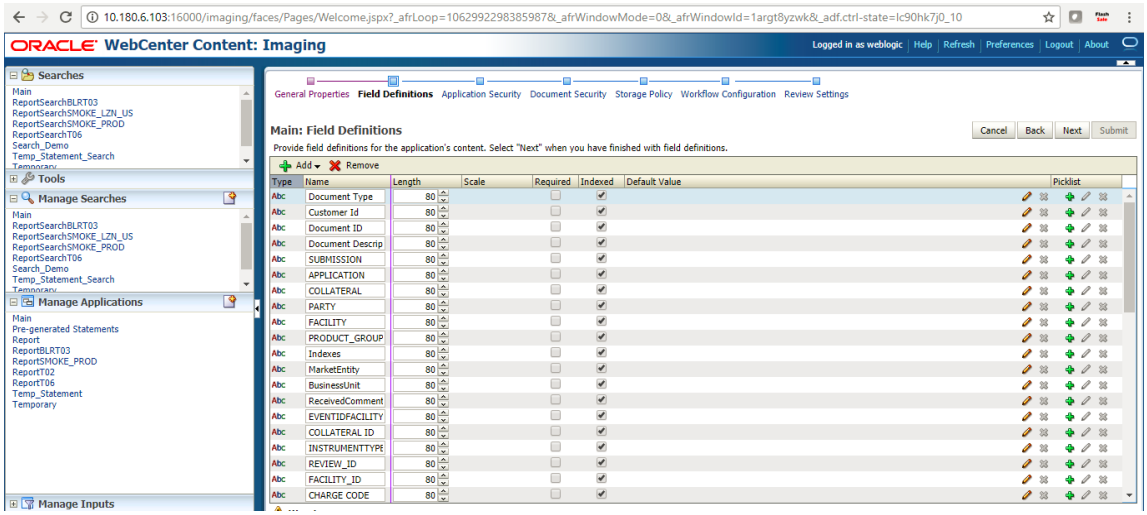
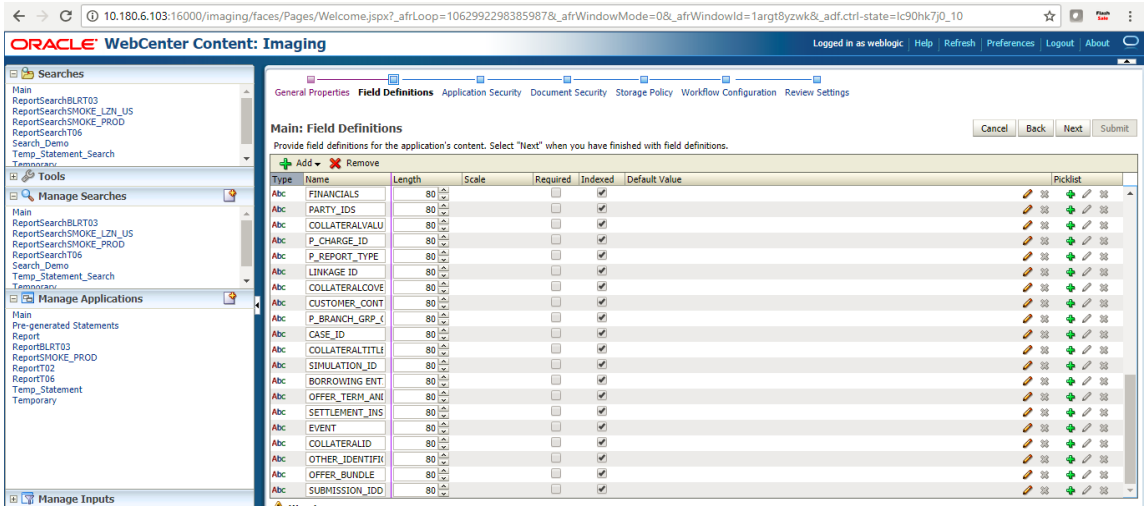


Figure 7–10 Field Definitions (cont.)



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

Figure 7–11 Main: Application Security

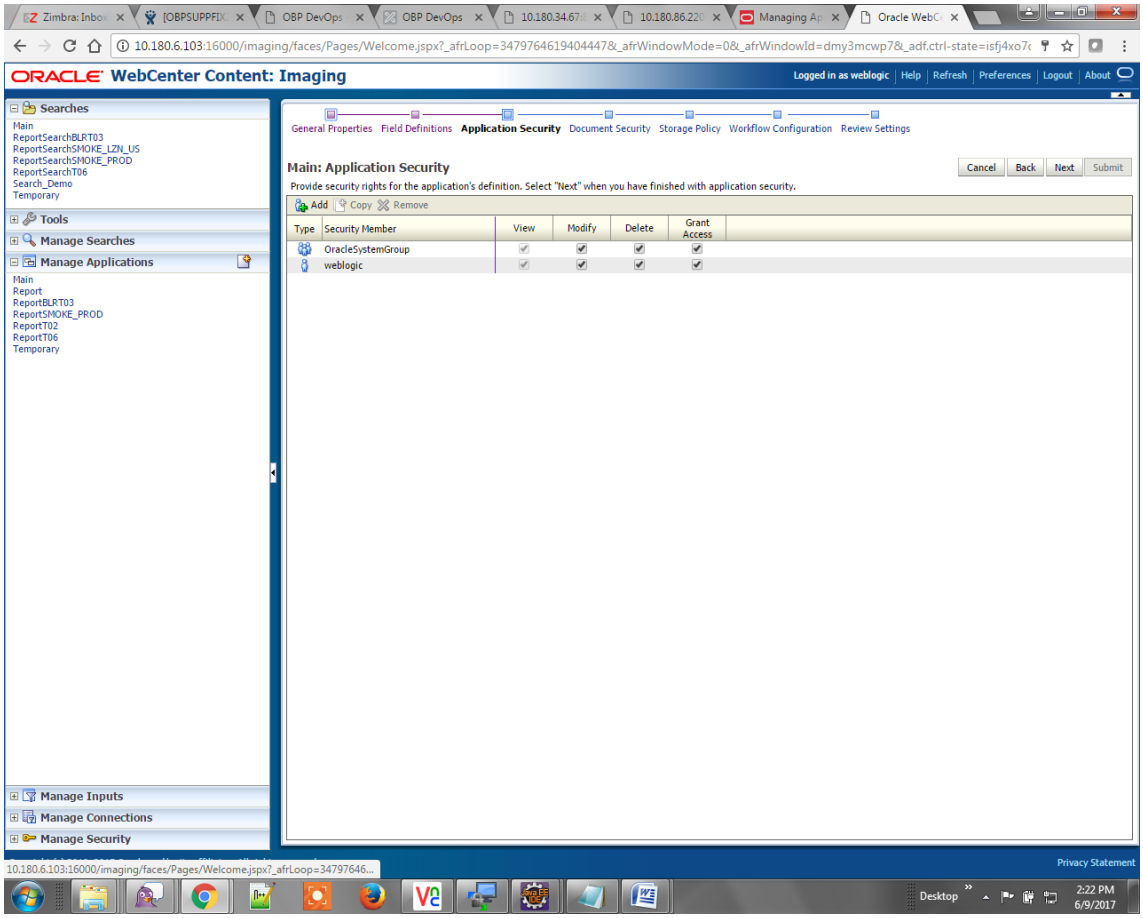
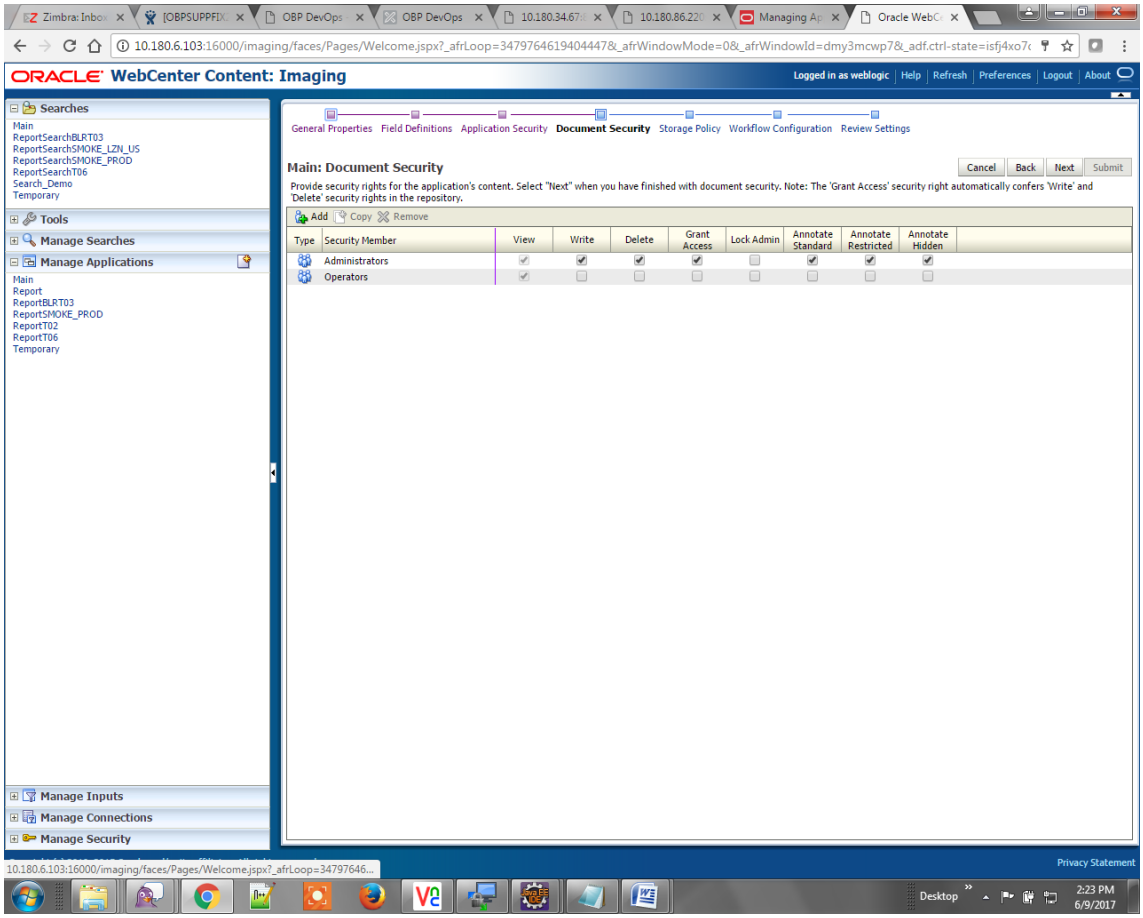
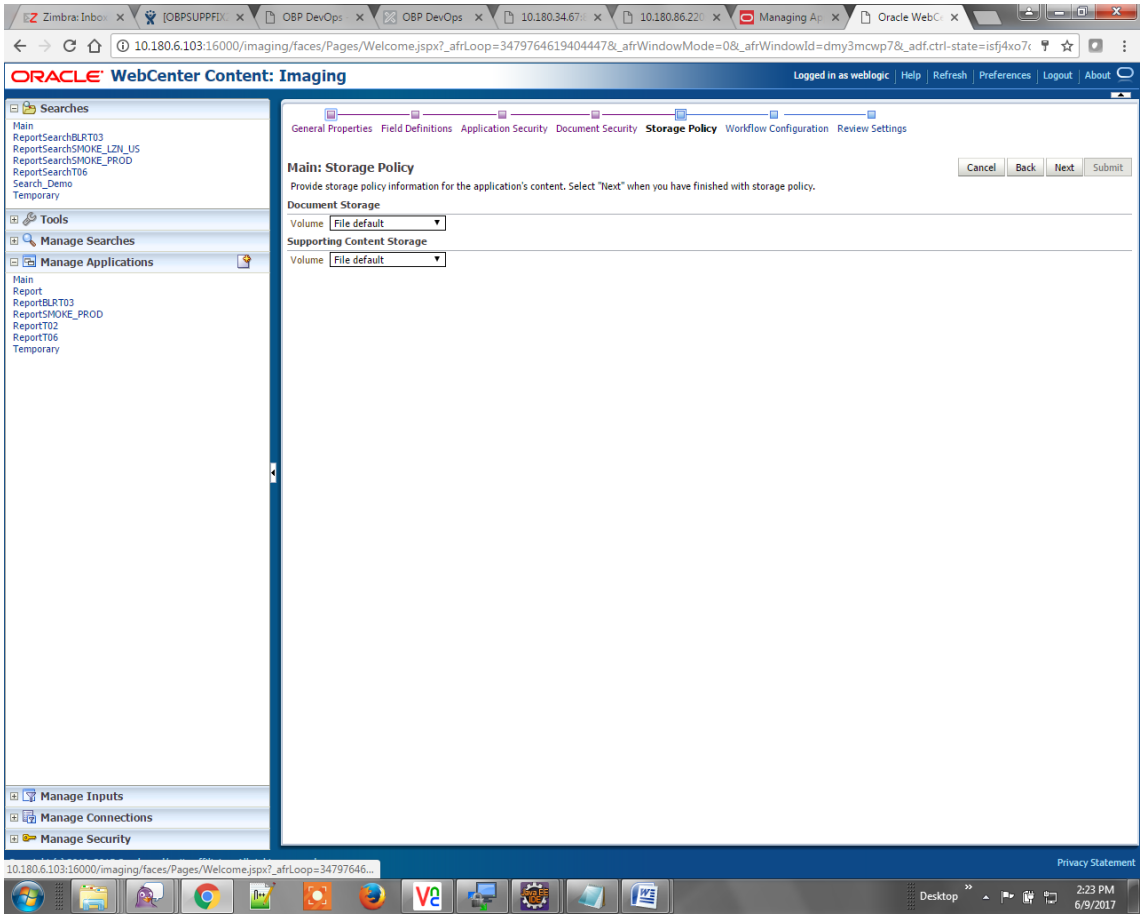


Figure 7–12 Main: Document Security



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

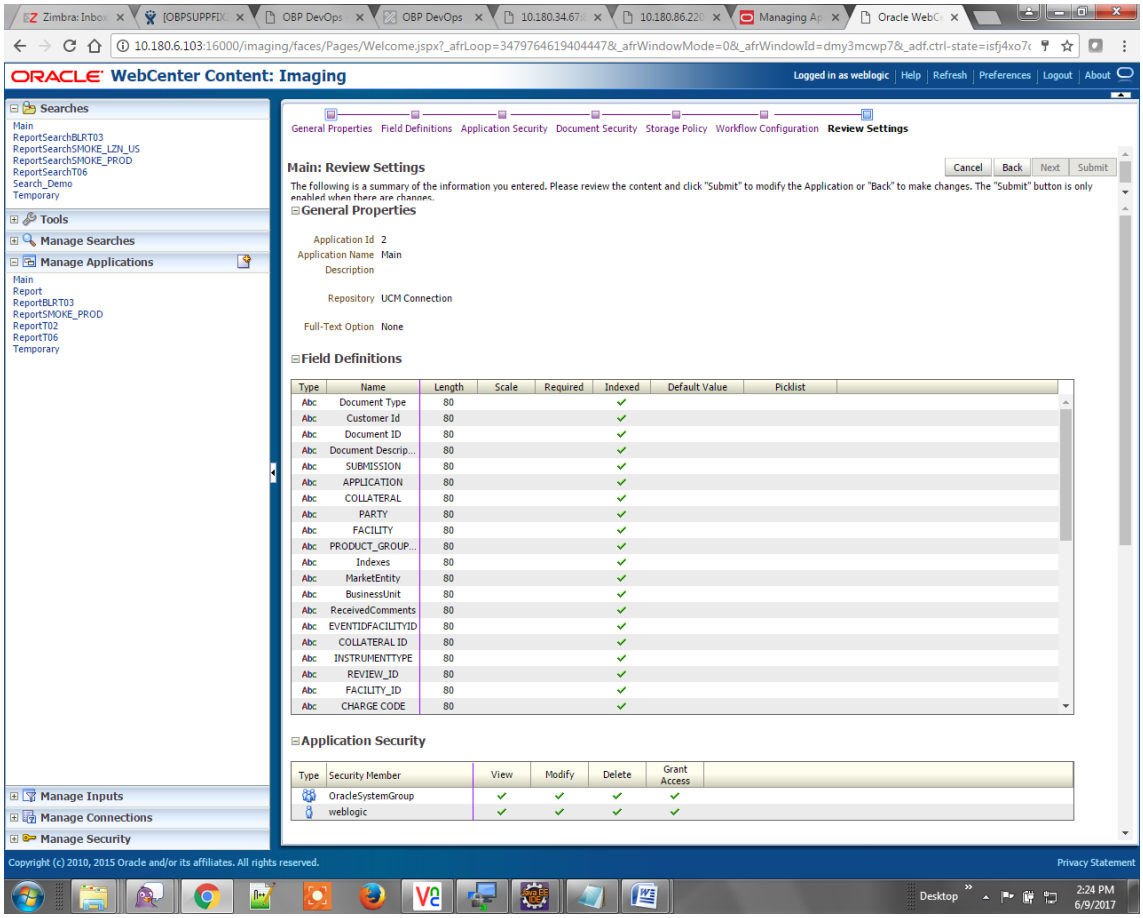
Figure 7–13 Main: Storage Policy



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

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

Figure 7–14 Main: Review Settings

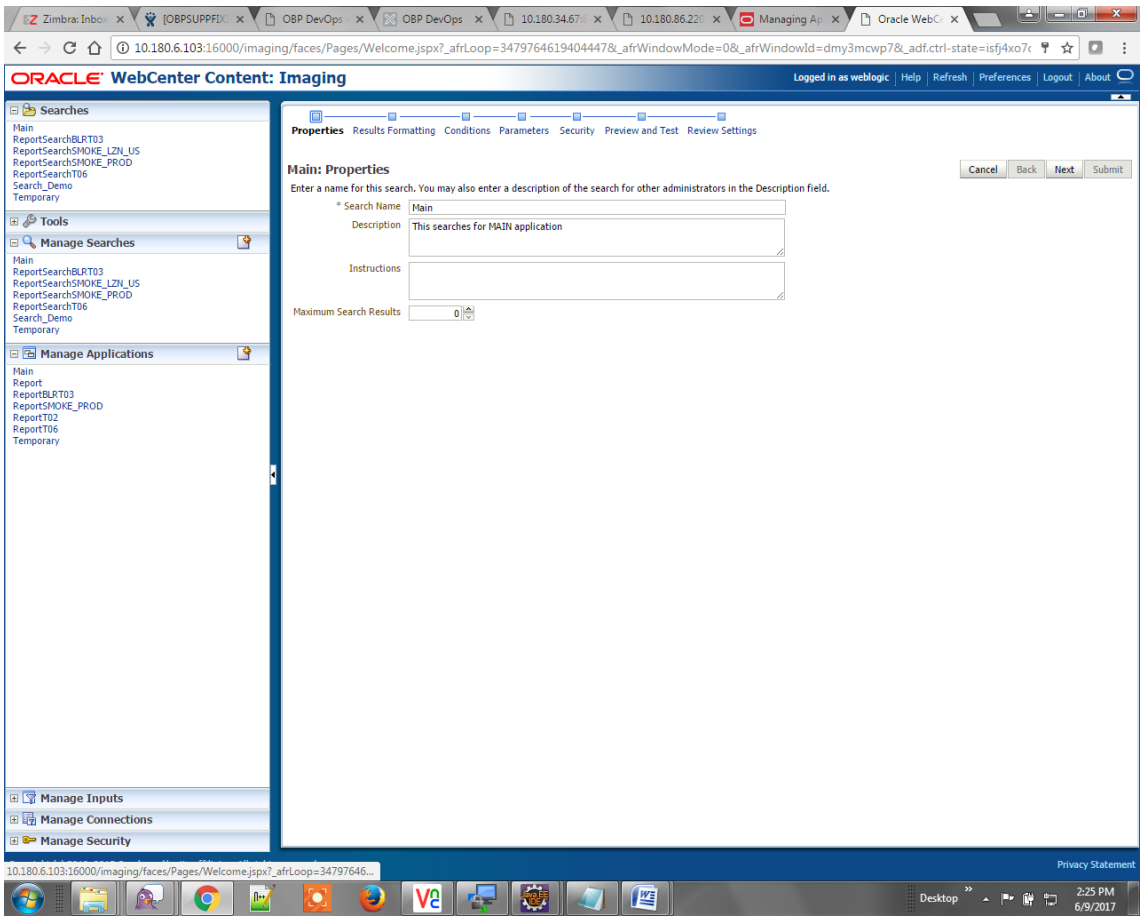


7.1.2.2 Manage Searches

To manage searches:

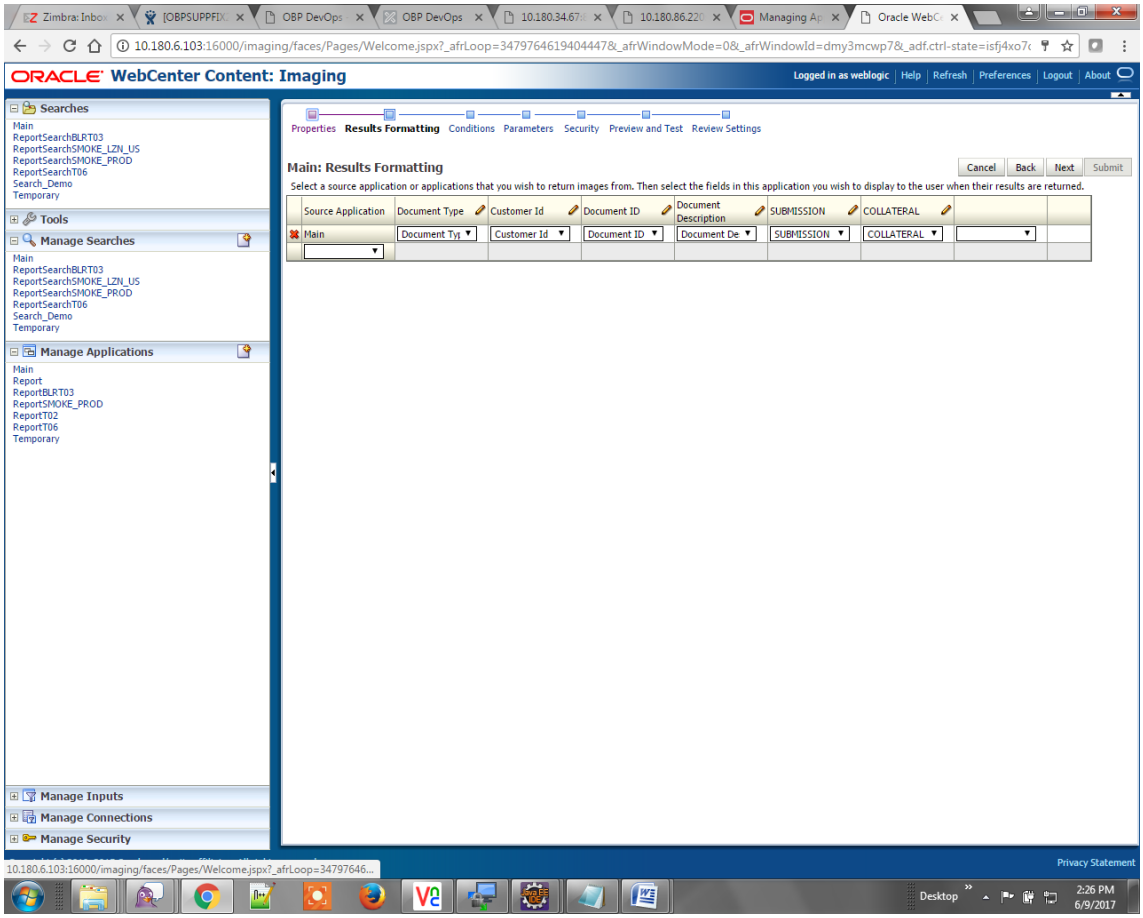
1. Click Manage Searches option and enter the search name with description.

Figure 7–15 Main: Properties



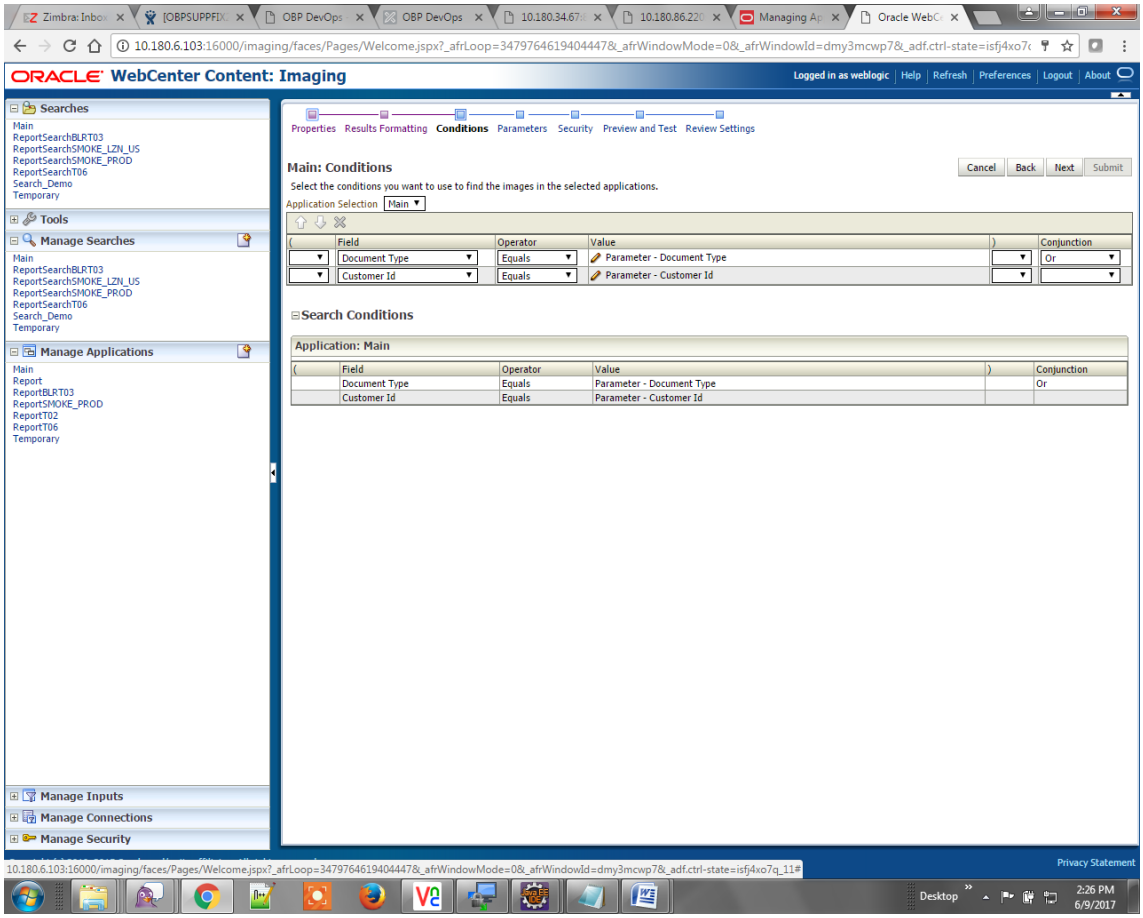
2. Click **Next.**
3. Select the source application along with its field details in the Results Formatting page.

Figure 7–16 Main: Results Formatting



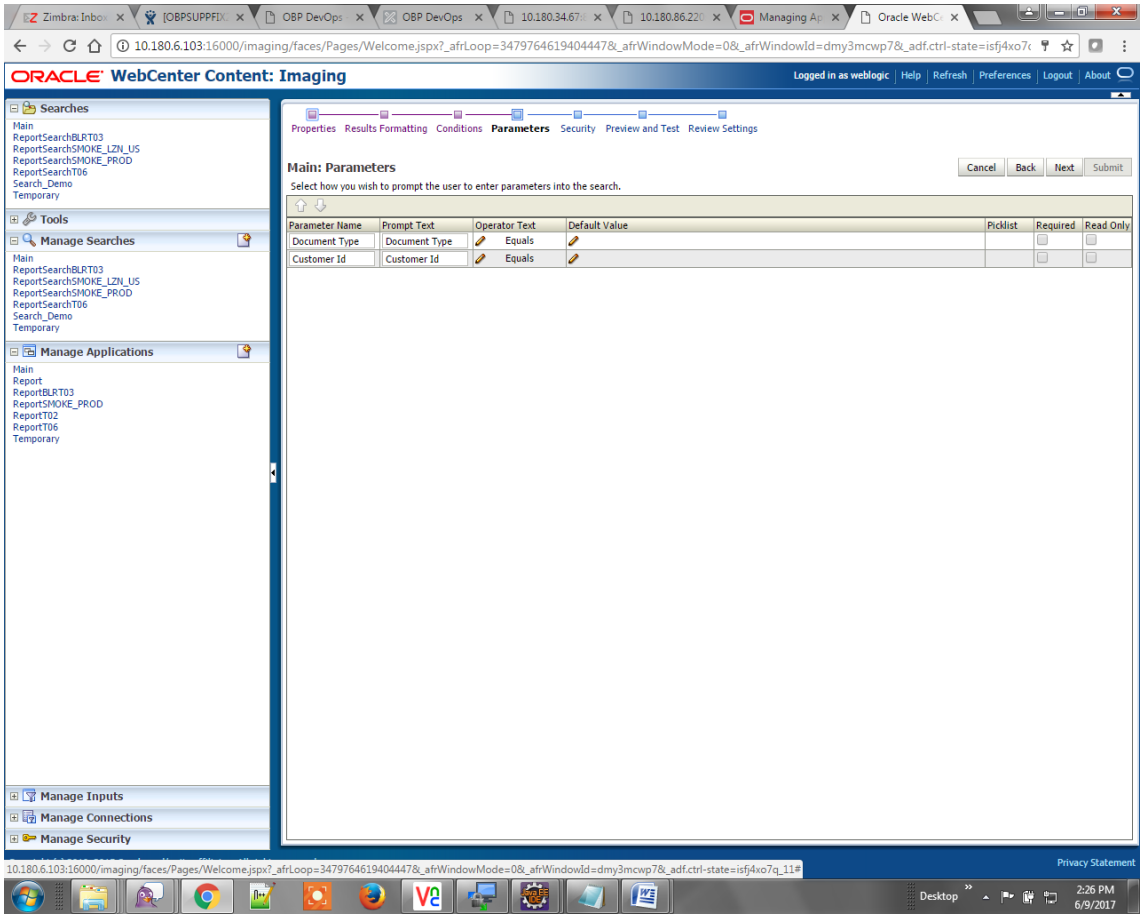
4. Select the appropriate conditions in the Conditions page as shown below.

Figure 7–17 Main: Conditions



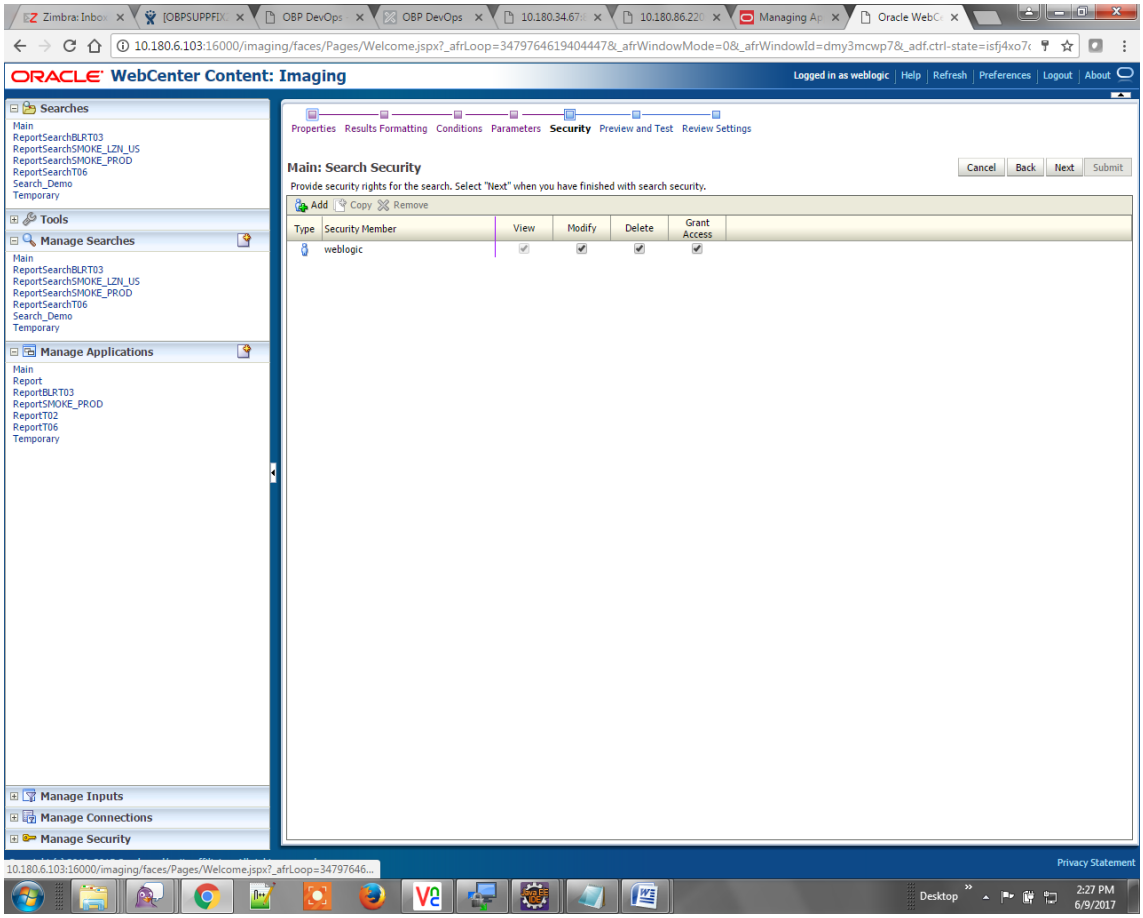
5. Select the appropriate settings in the Parameters page as shown below.

Figure 7–18 Main: Parameters



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

Figure 7–19 Main: Search Security



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

Figure 7–20 Main: Preview and Test

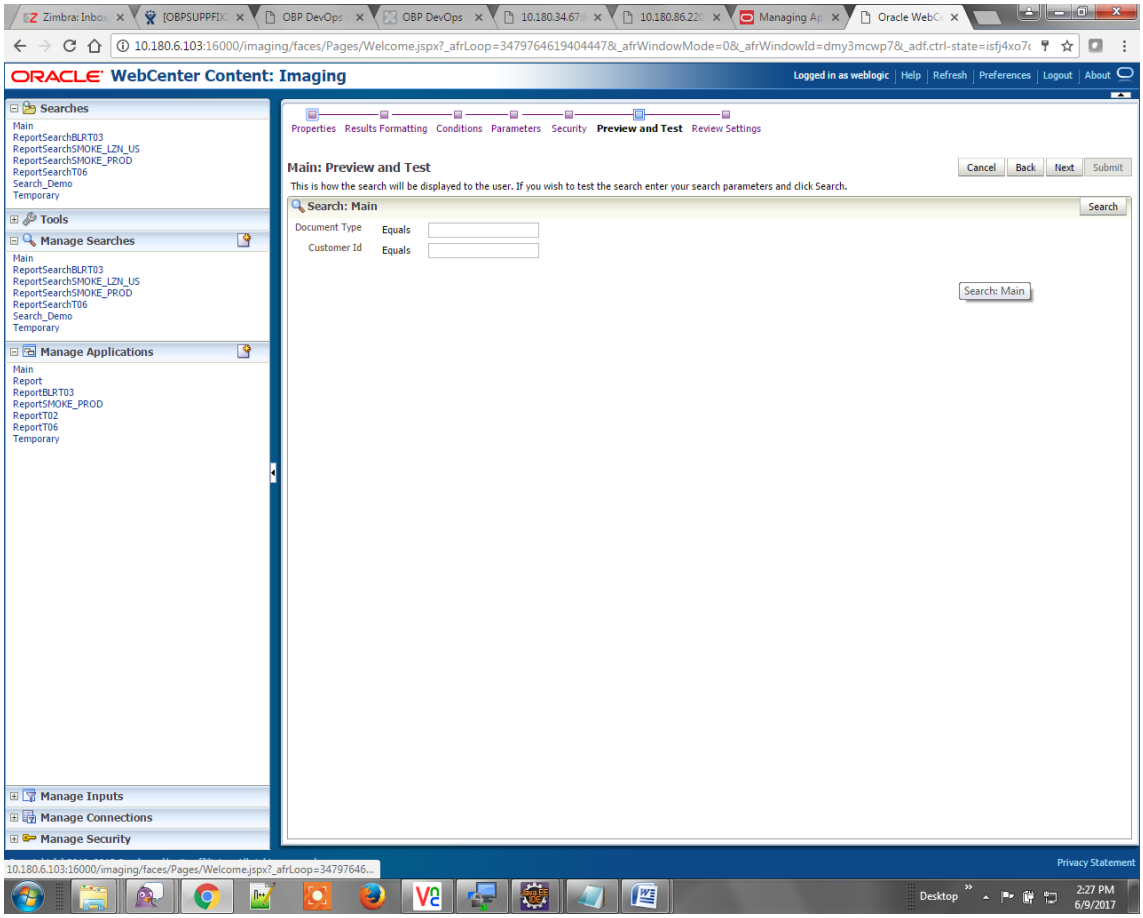
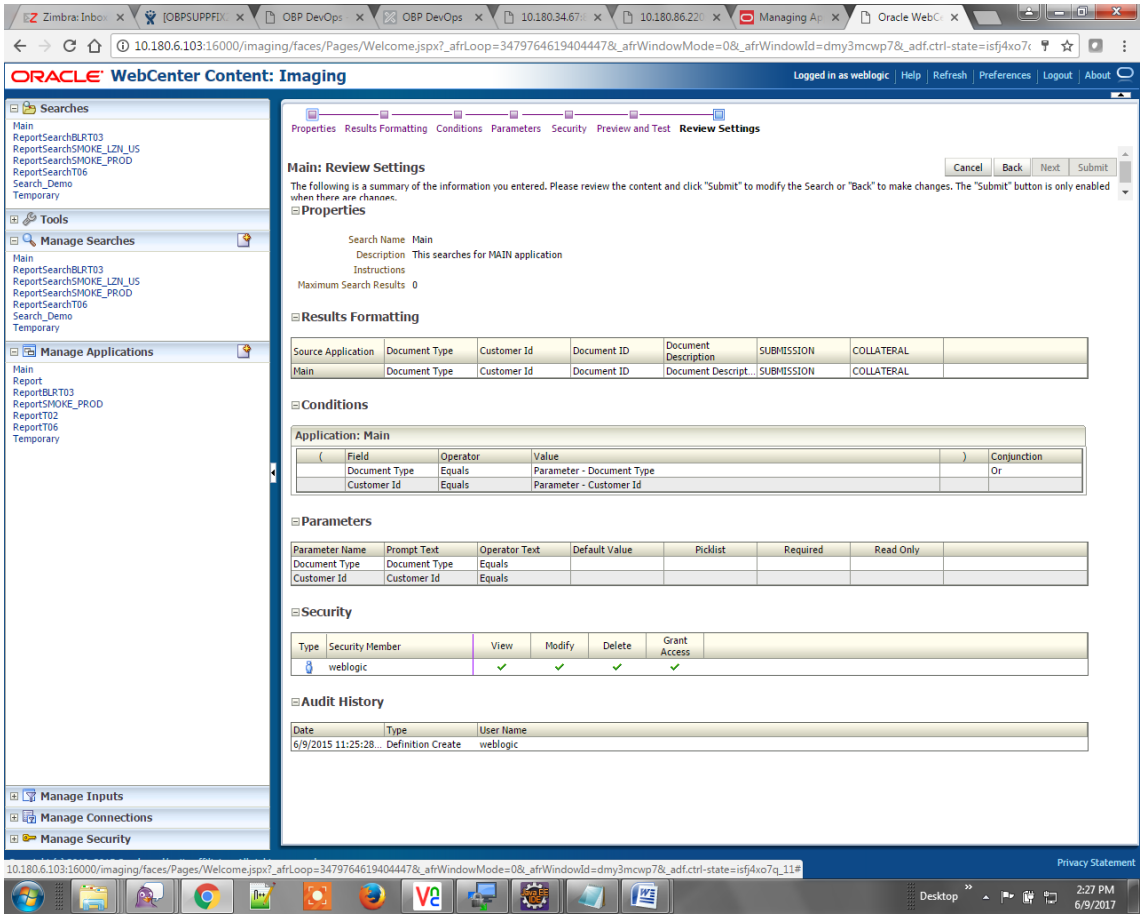


Figure 7–21 Main: Review Settings



7.1.3 Temp Application Configuration

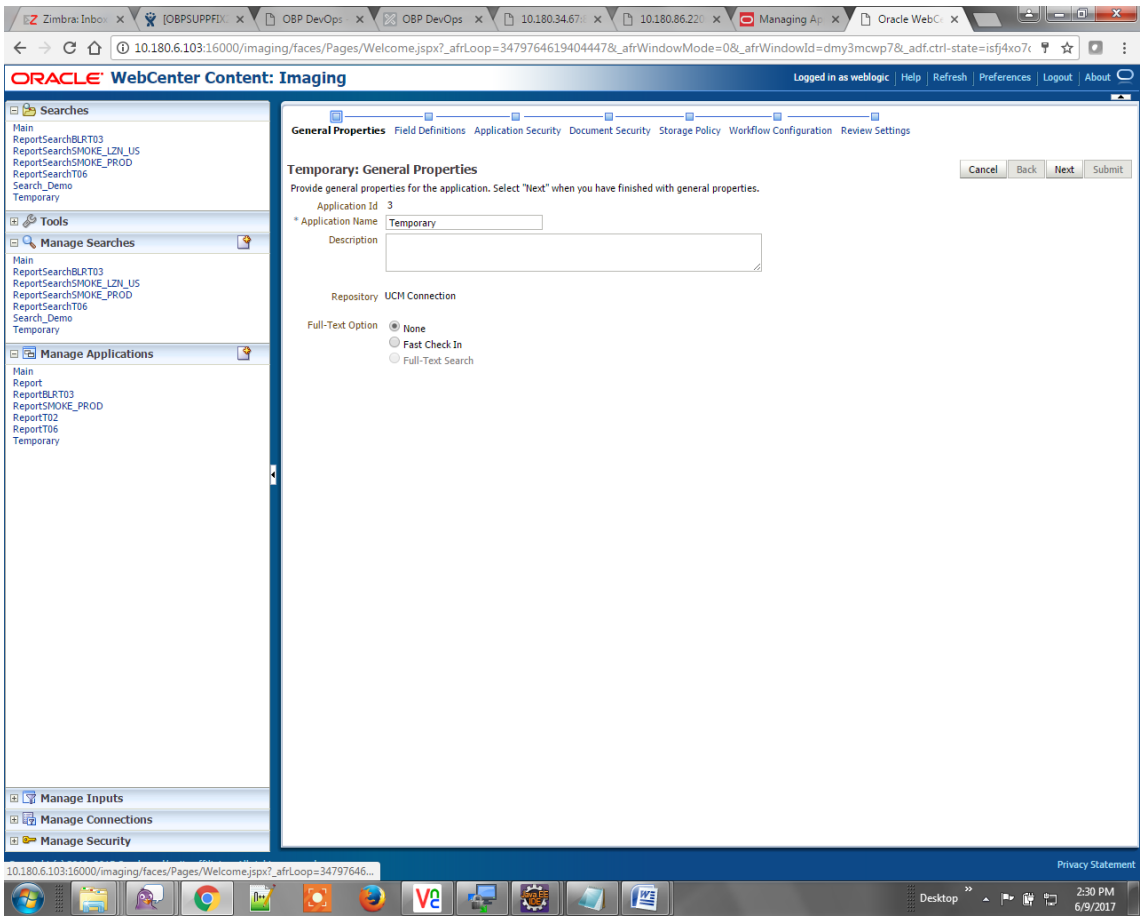
This section provides details about the temp application configuration.

7.1.3.1 Manage Application Configuration

To manage application configuration:

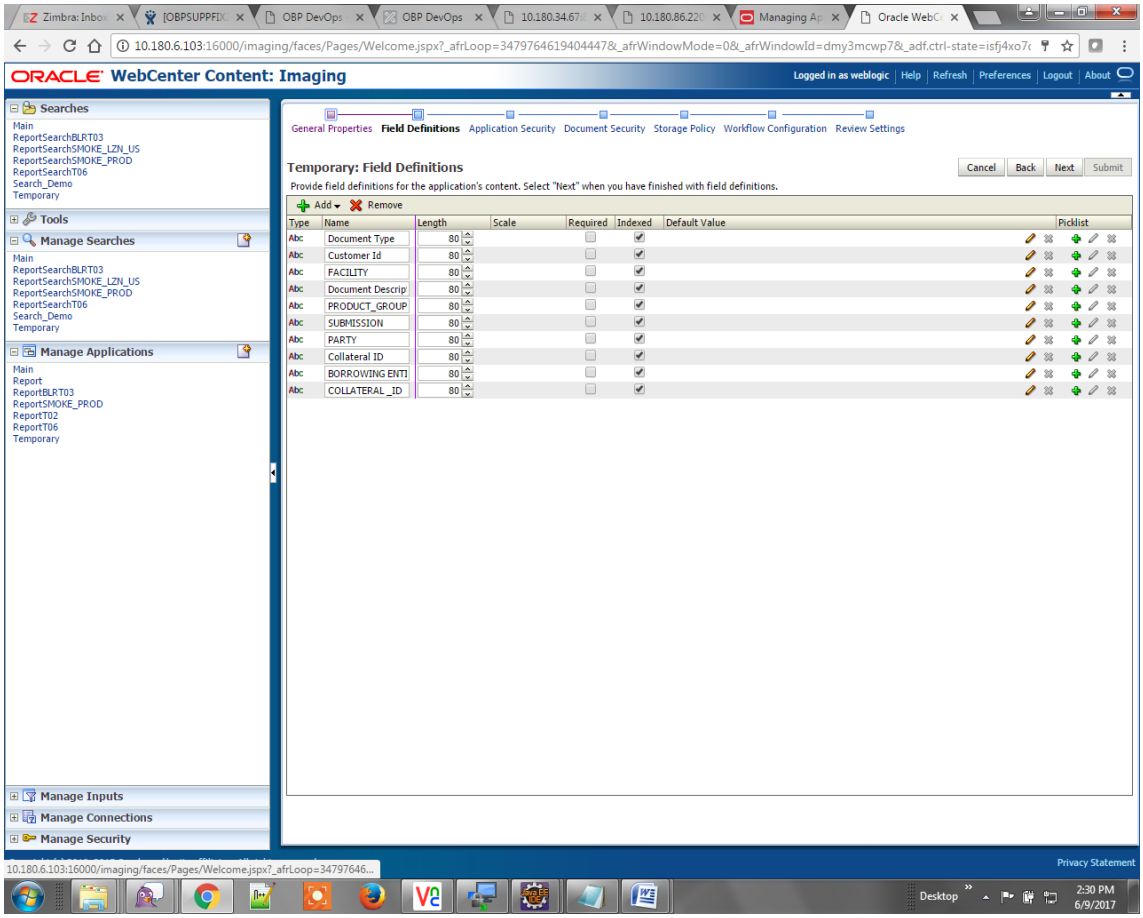
1. Select the Create New Application option.
2. Enter the general properties and click **Next.**

Figure 7–22 Temporary: General Properties



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

Figure 7–23 Temporary: Field Definitions



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

Figure 7–24 Temporary: Application Security

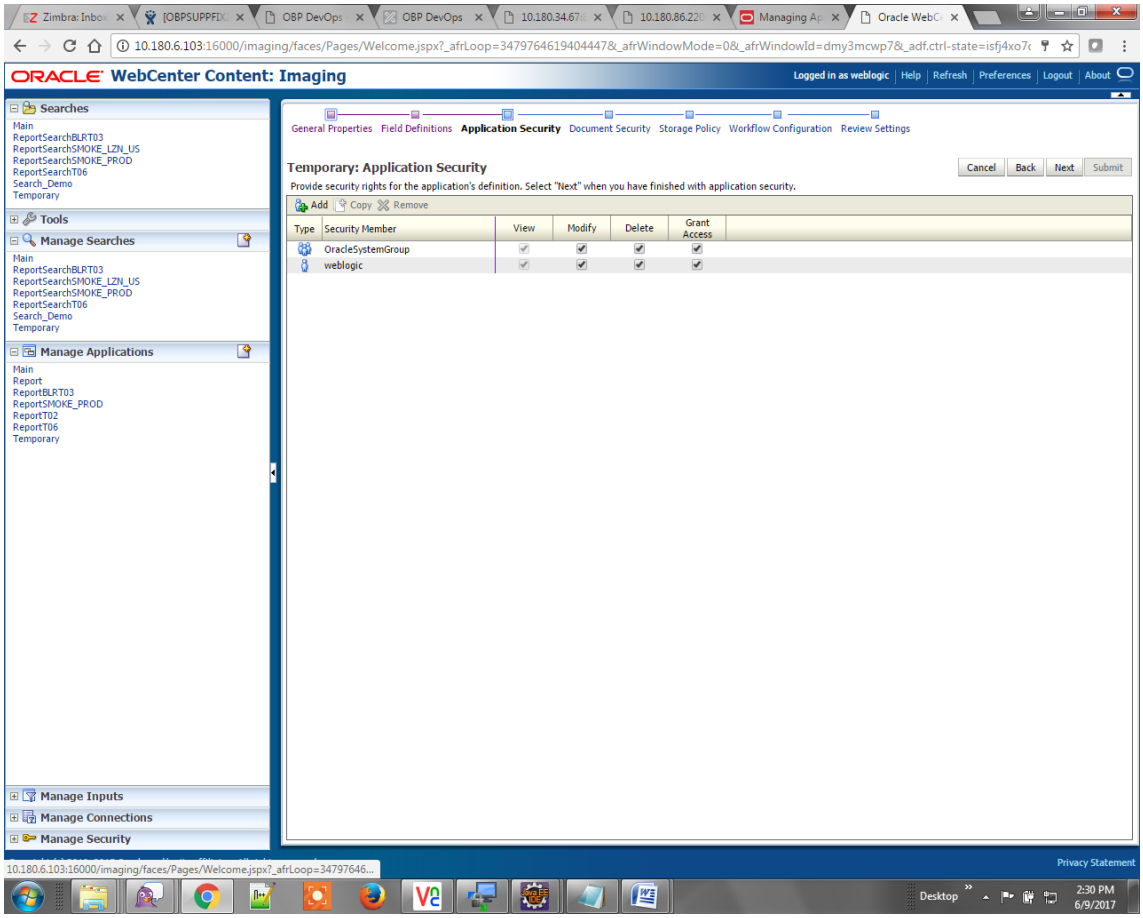
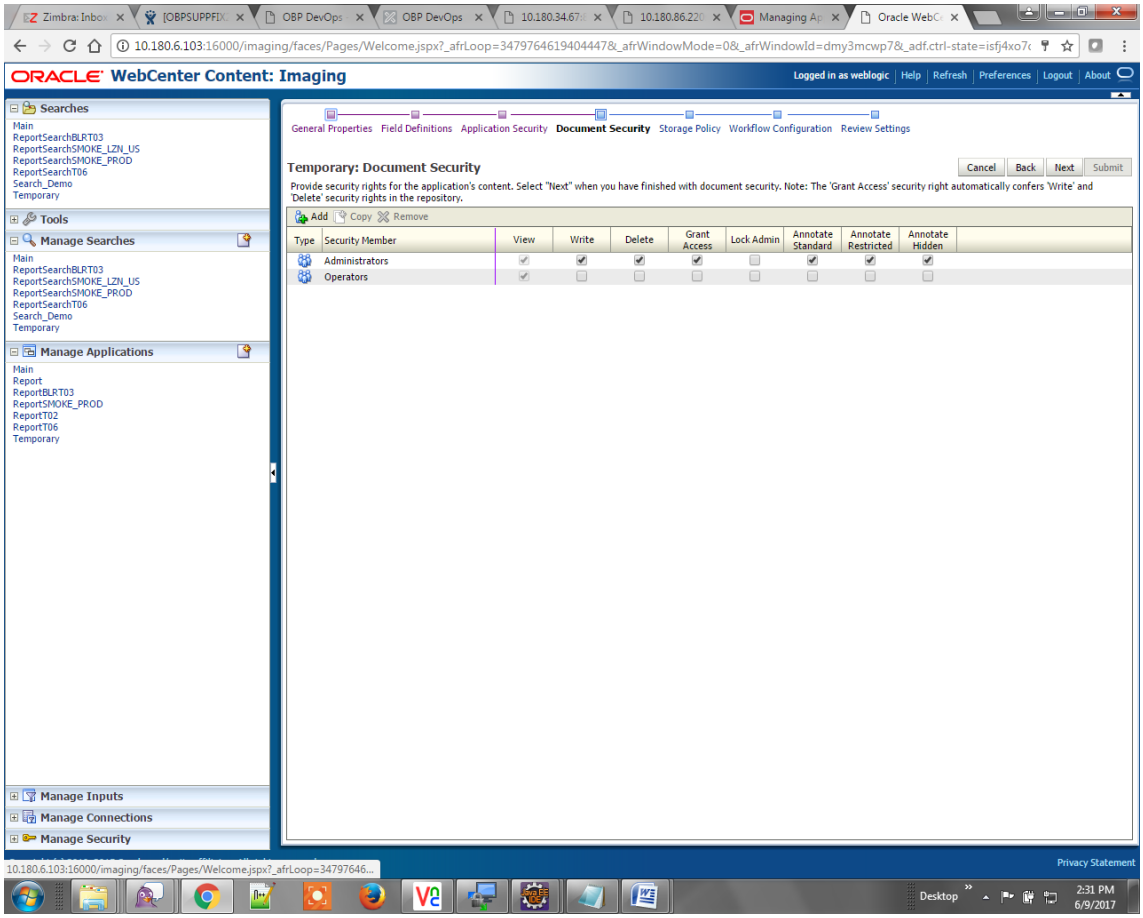
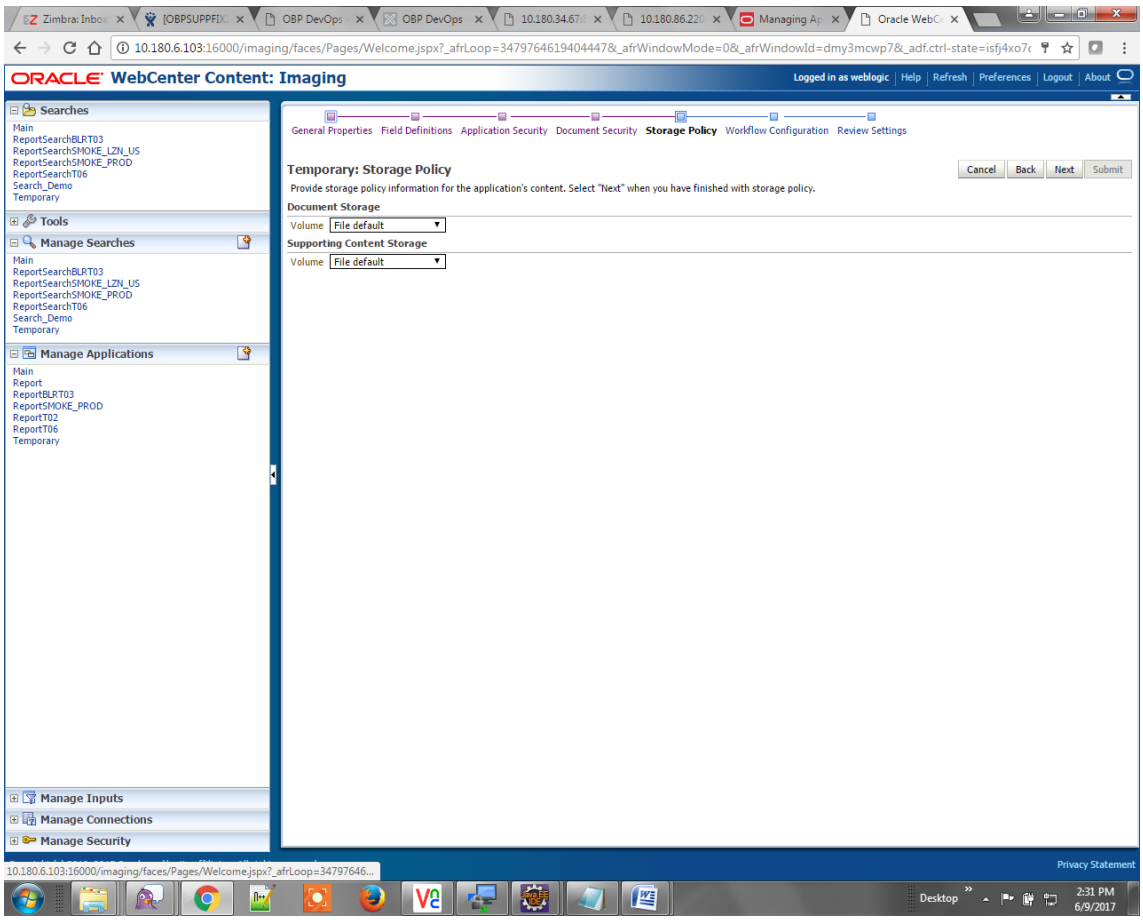


Figure 7–25 Temporary: Document Security



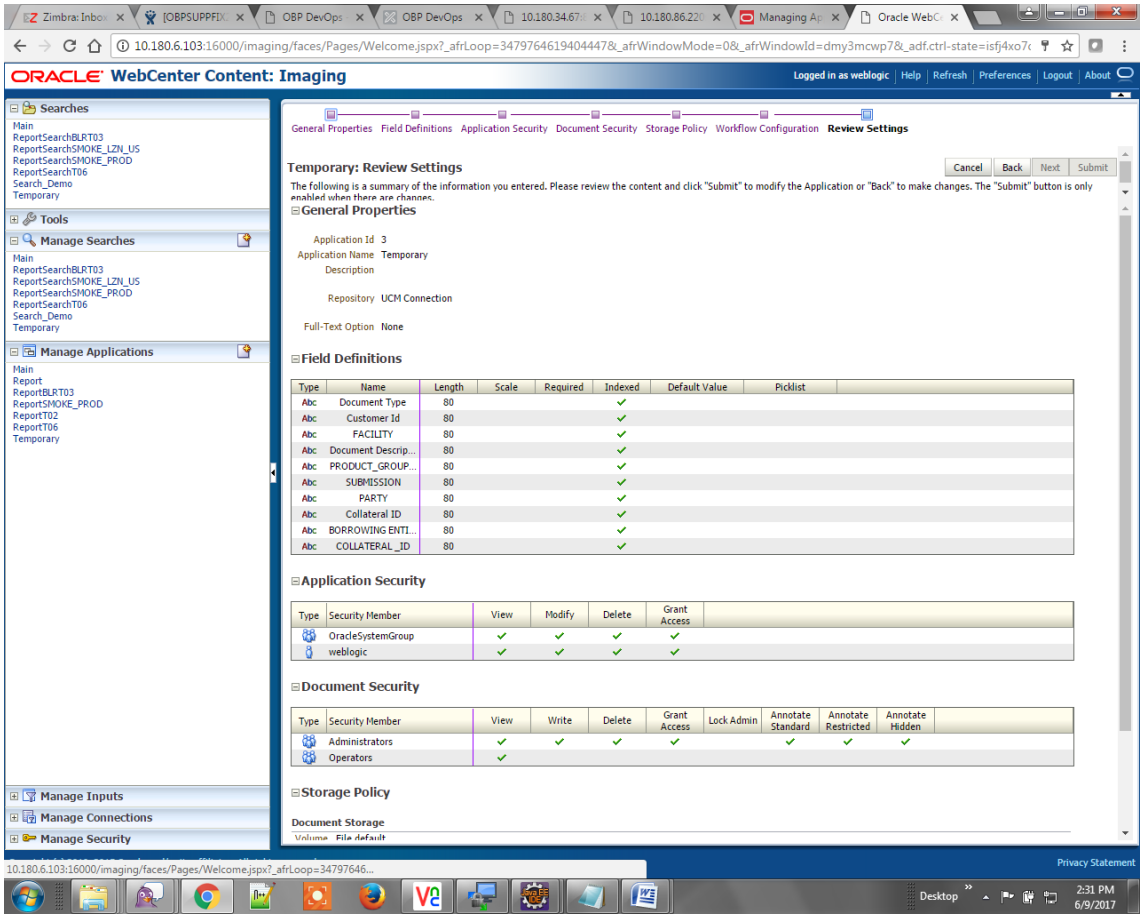
5. In the Storage Policy page, select the file default option has shown below.

Figure 7–26 Temporary: Storage Policy



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

Figure 7–27 Temporary: Review Settings

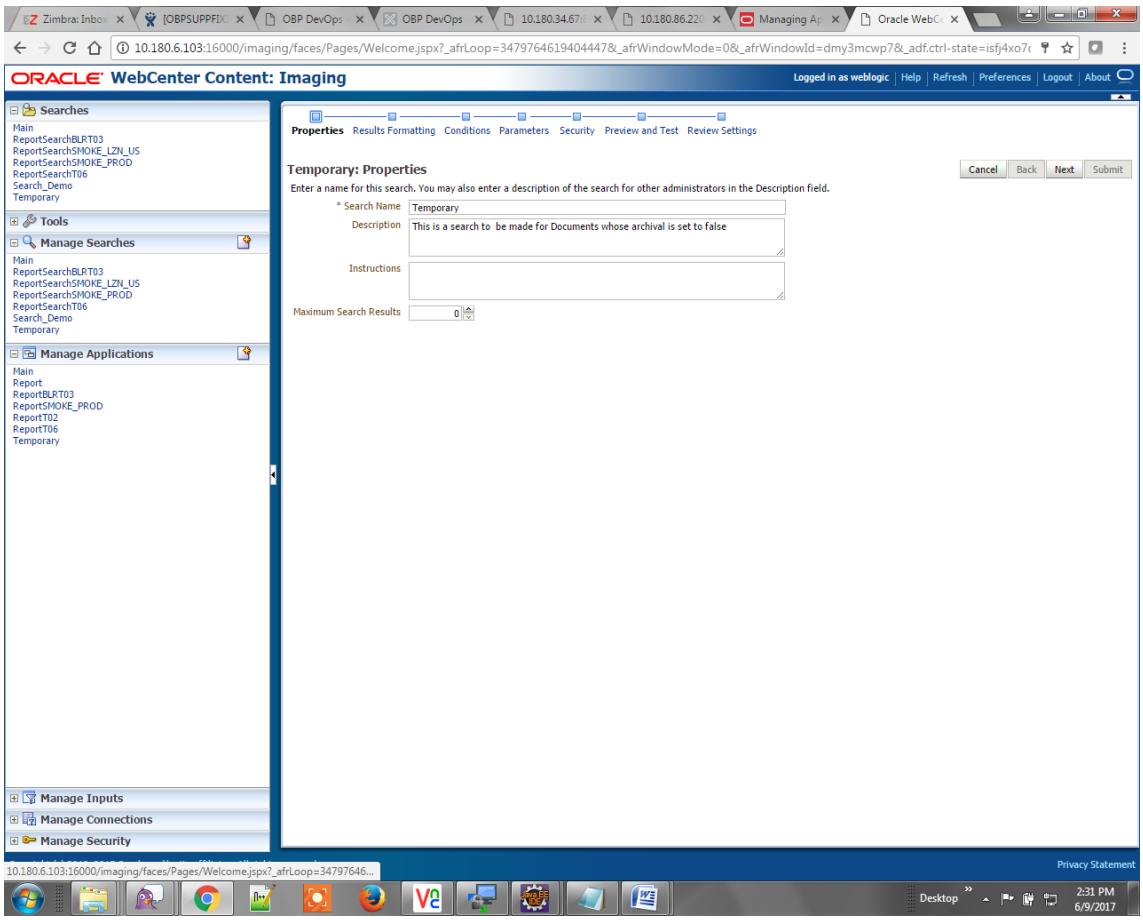


7.1.3.2 Manage Searches

To manage searches:

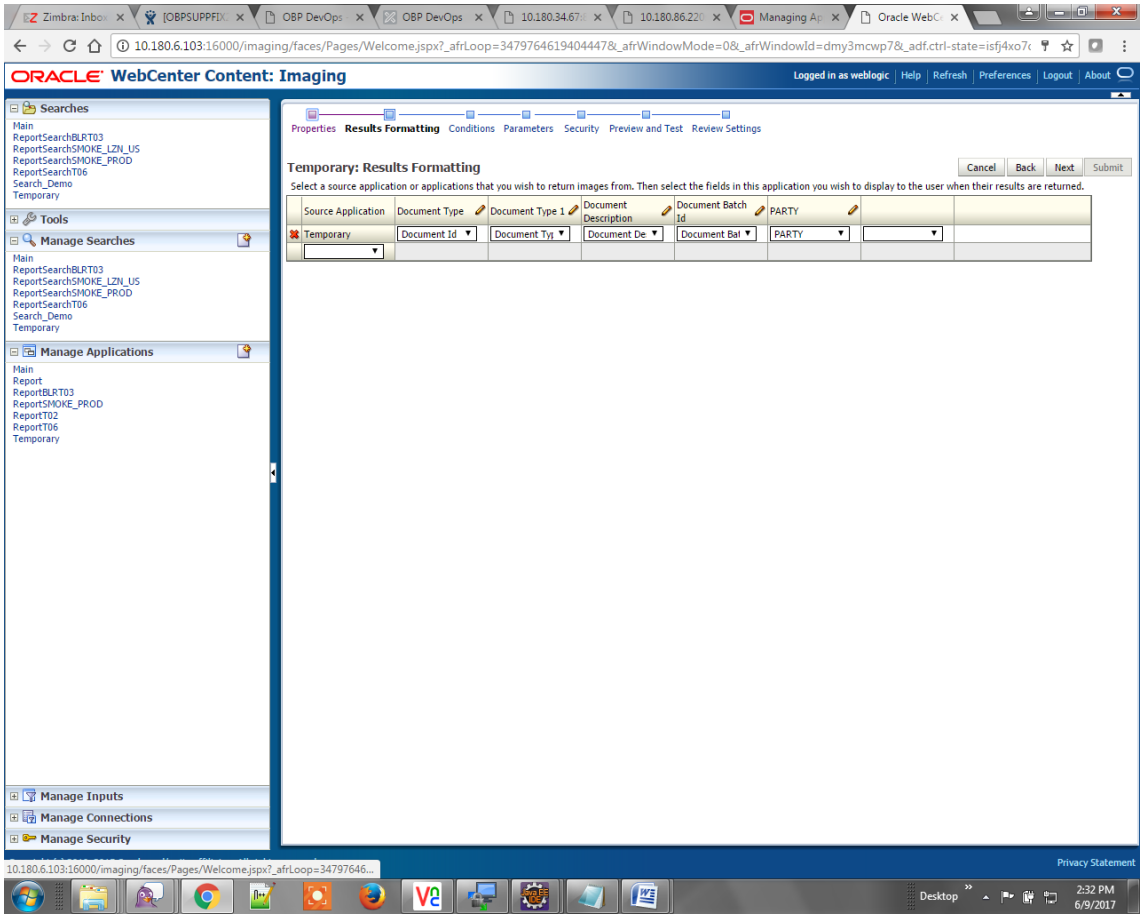
1. Click the Manage Searches option and enter the search name with description.

Figure 7–28 Temporary: Properties



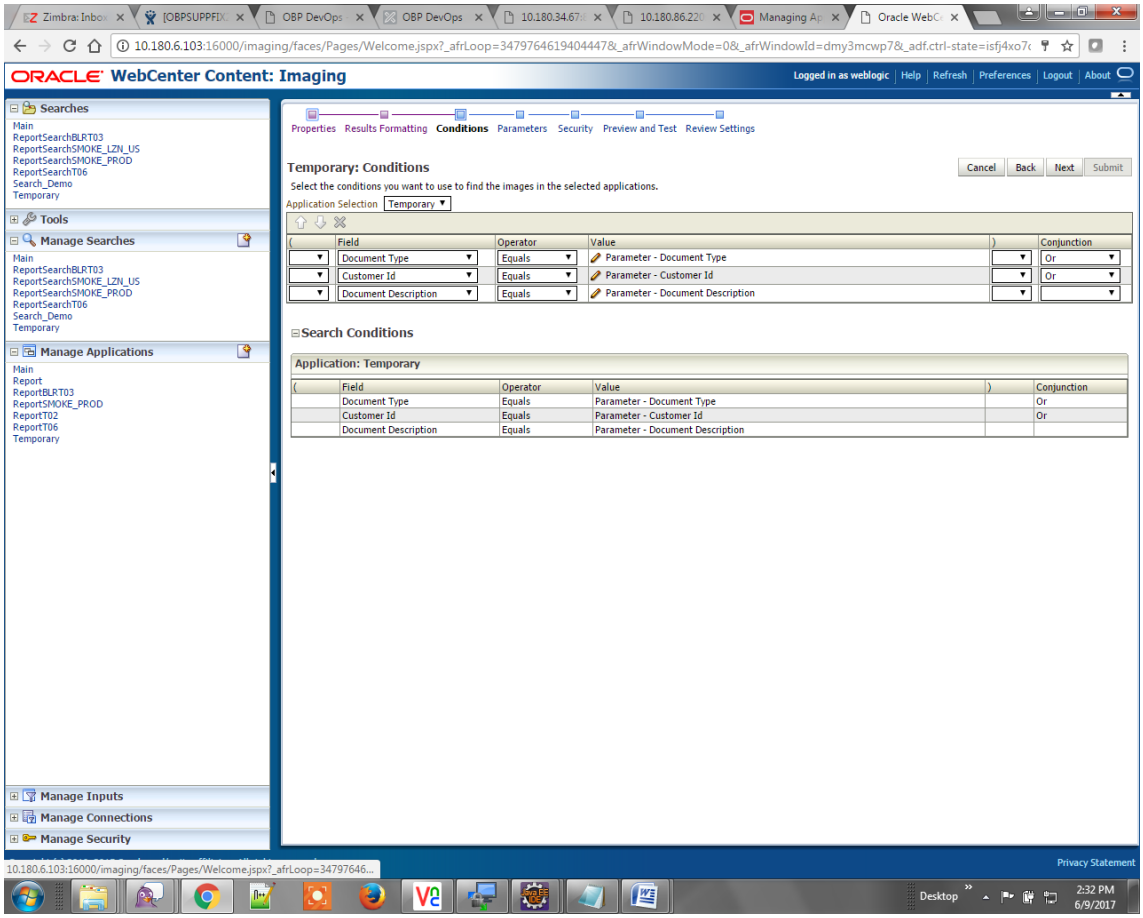
2. Select the source application along with its field details in the Results Formatting page.

Figure 7–29 Temporary: Results Formatting



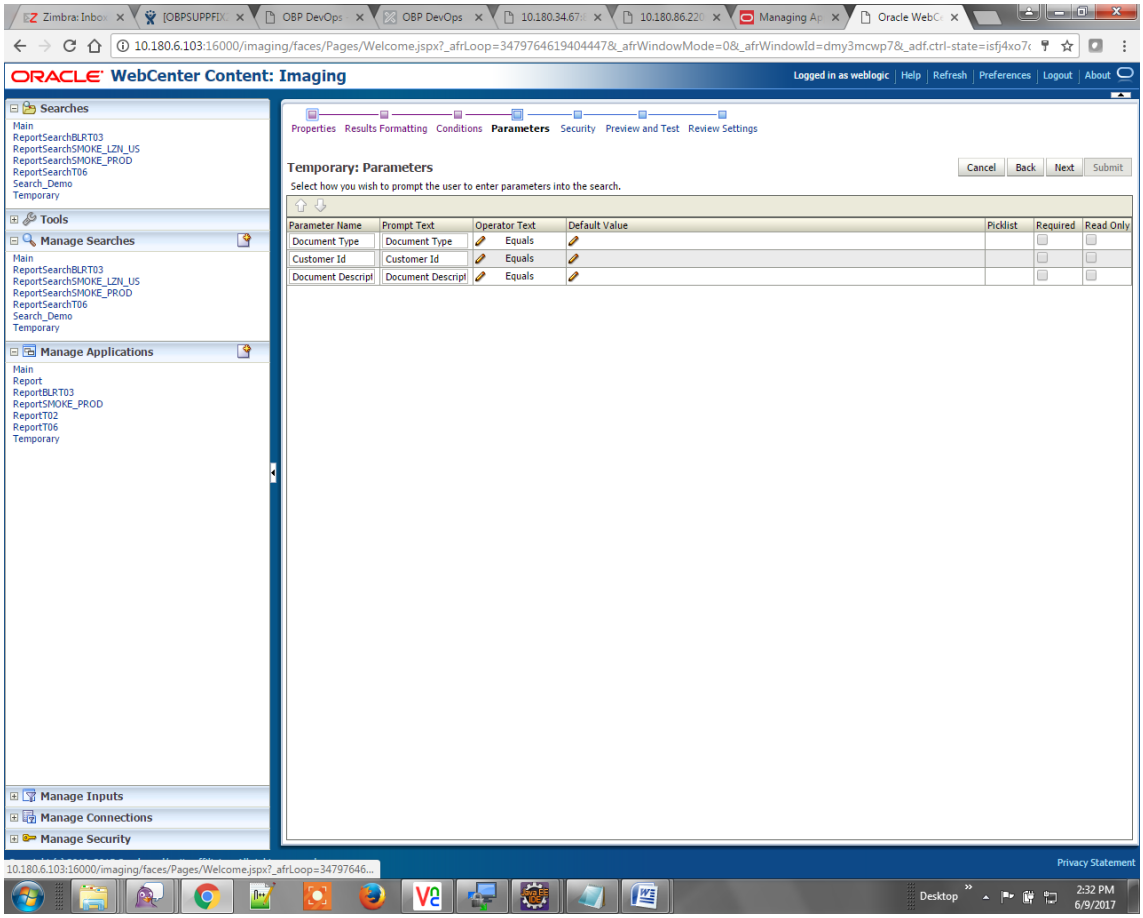
3. Select the appropriate conditions in the Conditions page as shown below.

Figure 7–30 Temporary: Conditions



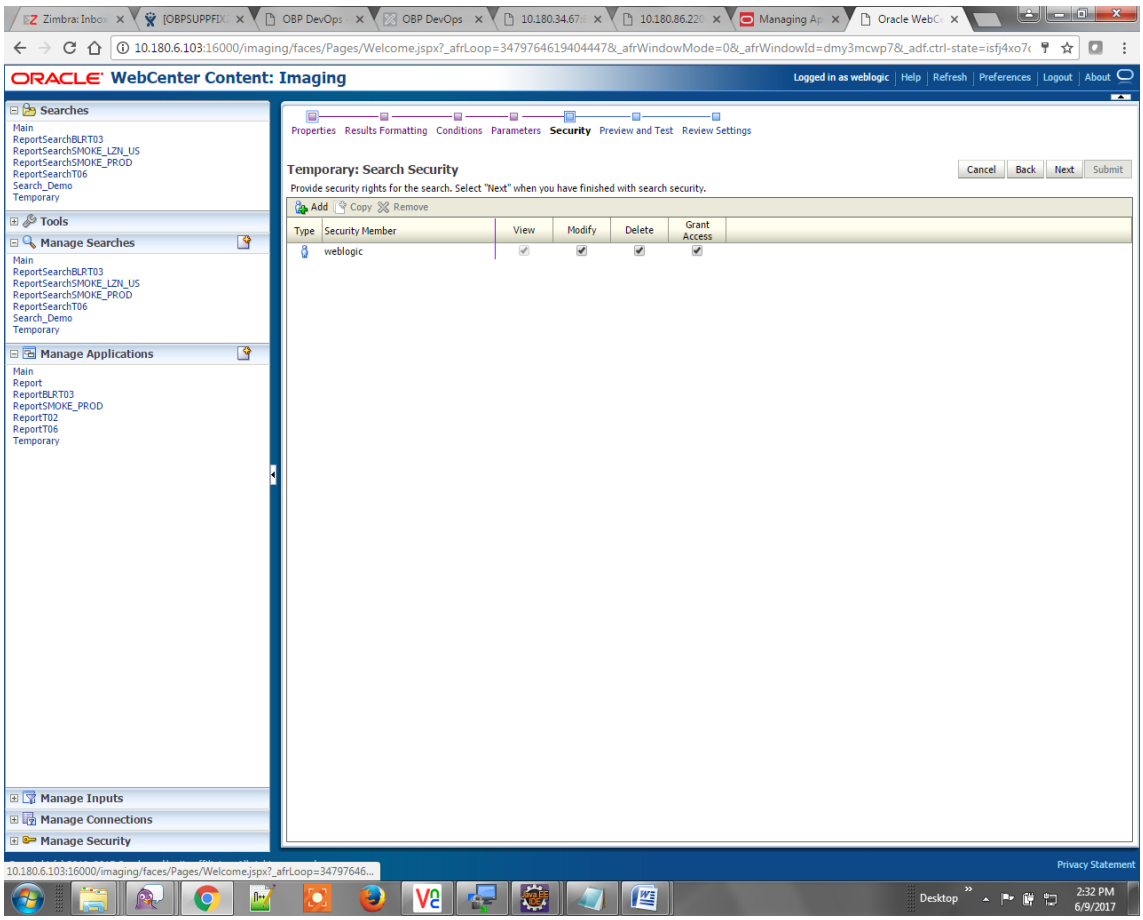
4. Select the appropriate settings in the Parameters page as shown below.

Figure 7–31 Temporary: Parameters



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

Figure 7–32 Temporary: Search Security



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

Figure 7–33 Temporary: Preview and Test

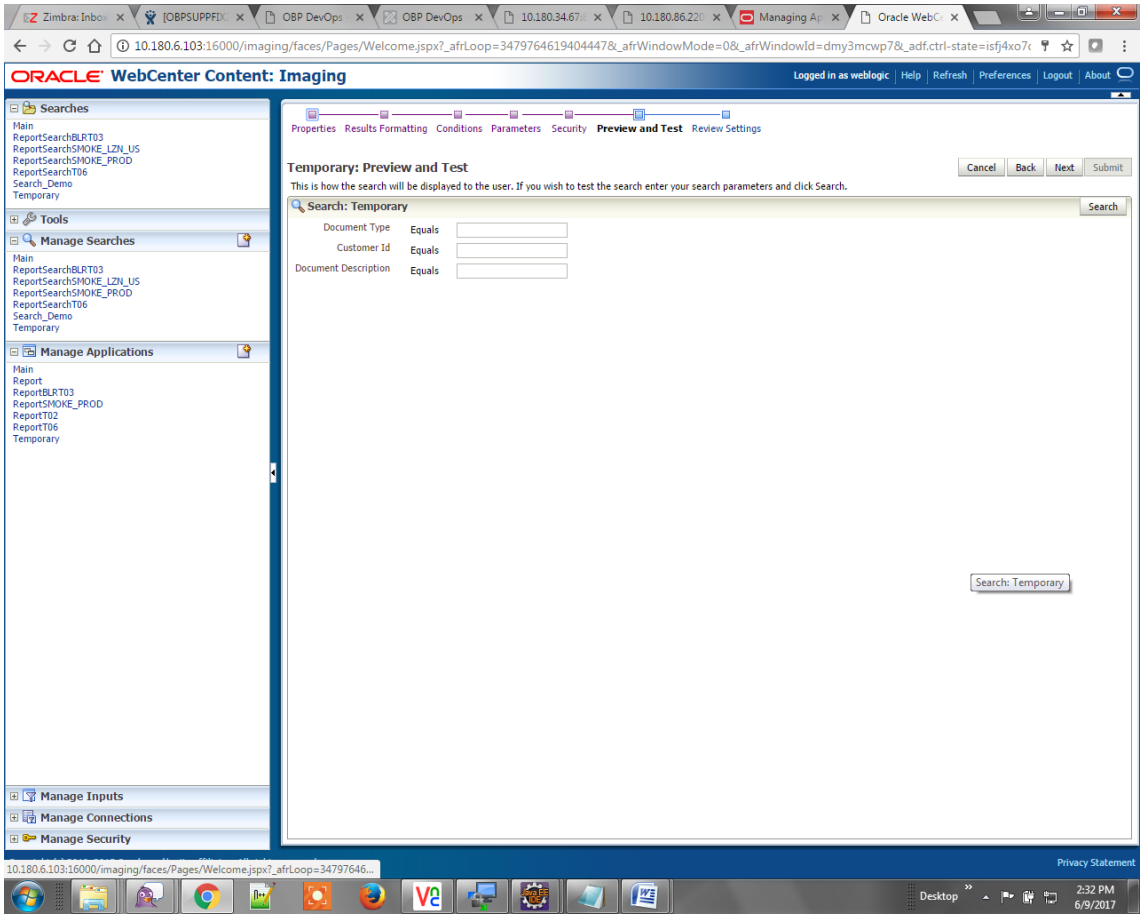
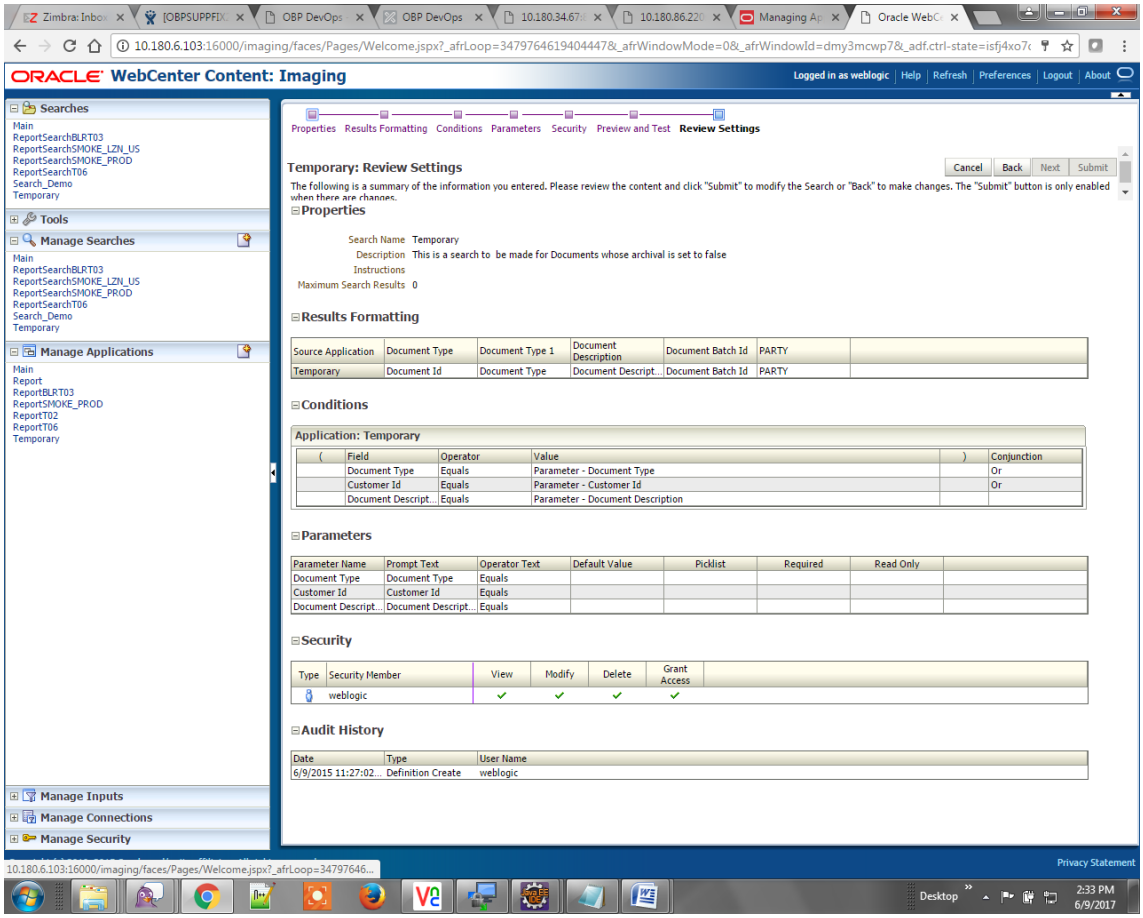


Figure 7–34 Temporary: Review Settings



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

7.2 IPM Configuration for Bulk Upload Process Setup

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

This upload takes place in the following steps:

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

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

7.2.1 Prerequisites

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

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

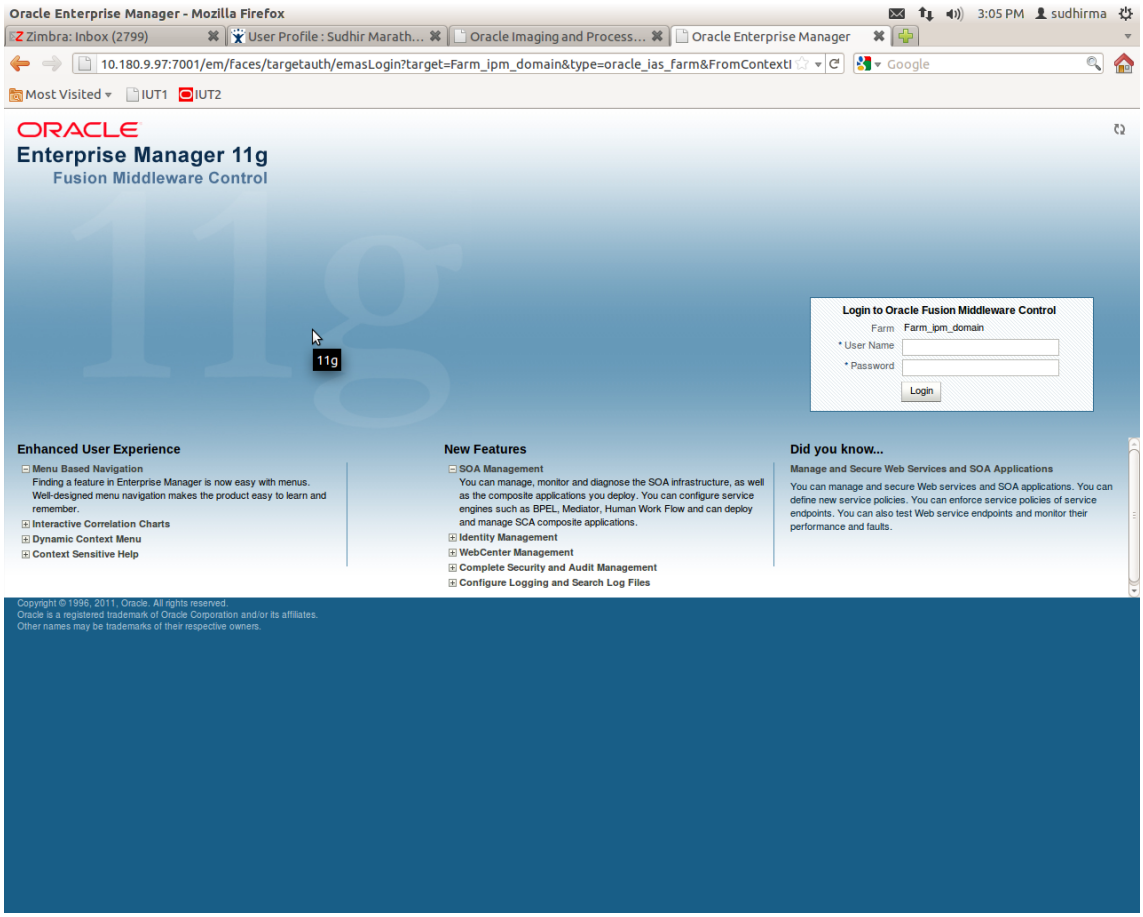
7.2.2 Setting up the Connection Name

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

To set up a bulk process:

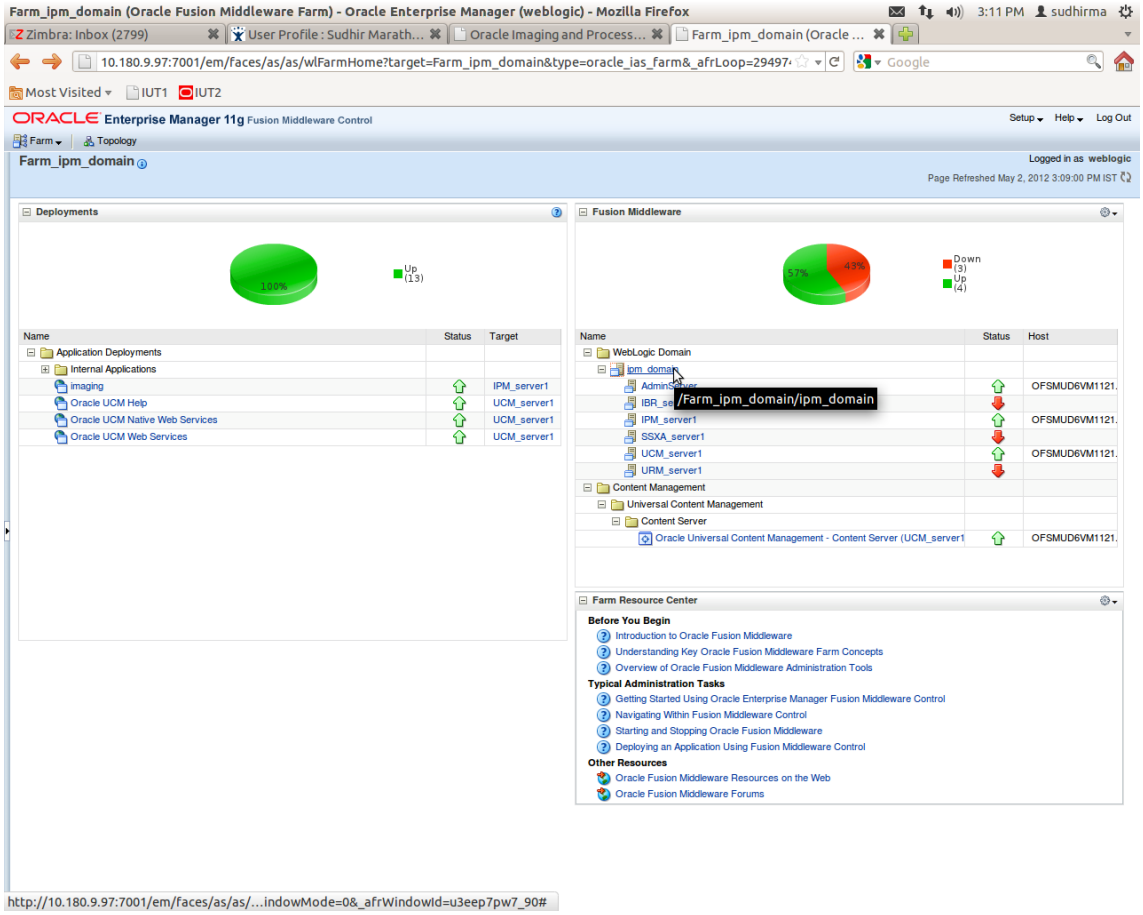
1. Log in to Enterprise Manager (EM) console.

Figure 7–35 EM Console Login



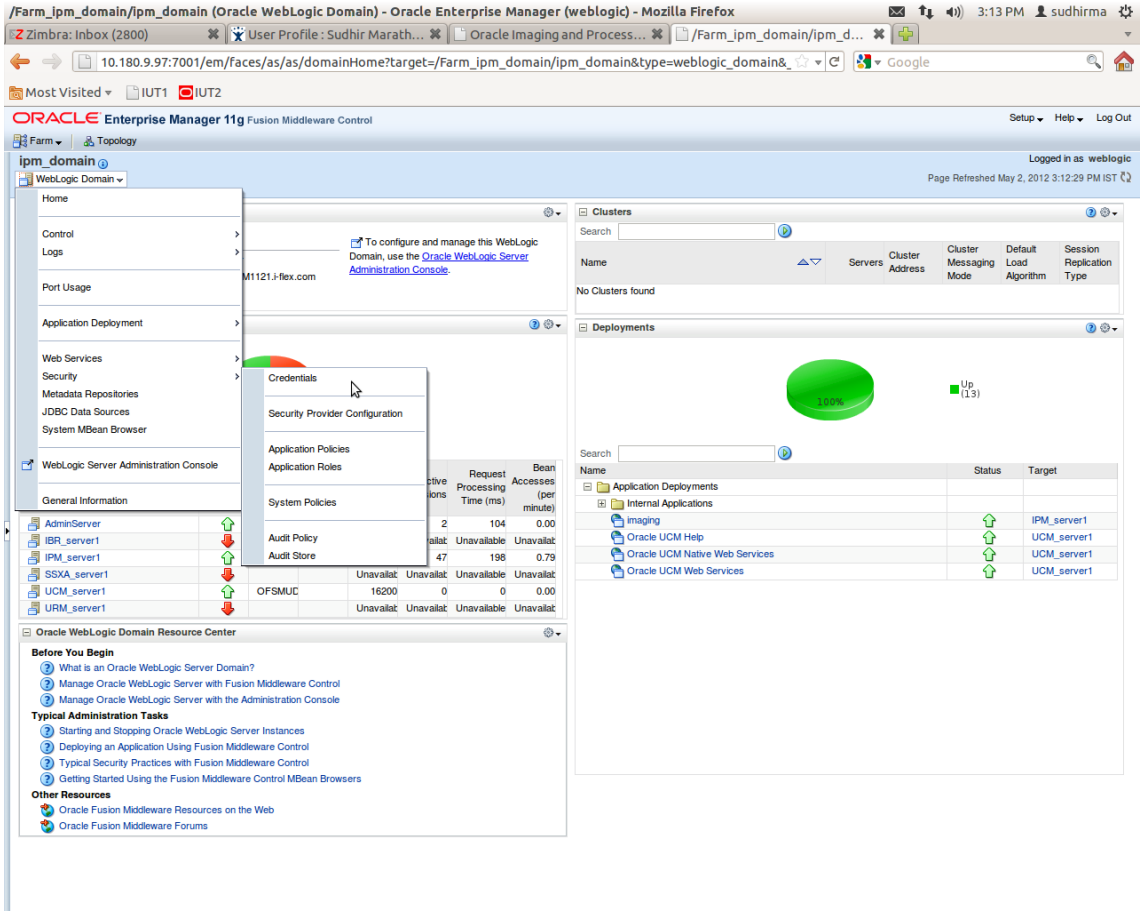
2. In the Name section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 7–36 Click Weblogic Domain: ipm domain



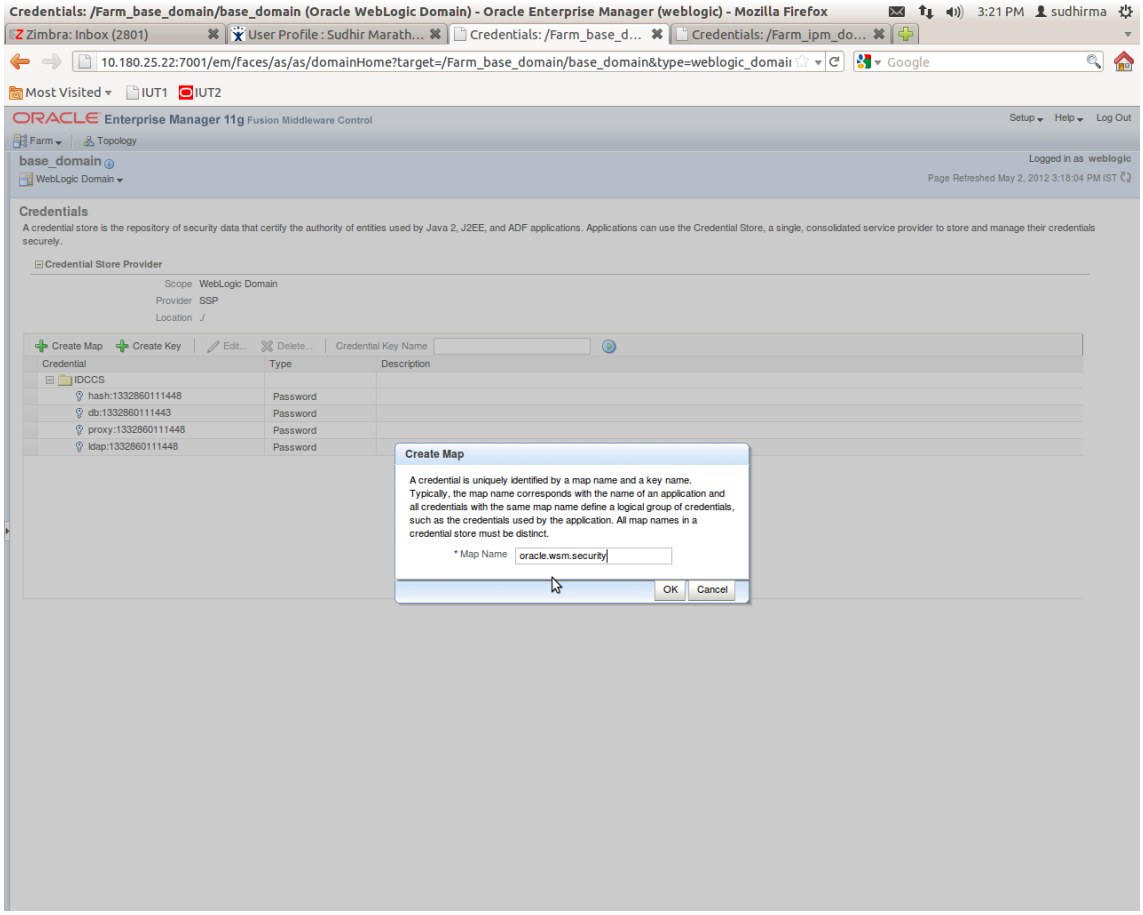
3. In the top menu, **click Weblogic Domain**. The corresponding menu appears.
4. Navigate to **Security > Credentials**. The Credentials page appears.

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



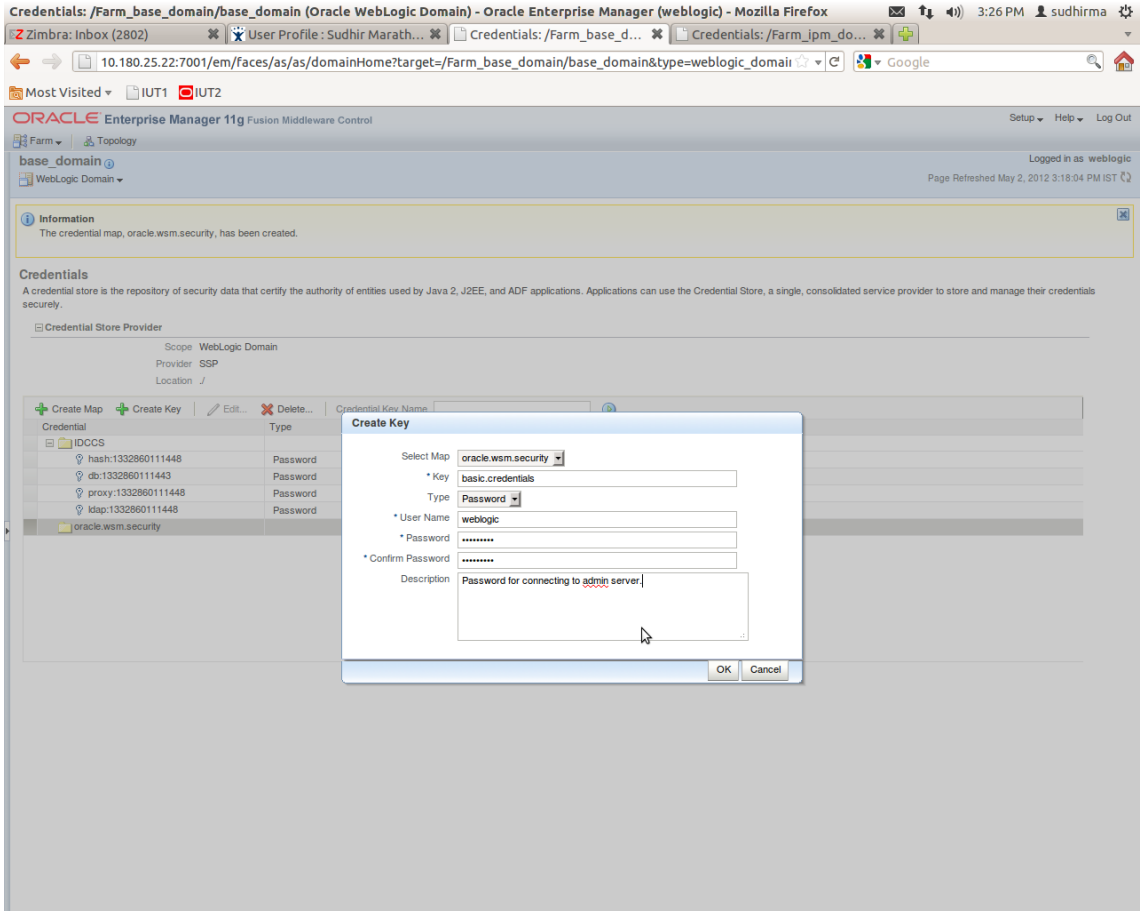
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 7–38 Create Map oracle.wsm.security



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

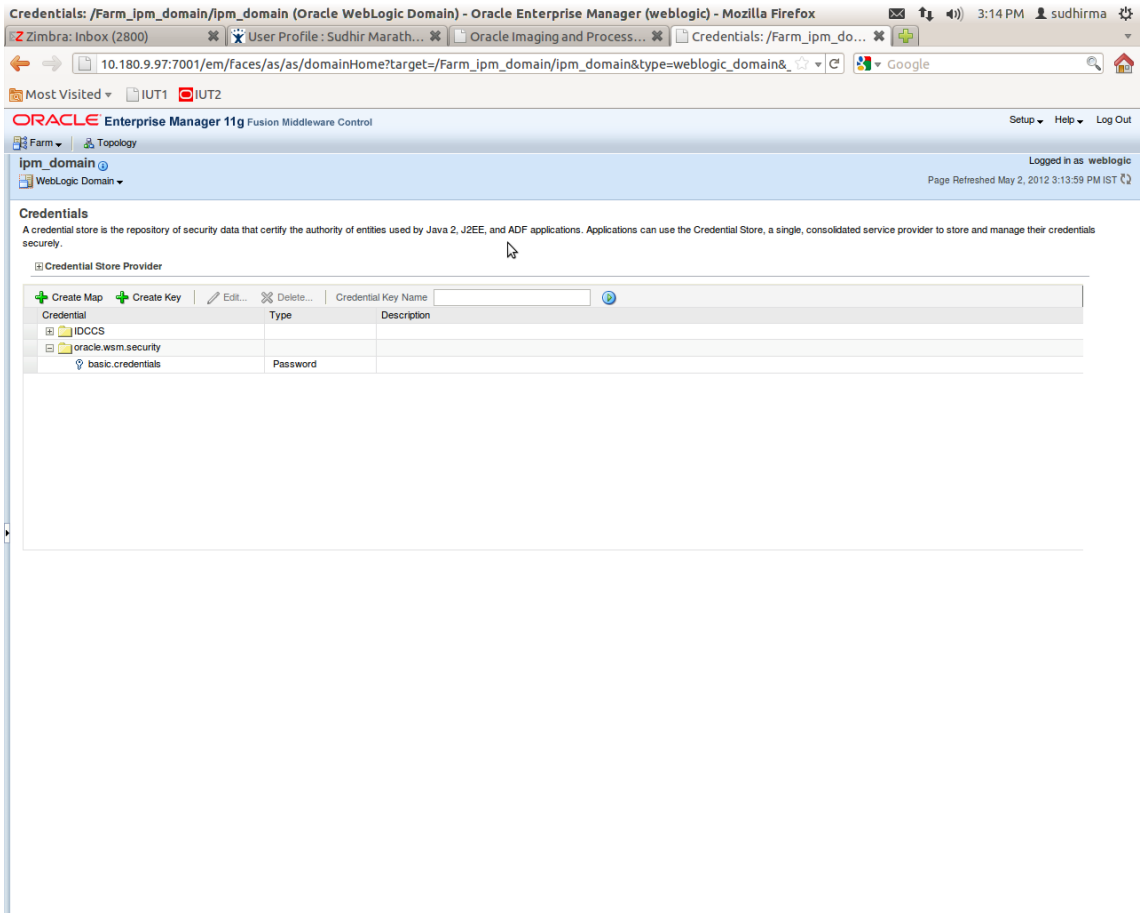
Figure 7–39 Create Key basic.credentials



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

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

Figure 7–40 ipm_domain: Credentials Created

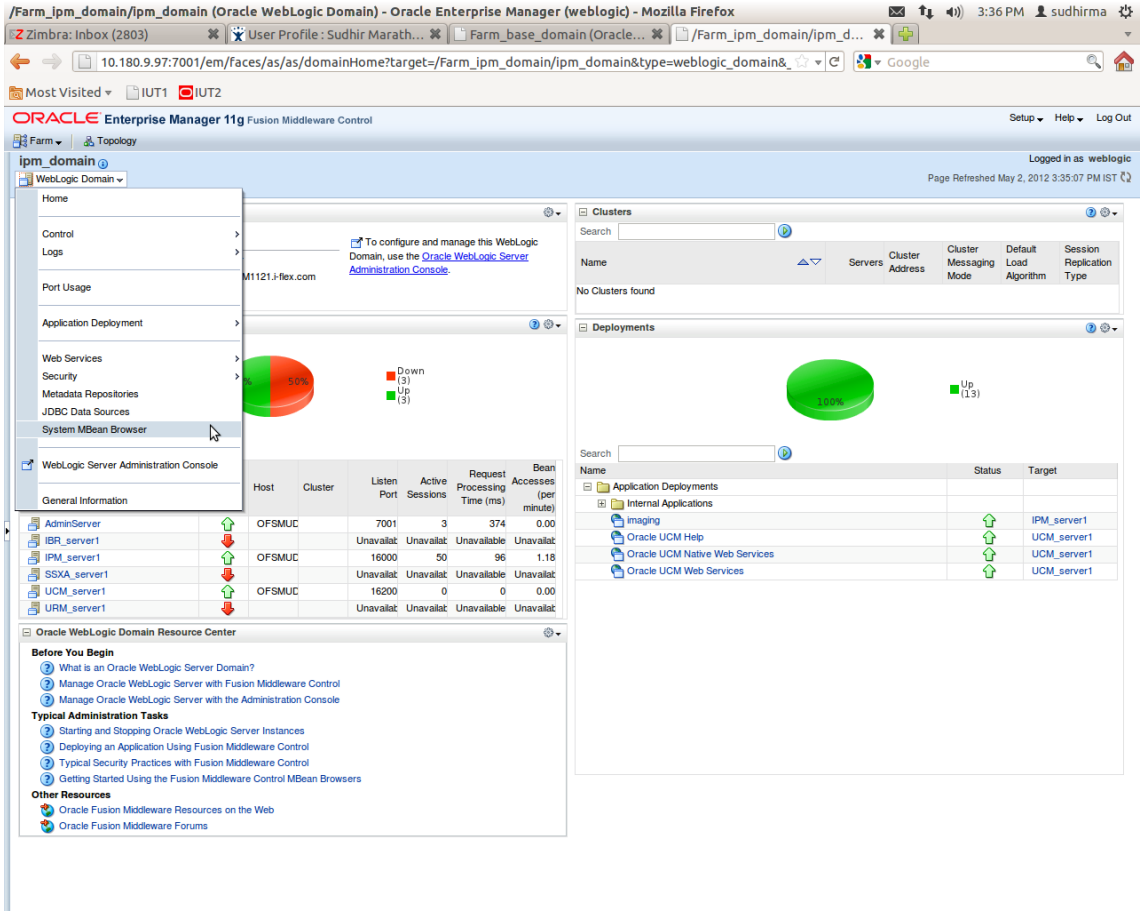


7.2.3 Setting up Input Agent Path

To set up input agent path:

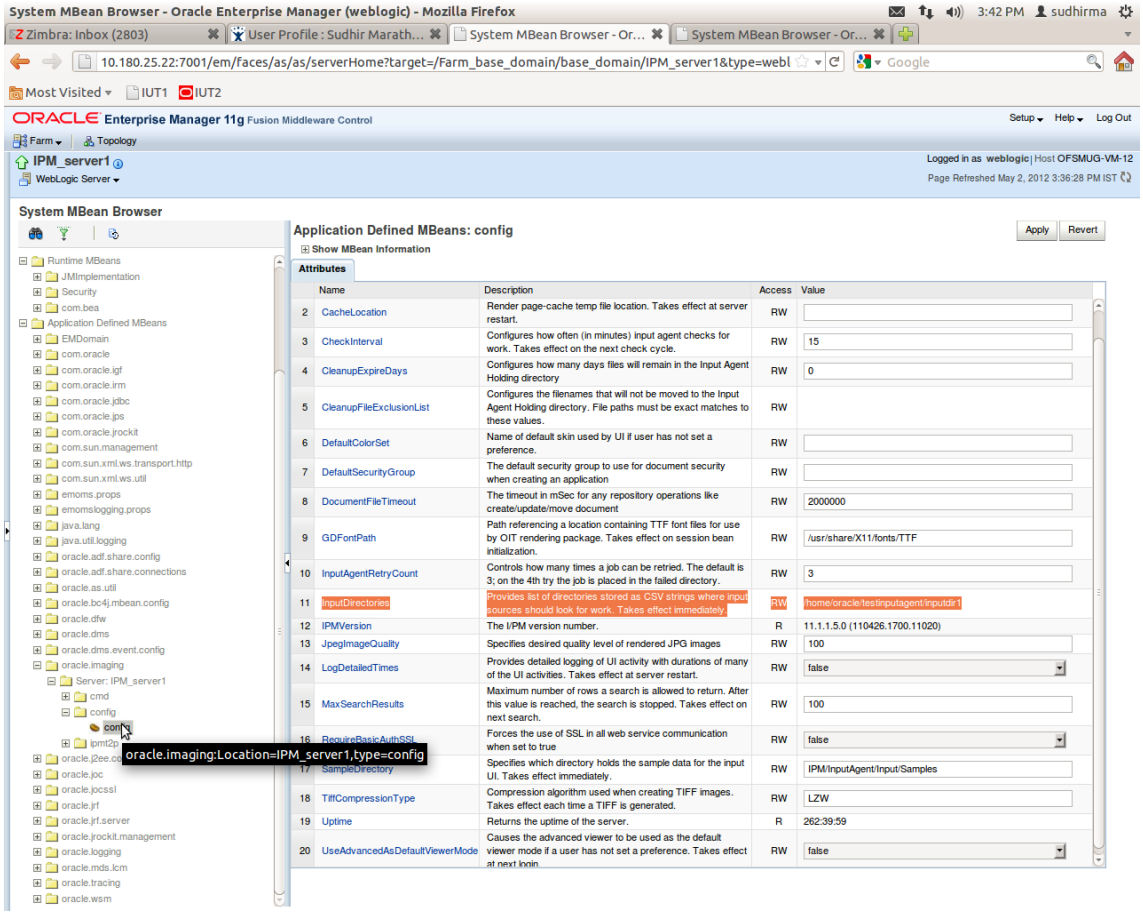
1. Log in to Enterprise Manager (EM) console.
2. In the Name section, under Weblogic domain, click **ipm domain.**
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

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



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

Figure 7–42 InputDirectories: Enter Input Agent Path



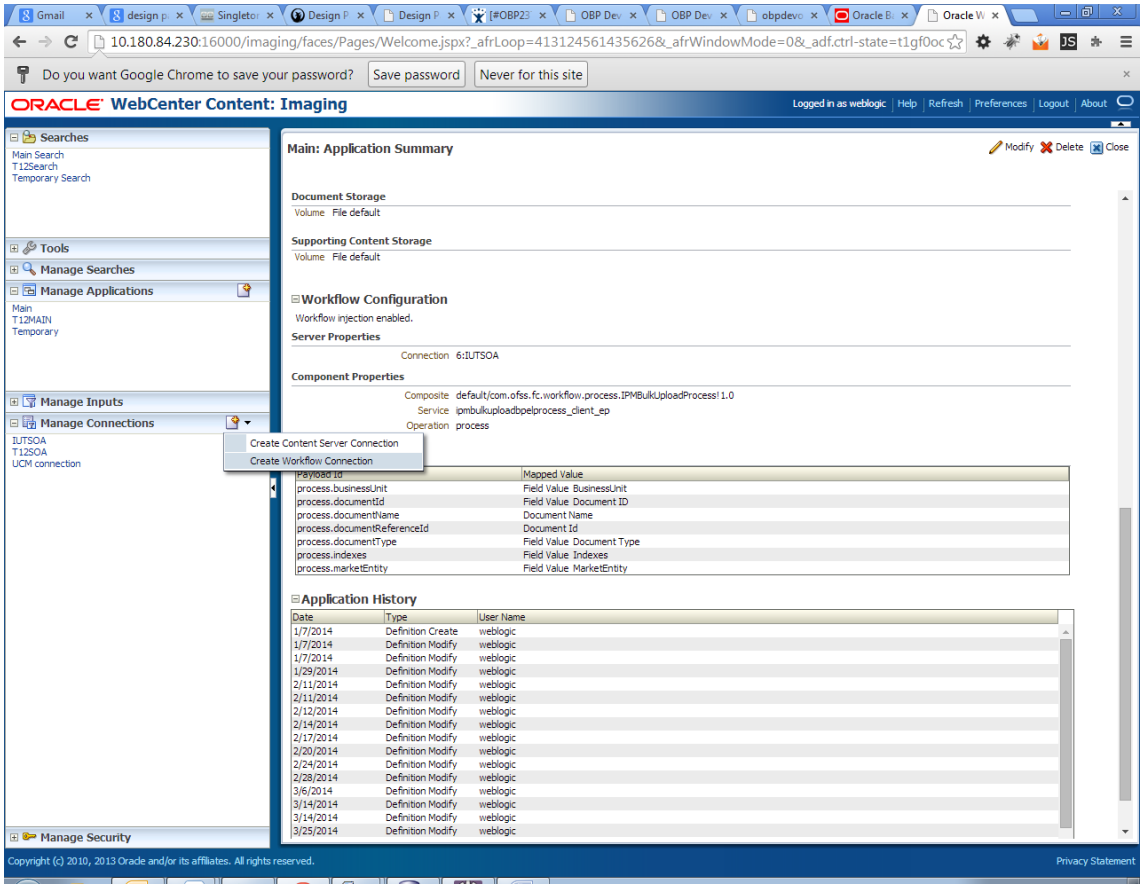
7. Restart IPM server.

7.2.4 Create SOA Connection

To create a SOA Connection:

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

Figure 7–43 Manage Connections: Create Workflow Connection



3. Click **Create Workflow Connection.**

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

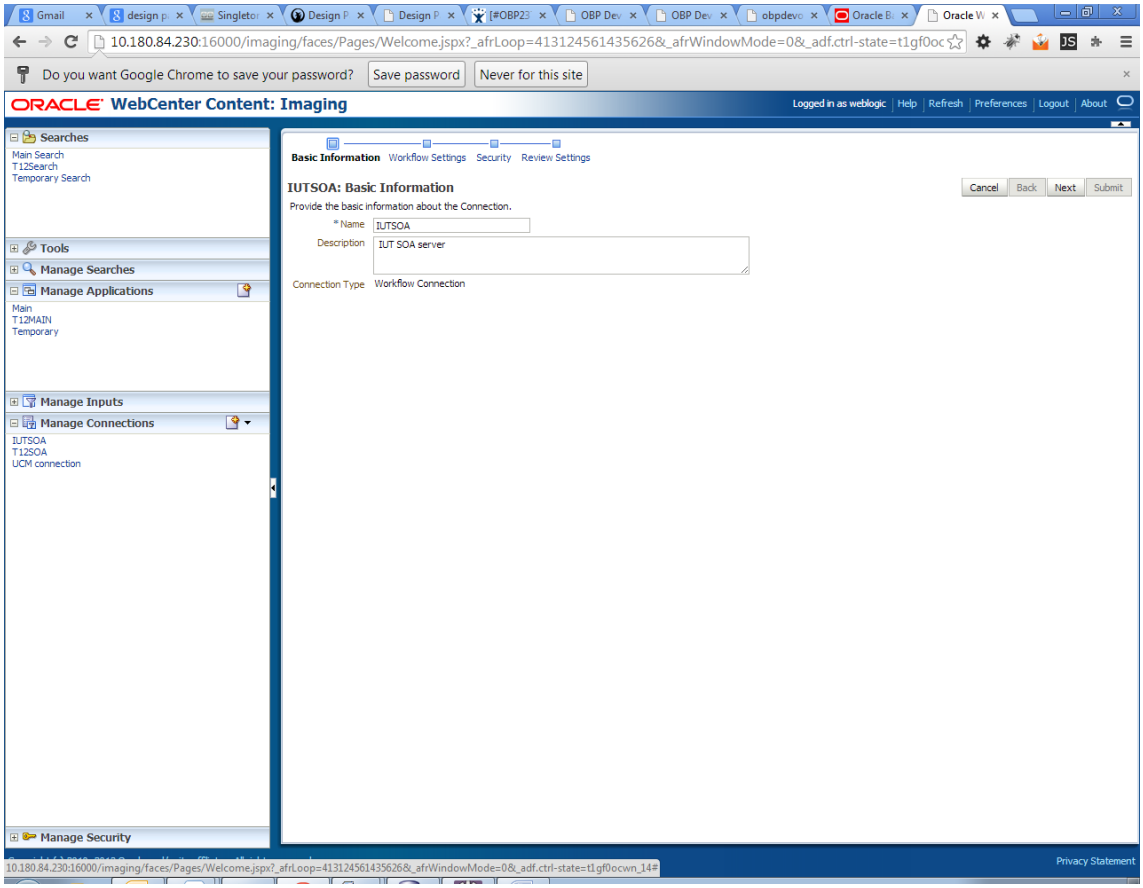
   `OBP_IPM_SOA_CONN_NAME`

   `SOA_MANAGED_SERVER_LISTEN_ADDRESS`

   `SOA_MANAGED_SERVER_LISTEN_PORT`

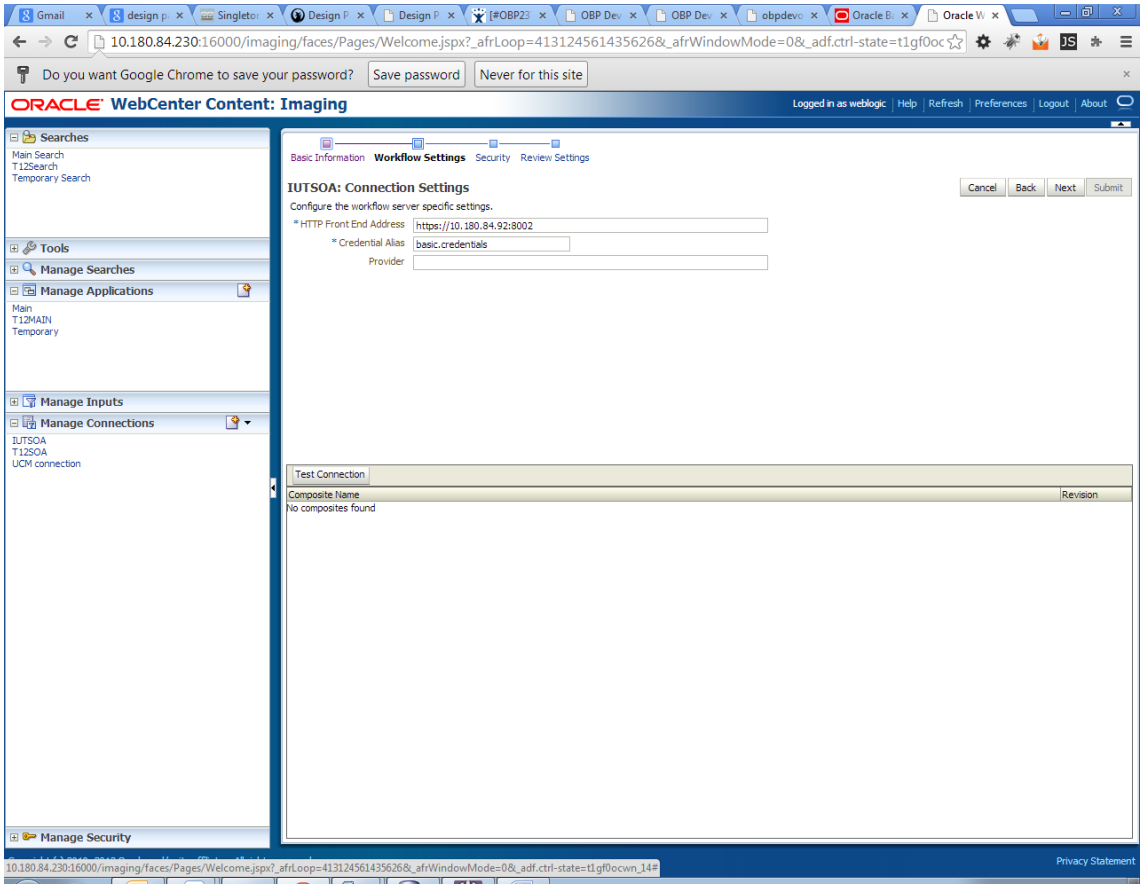
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 7–44 IUTSOA: Basic Information



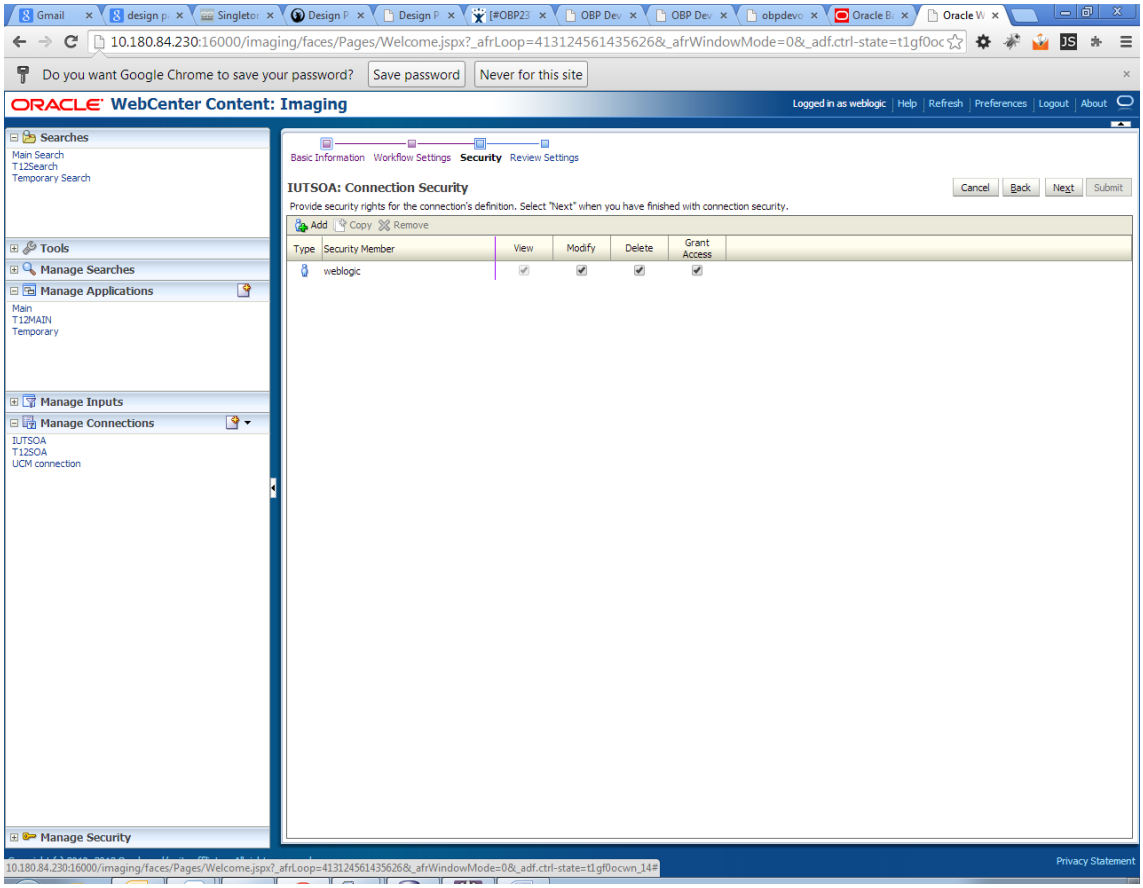
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 7–45 IUTSOA: Workflow Settings



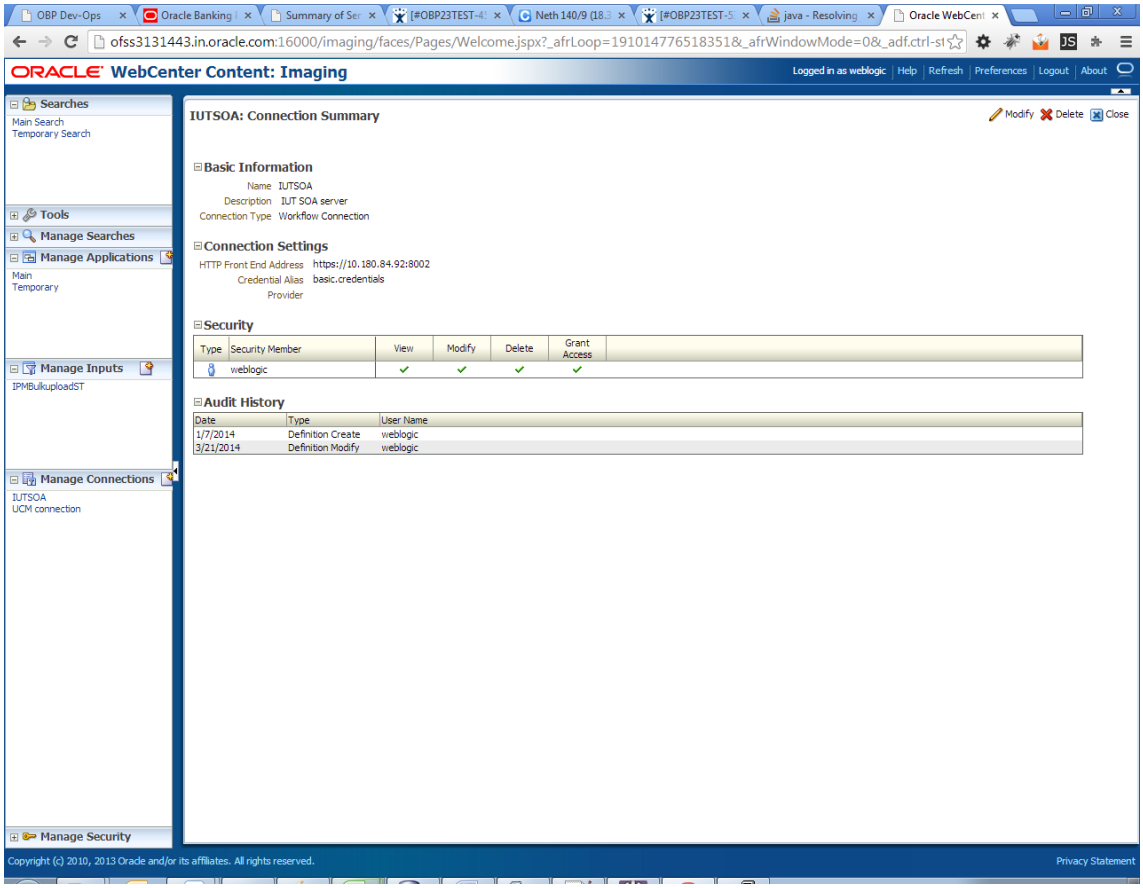
6. In the **Credential Alias** field, enter the value as **basic.credentials**.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 7–46 IUTSOA: Connection Security



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

Figure 7–47 IUTSOA: Review Settings

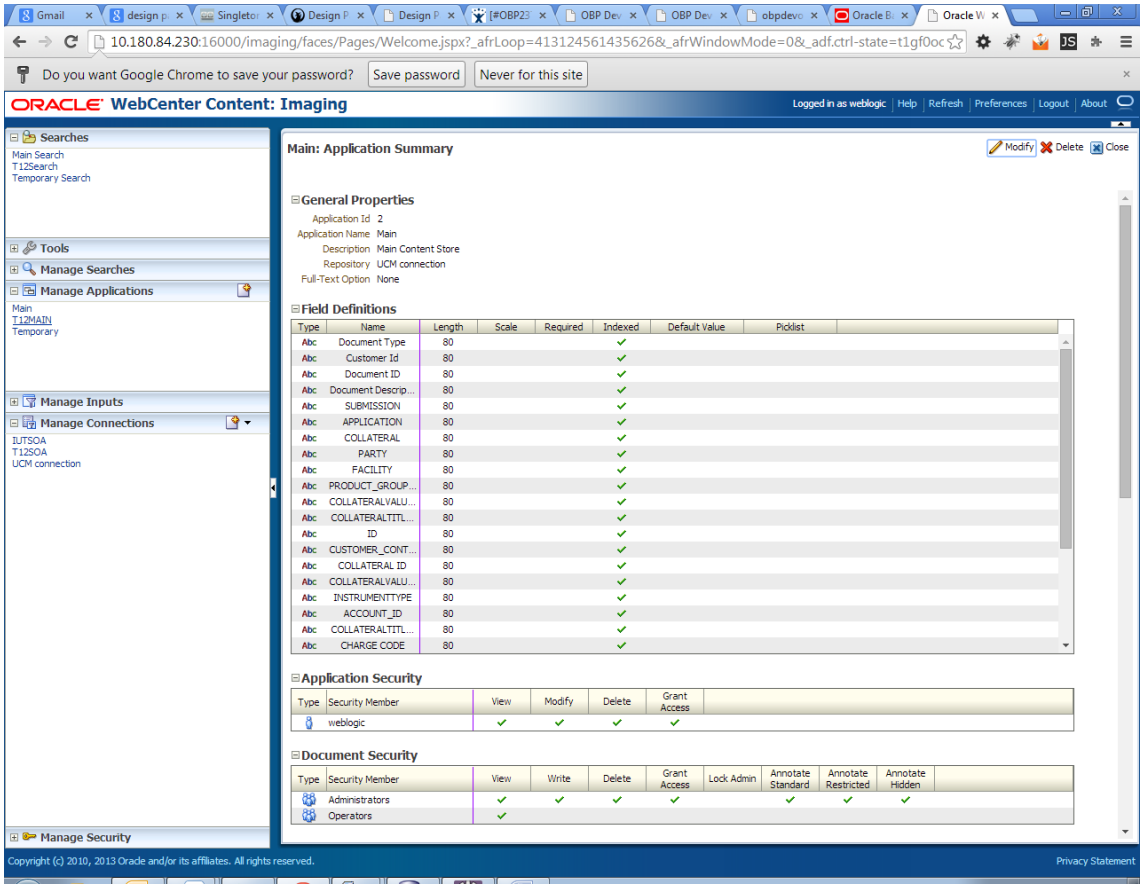


7.2.5 Manage Workflow Configuration

To manage workflow configuration:

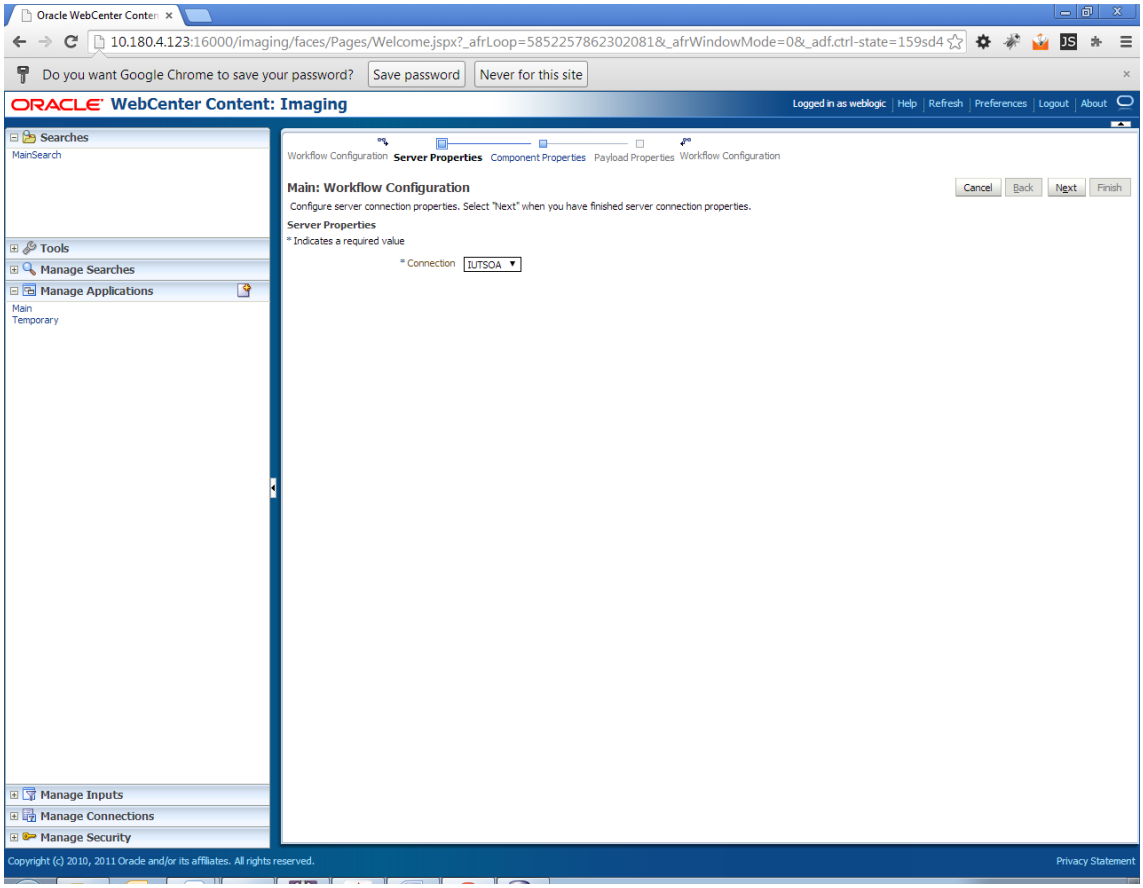
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Applications** section.

Figure 7–48 Main: Application Summary



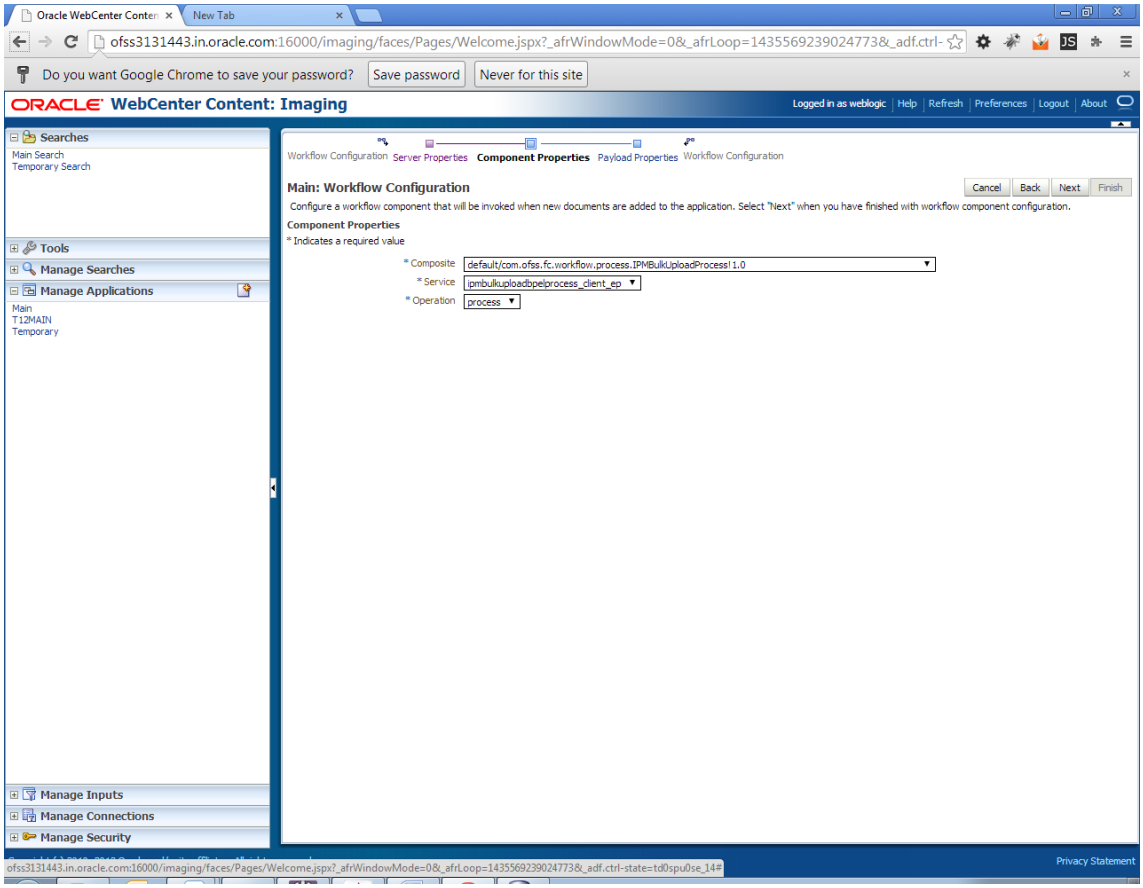
3. Select the application for which workflow configuration has to be done as shown in Figure 7–48.
4. Click **Modify.**
5. Navigate to the Workflow Configuration section.
6. Click the **Add/Modify** button.
7. In the Server Properties section, select the connection (IUTSOA) which was created in **Manage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

Figure 7–49 Manage Applications - Server Properties



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

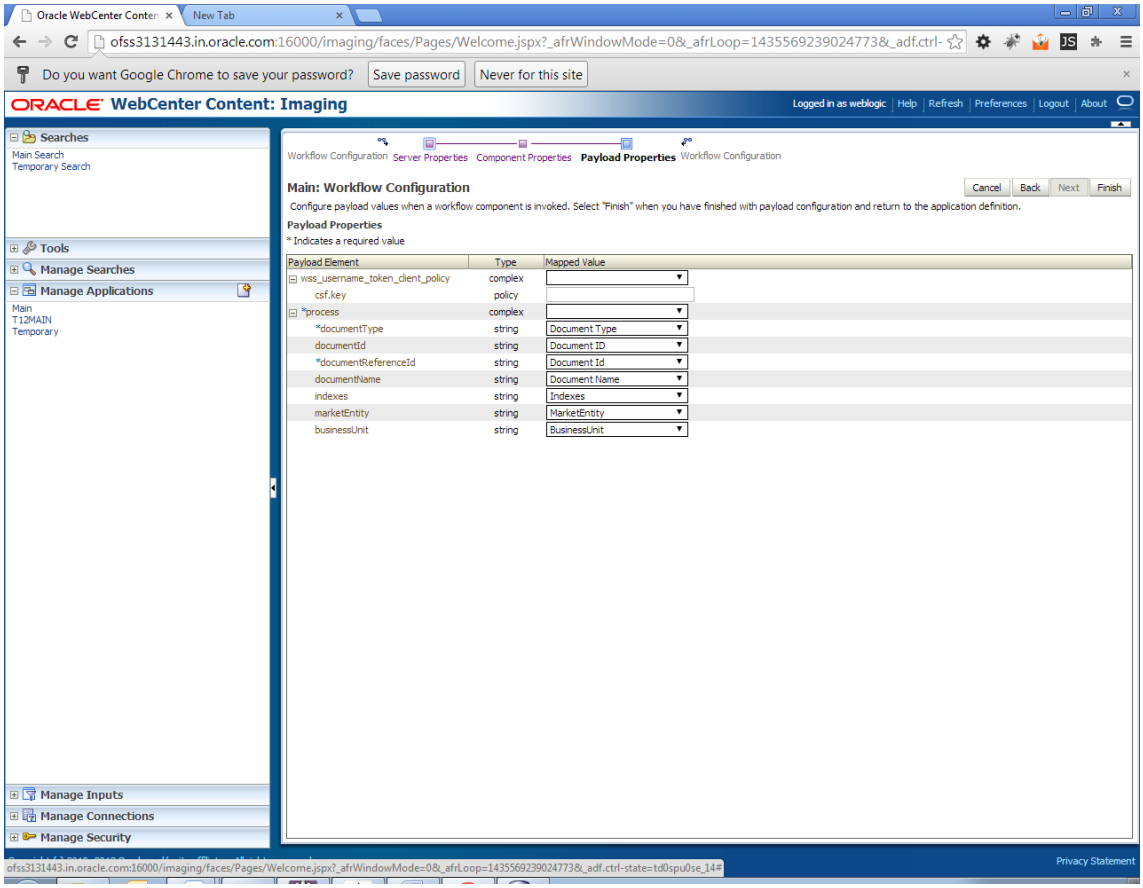
Figure 7–50 Manage Applications - Component Properties



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

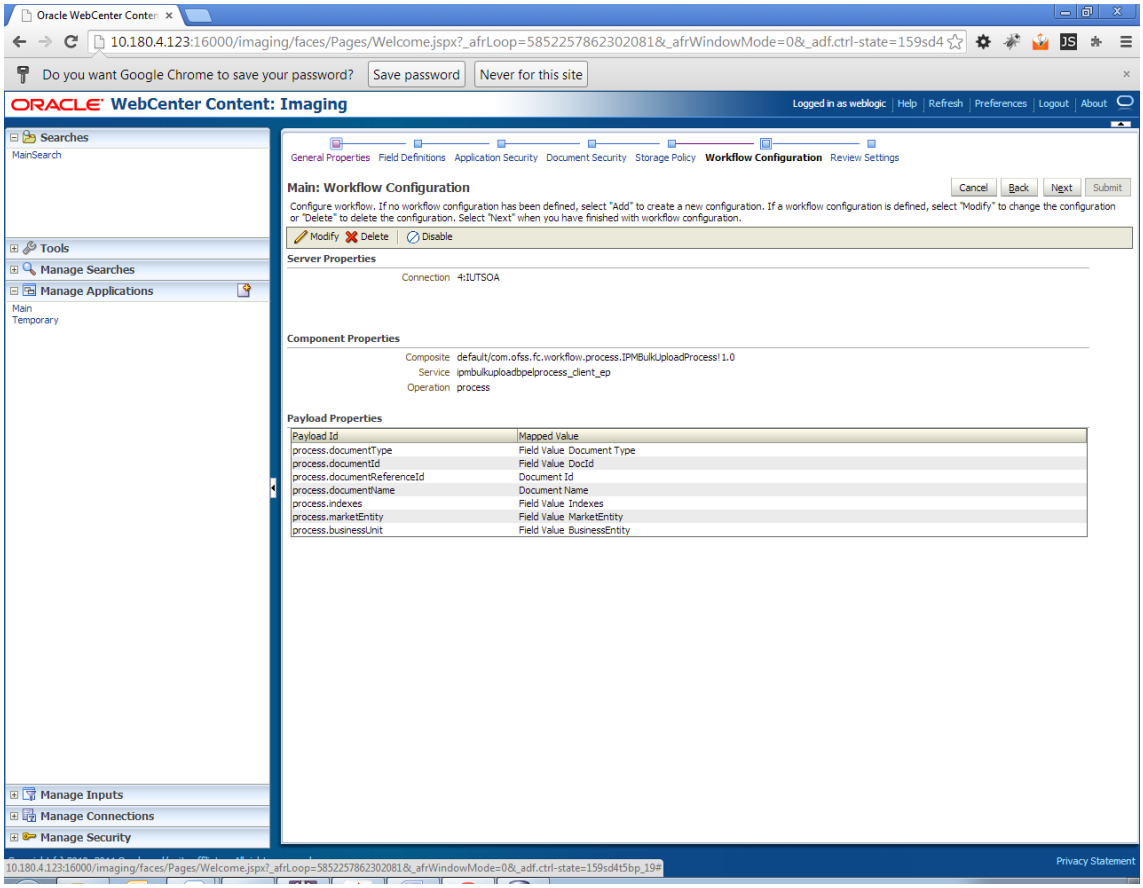
> **Note**
>
> The document ReferenceId is mapped to Document Id (IPM internal field), whereas documentId is mapped to doc Id which is application field.

Figure 7–51 Manage Applications - Payload Properties



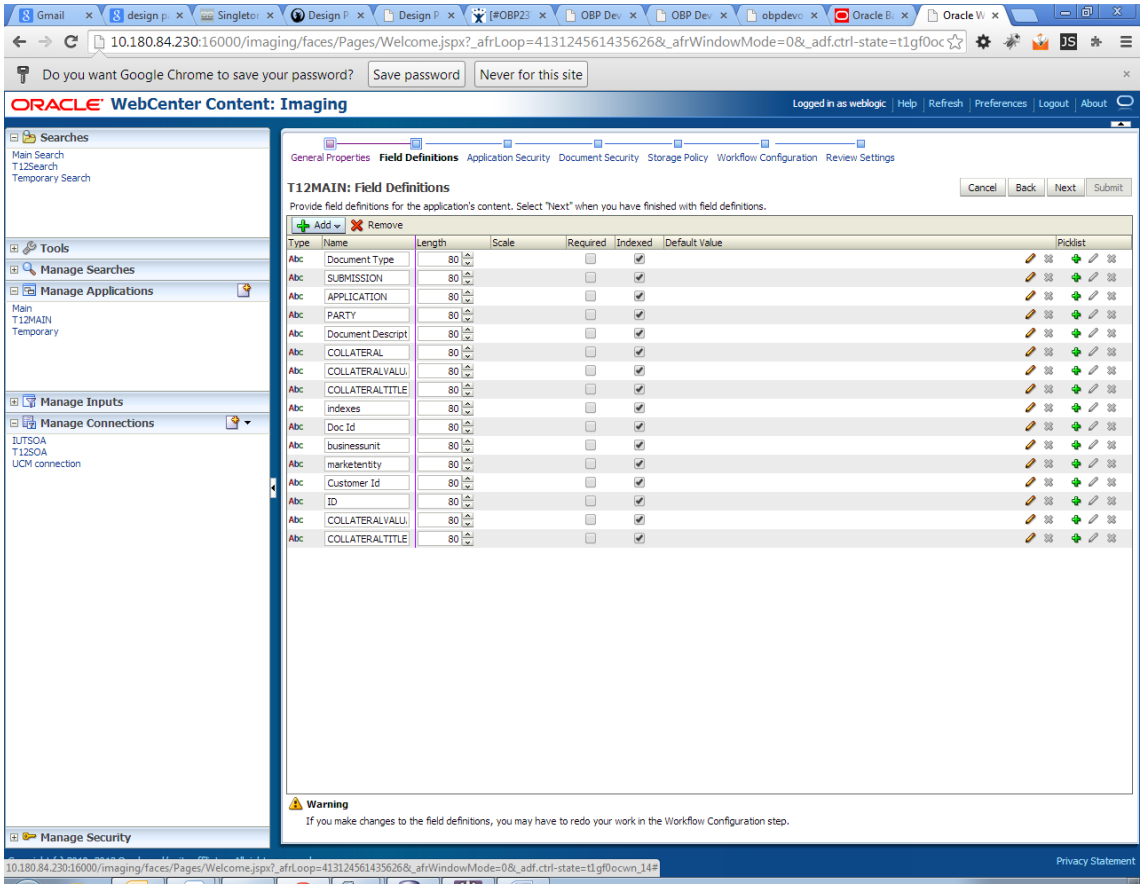
16. Click **Next.**
17. Complete the Workflow Configuration. Click **Next.**

Figure 7–52 Manage Applications - Workflow Configuration



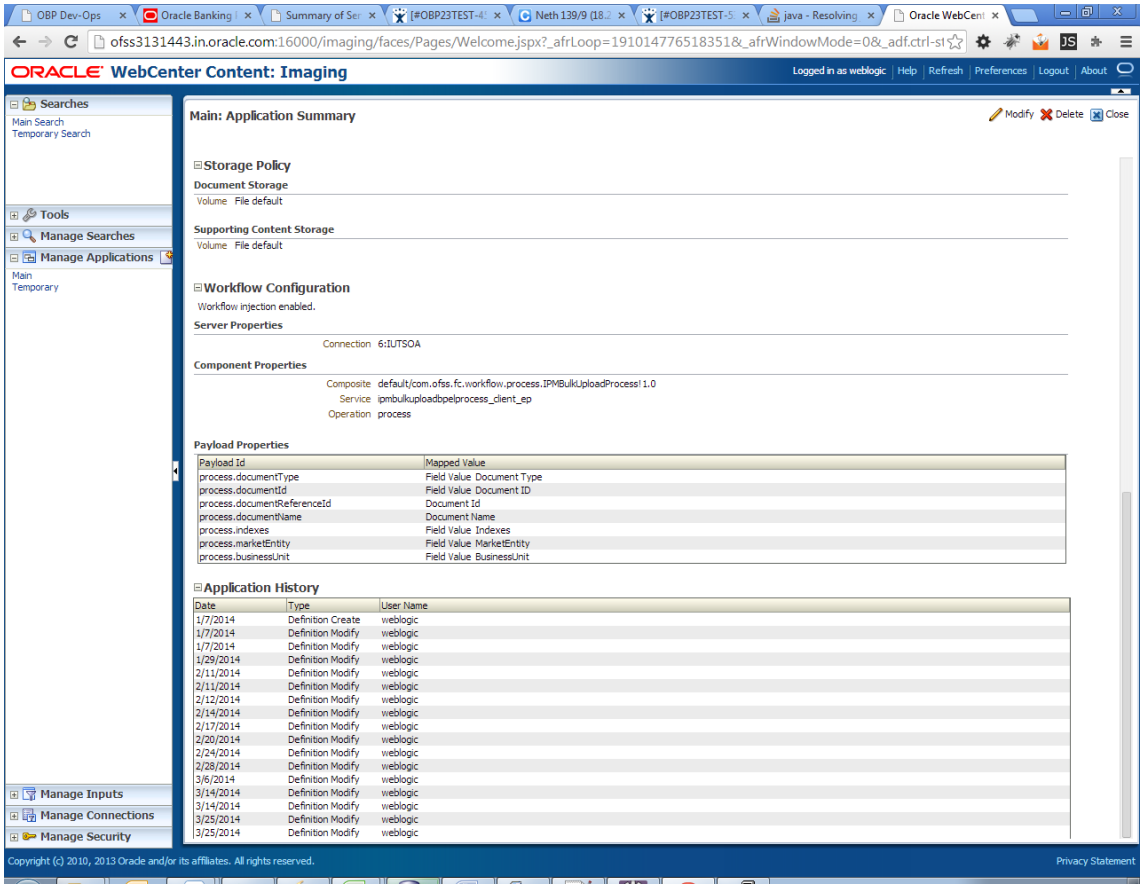
18. Add all those fields which are not present in the application as shown below.

Figure 7–53 Field Definitions



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

Figure 7–54 Main: Application Summary

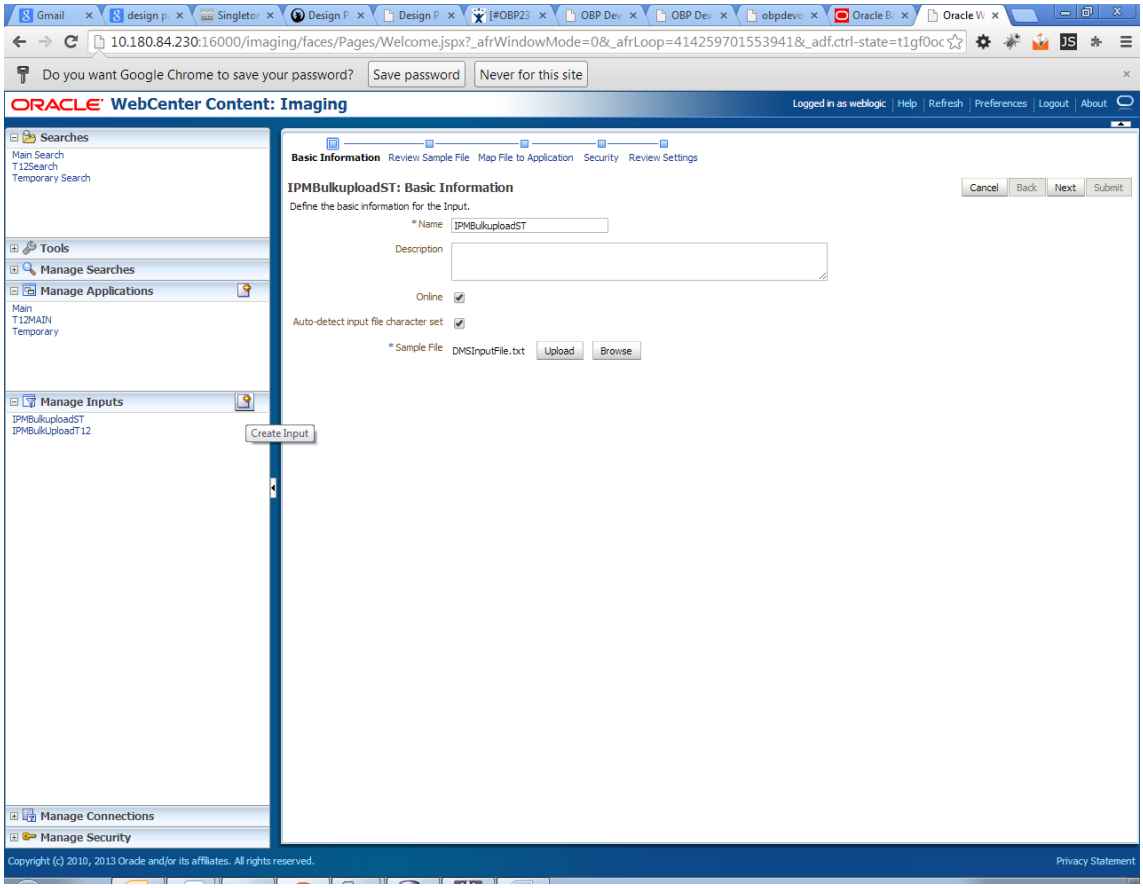


7.2.6 Manage Inputs for Input Agents

To manage workflow configuration:

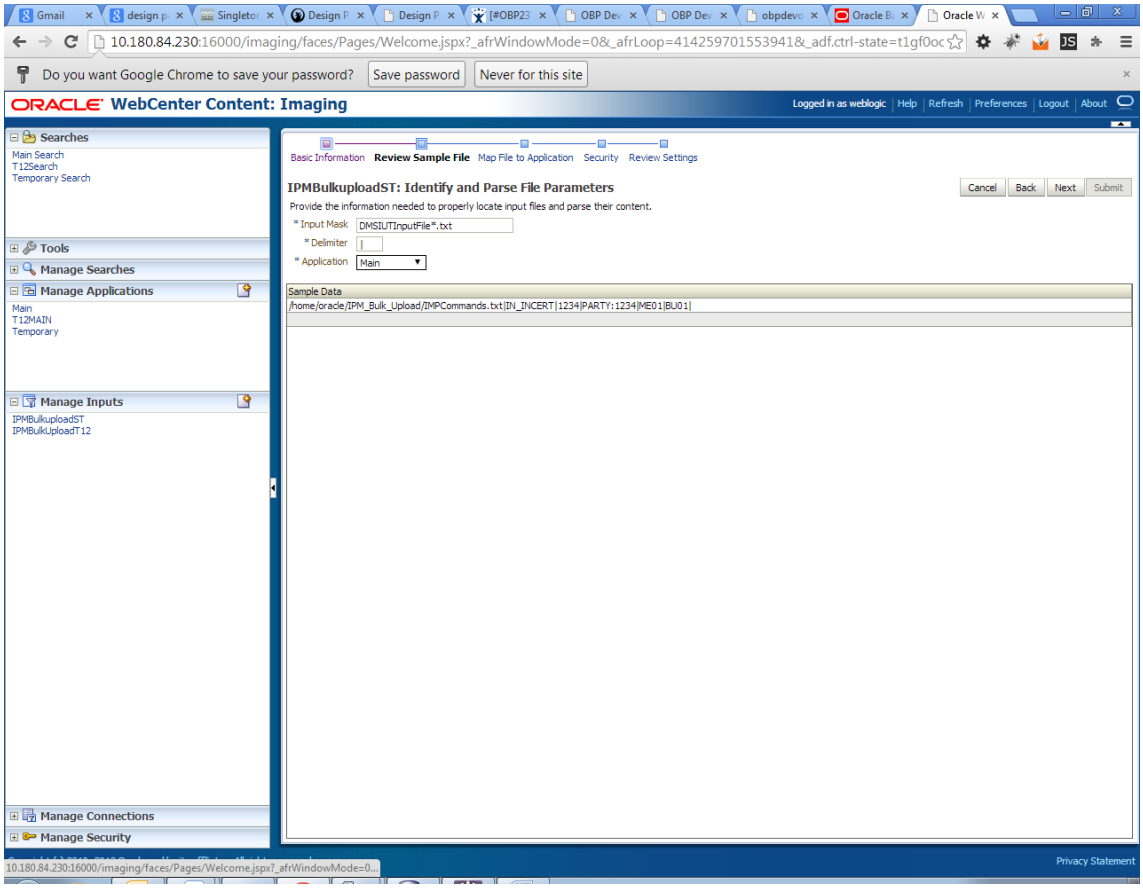
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Inputs** section.

Figure 7–55 Input Agent: Basic Information



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

Figure 7–56 Input Agent: Input Mask



5. Upload the attached sample file.

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

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

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

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

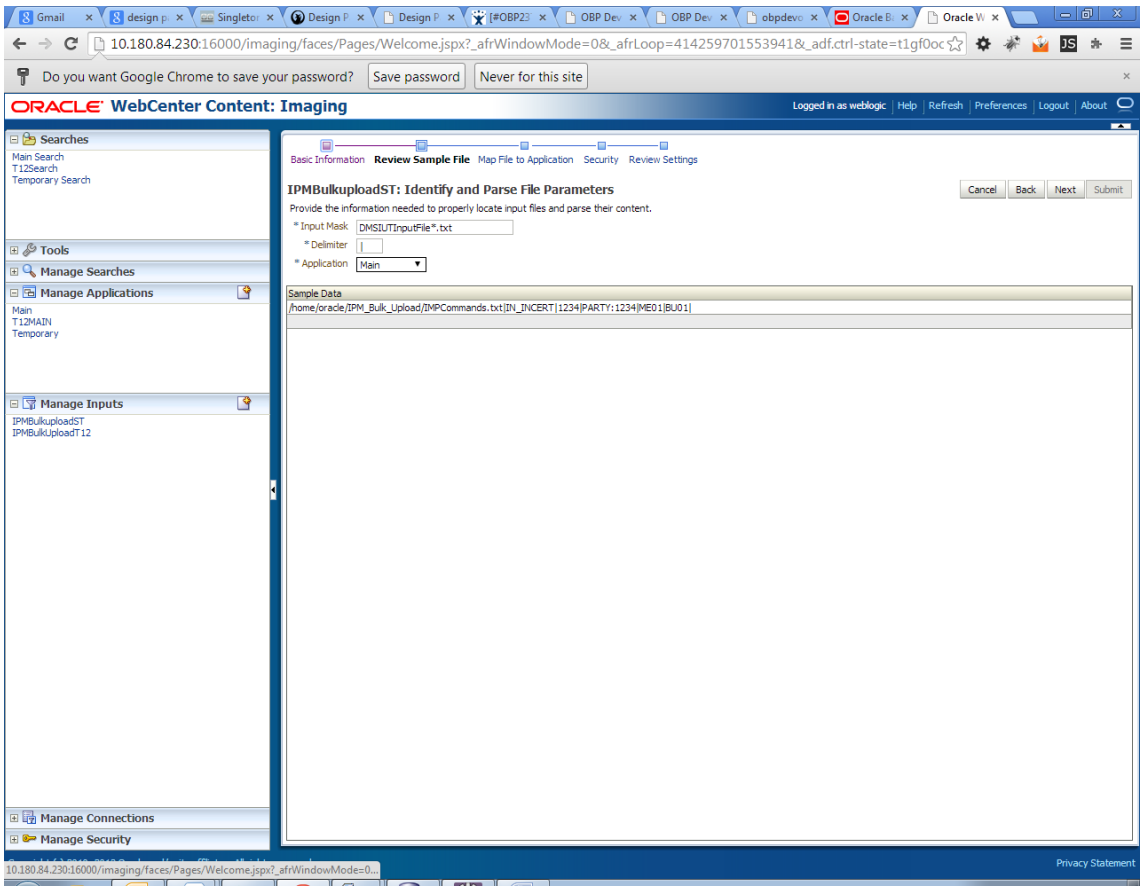
   Note

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

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

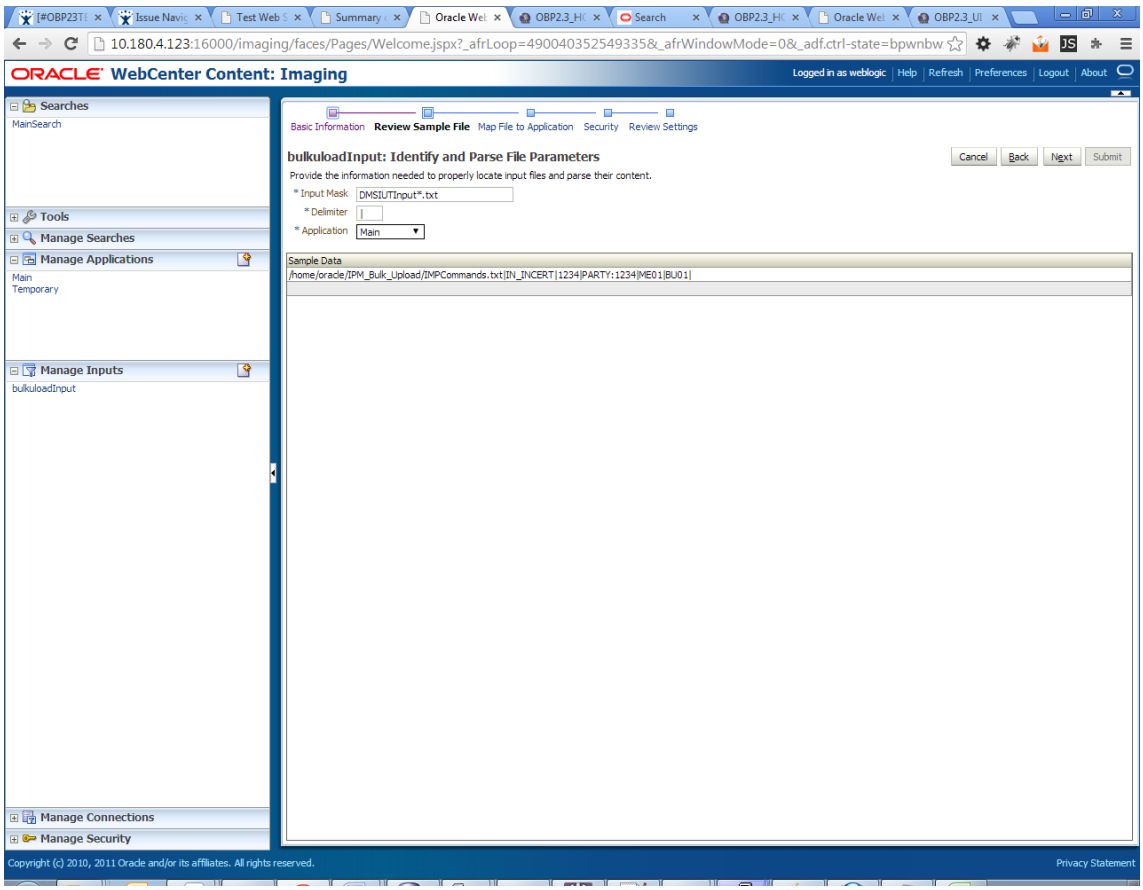
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 7–57 Input Agent: File Parameters



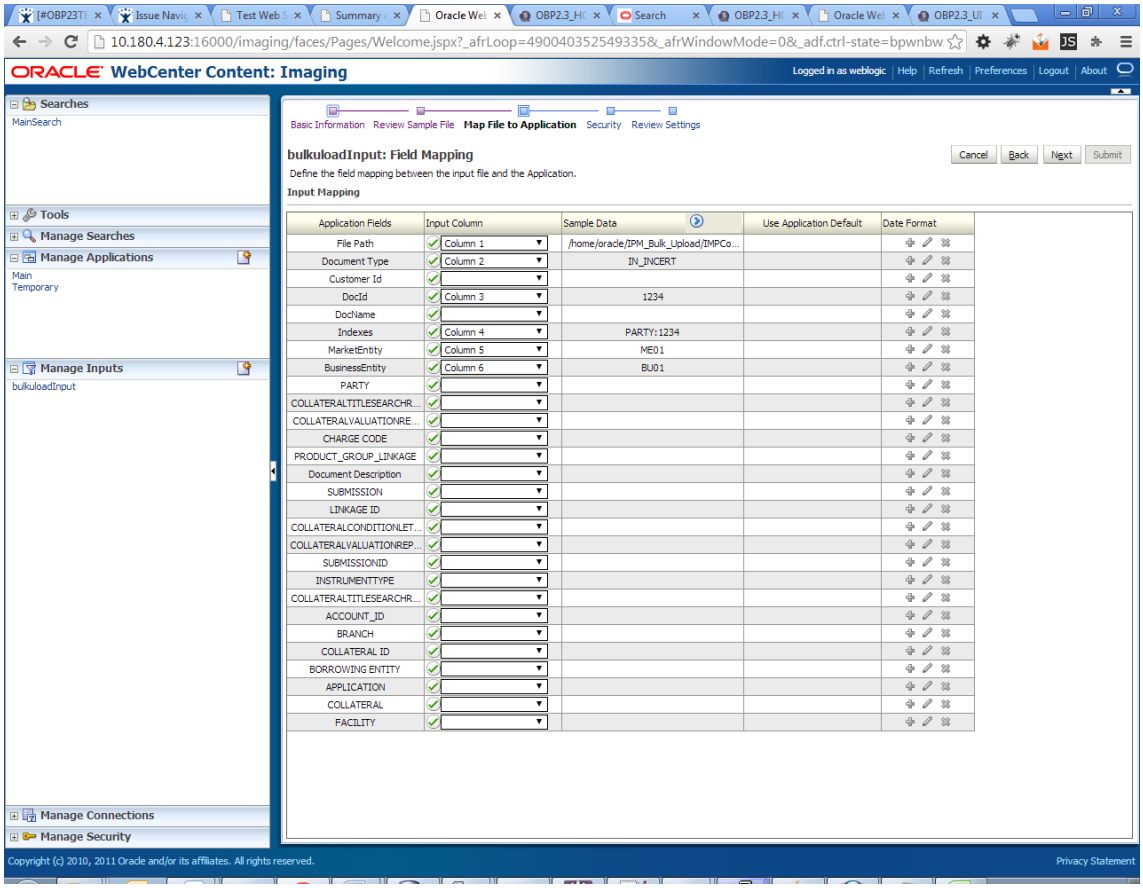
9. In the Field Mapping section, map the **Application Fields.**

Figure 7–58 Input Agent: Fields Mapping



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

Figure 7–59 Input Agent: Summary



Note

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

7.2.7 Additional Steps

1. Update user and bankcode as follows:

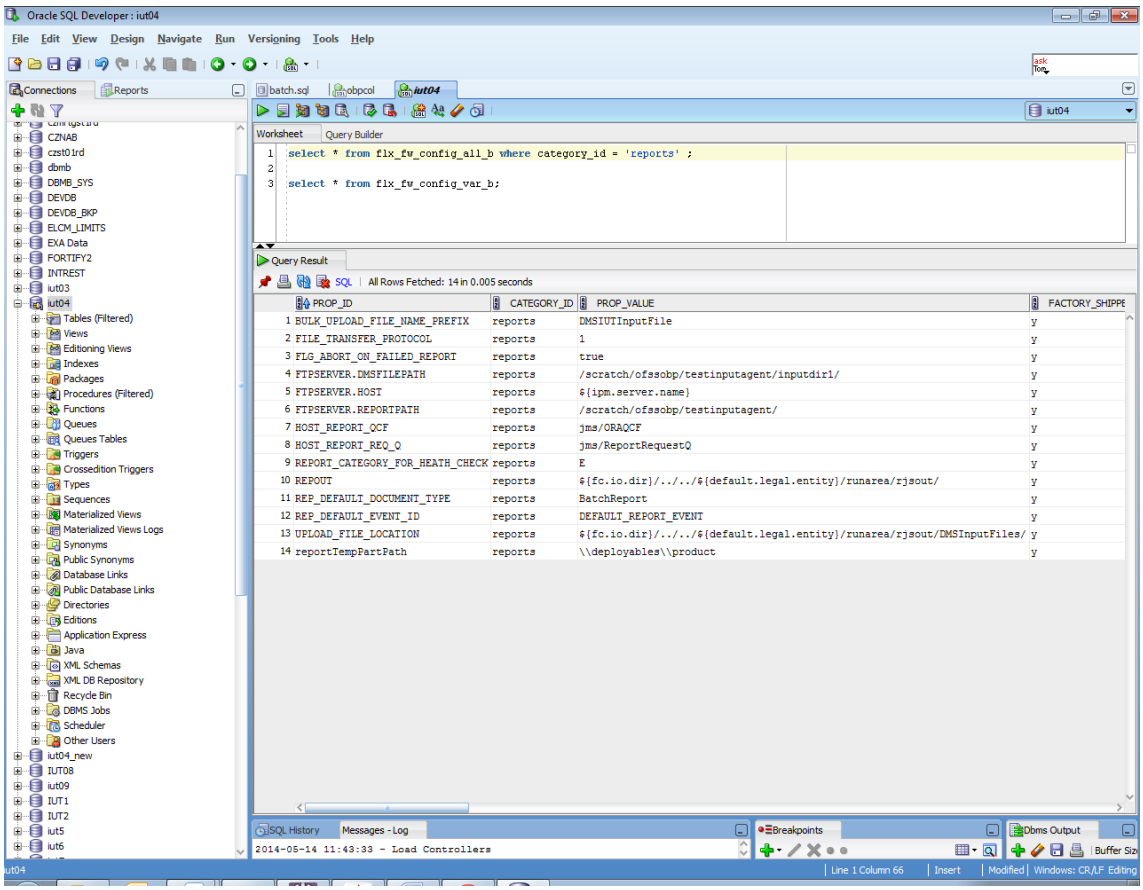
```
update flx_fw_config_all_b set prop_value='48' where prop_
value='335' and category_id like 'contentmanager%';
update flx_fw_config_all_b set prop_value='ofssuser' where
prop_id='userId' and category_id like 'contentmanager%';
```

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

Table 7–1 PROP ID Values

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

Figure 7–60 flx_fw_config_all_b table



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

7.2.8 SSL Handshake Resolution

For resolving the SSLHandshake between IPM and SOA server:

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

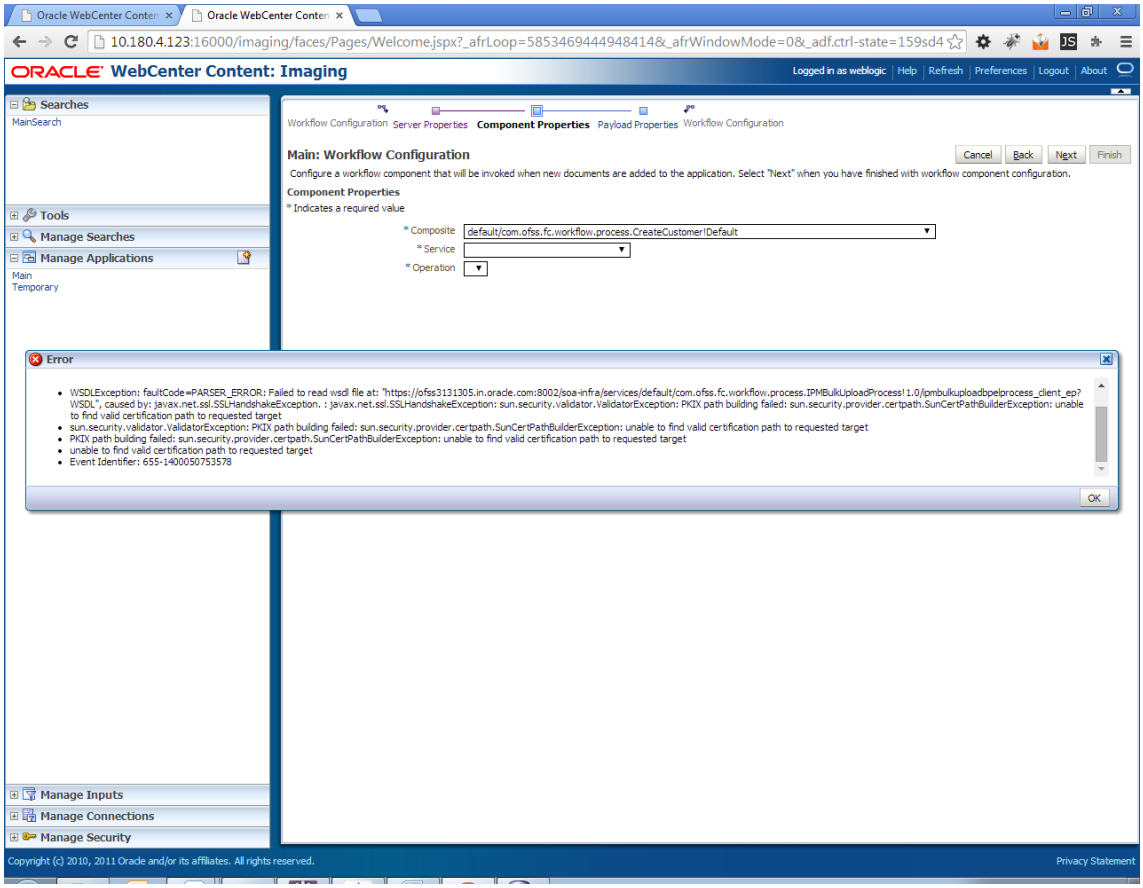
   Copy certificate at following path on IPM server.

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

   Security for called method

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

Figure 7–61 SSL Handshake Resolution



7.3 IPM Report Upload Setup

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

7.3.1 Prerequisites

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

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

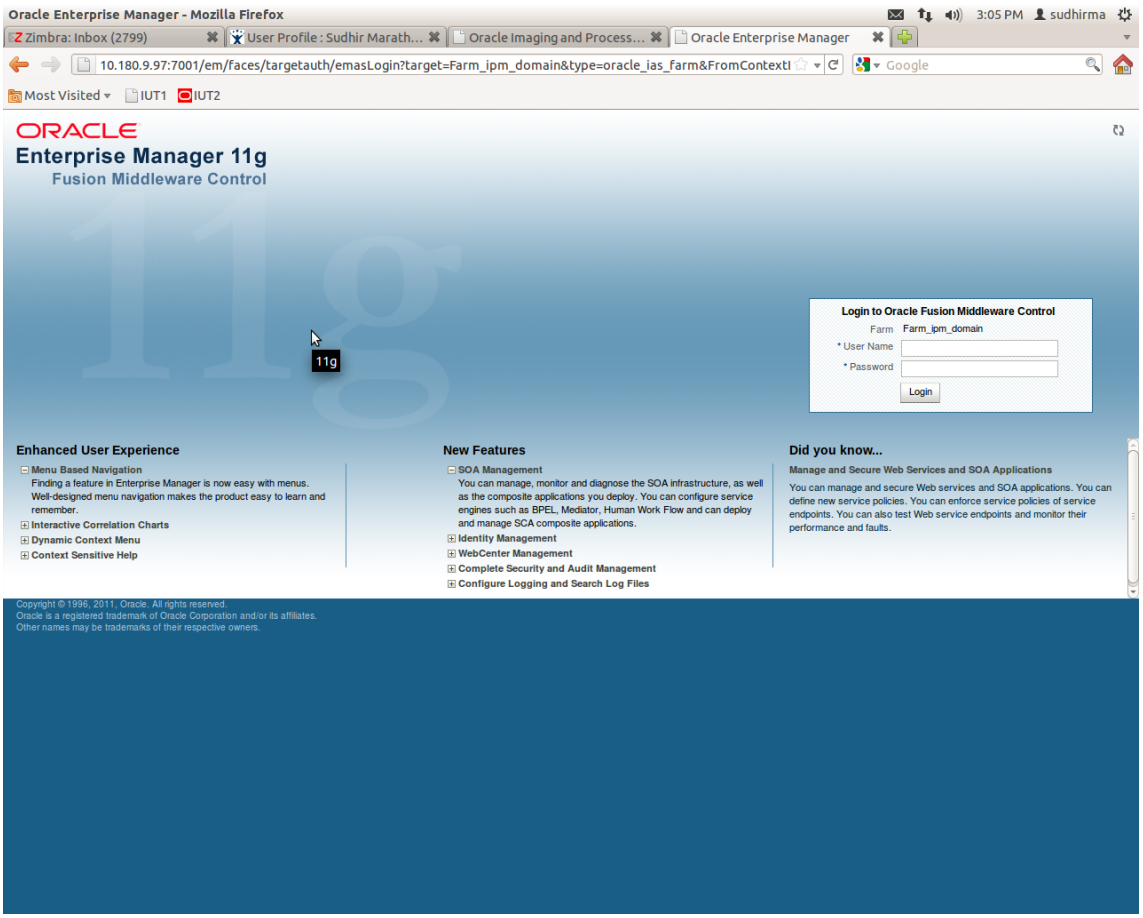
7.3.2 Setting up the Connection Name

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

To set up a bulk process:

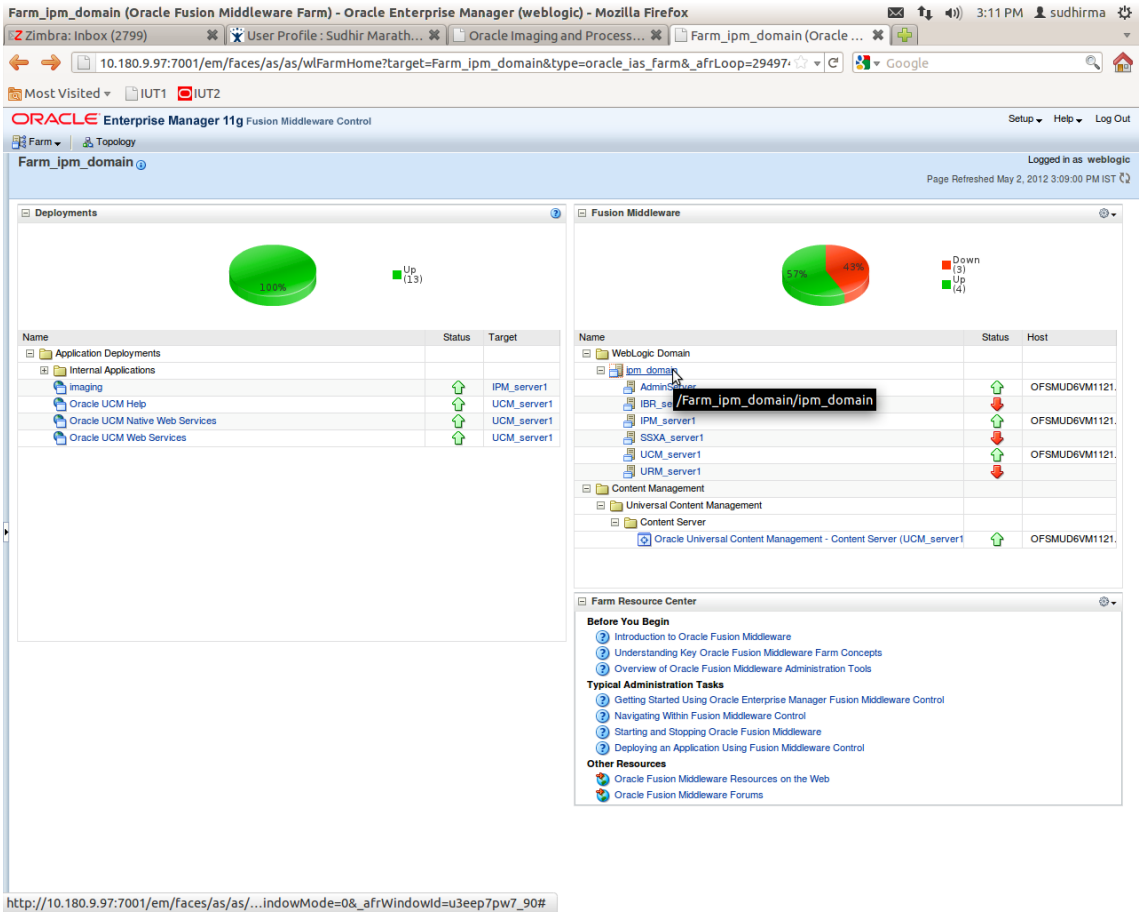
1. Log in to Enterprise Manager (EM) console.

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



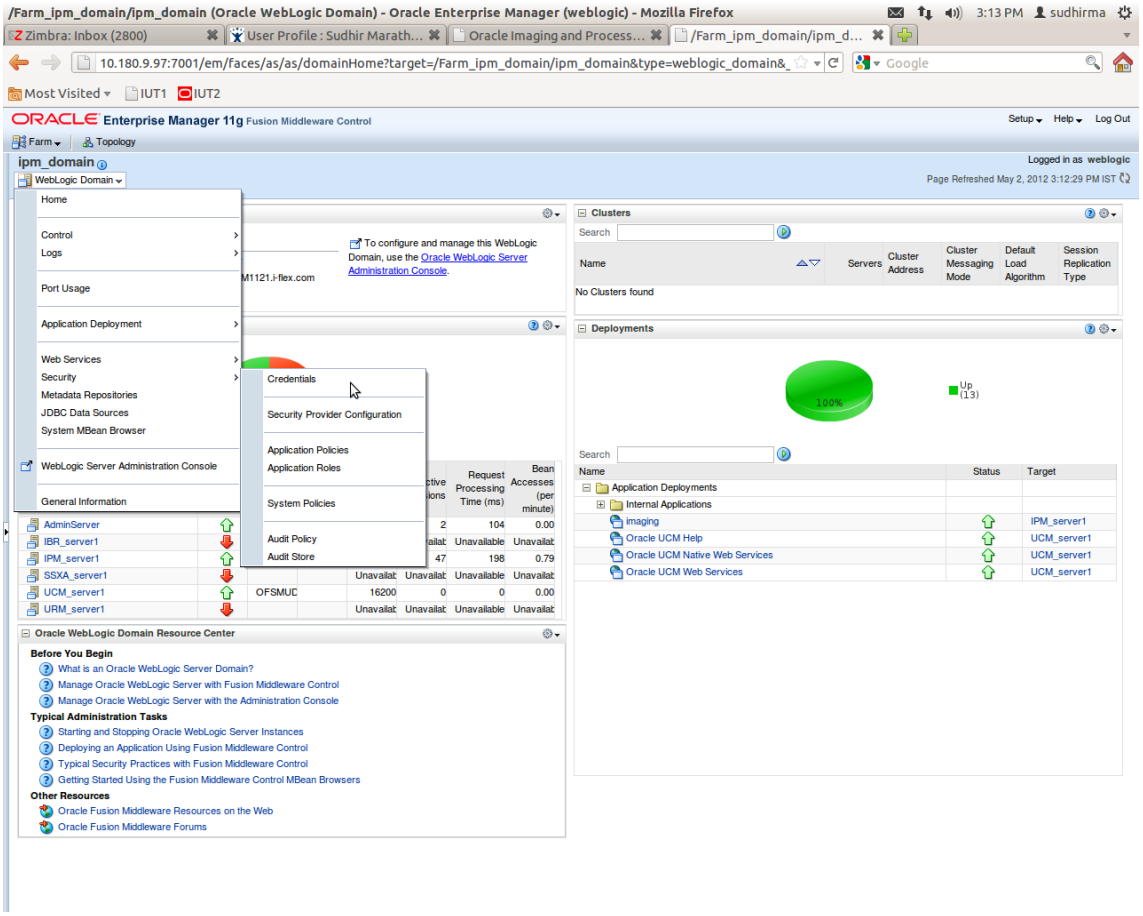
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 7–63 Click Weblogic Domain: ipm domain



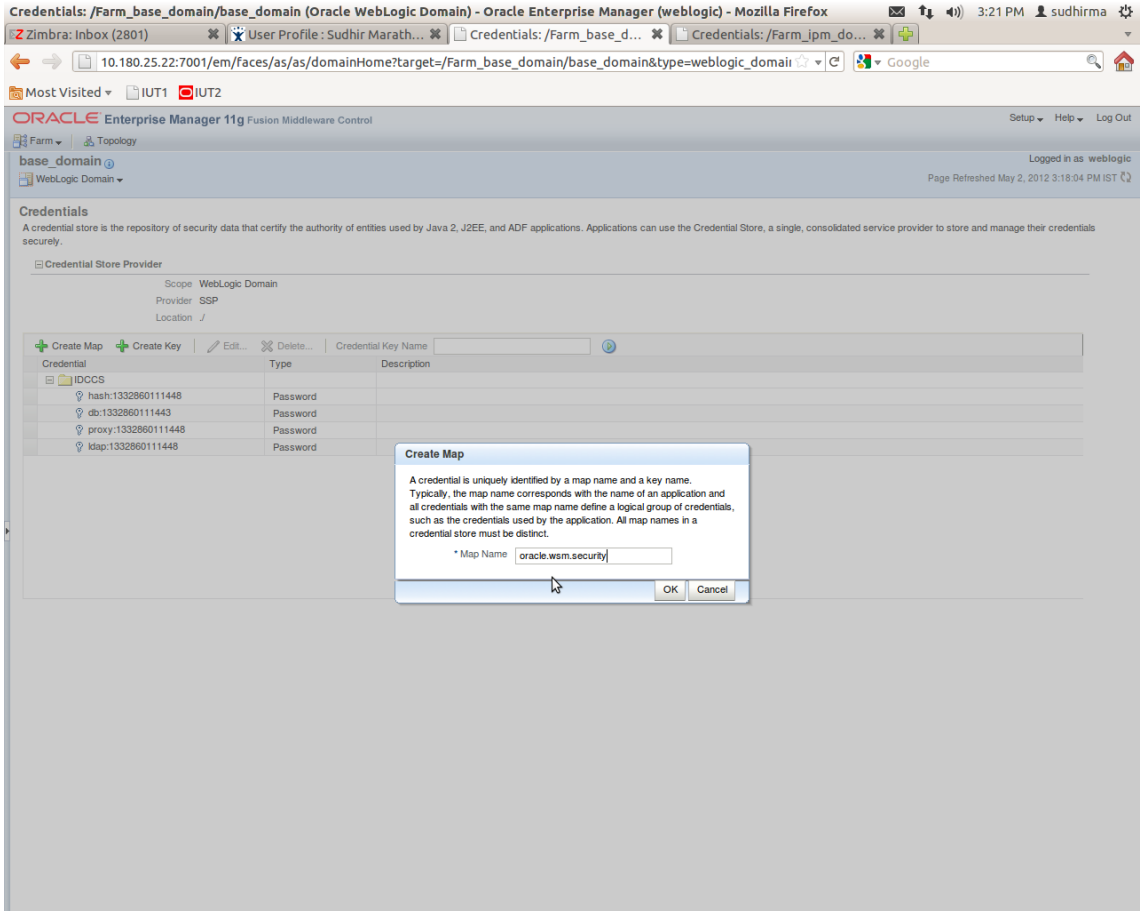
3. In the top menu, click **Weblogic Domain.** The corresponding menu appears.
4. Navigate to **Security > Credentials.** The Credentials page appears.

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



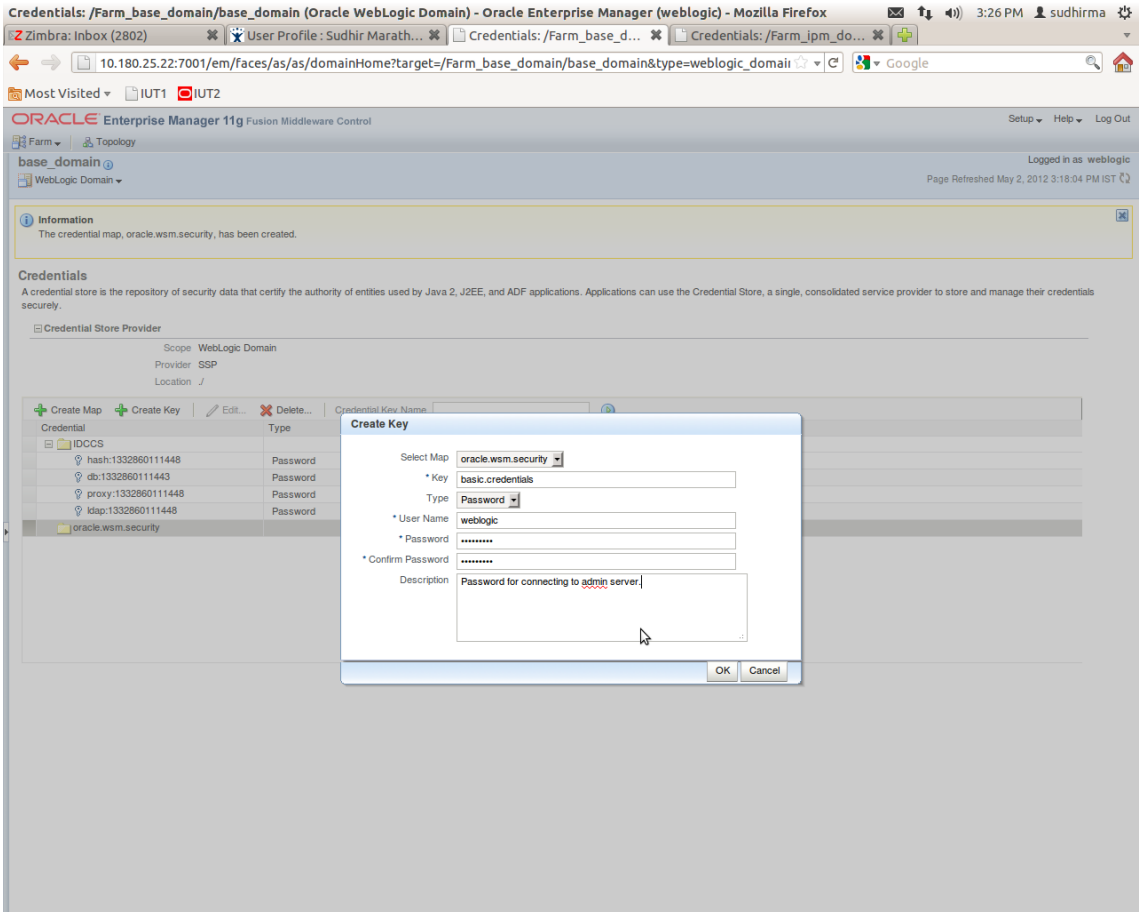
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 7–65 Create Map oracle.wsm.security



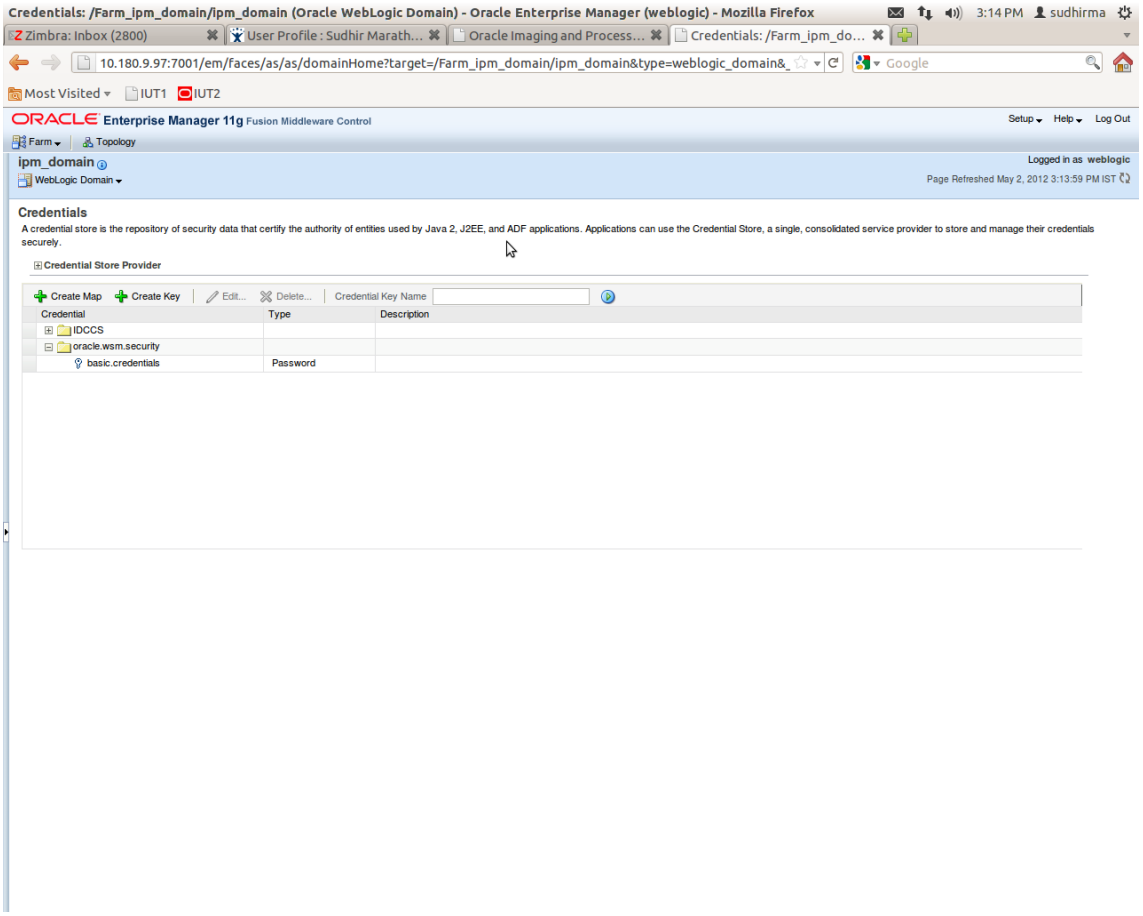
6. Click **Create Key** to create a key under the map **oracle.wsm.security.**

Figure 7–66 Create Key: basic.credentials



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

Figure 7–67 ipm_domain: Credentials Created

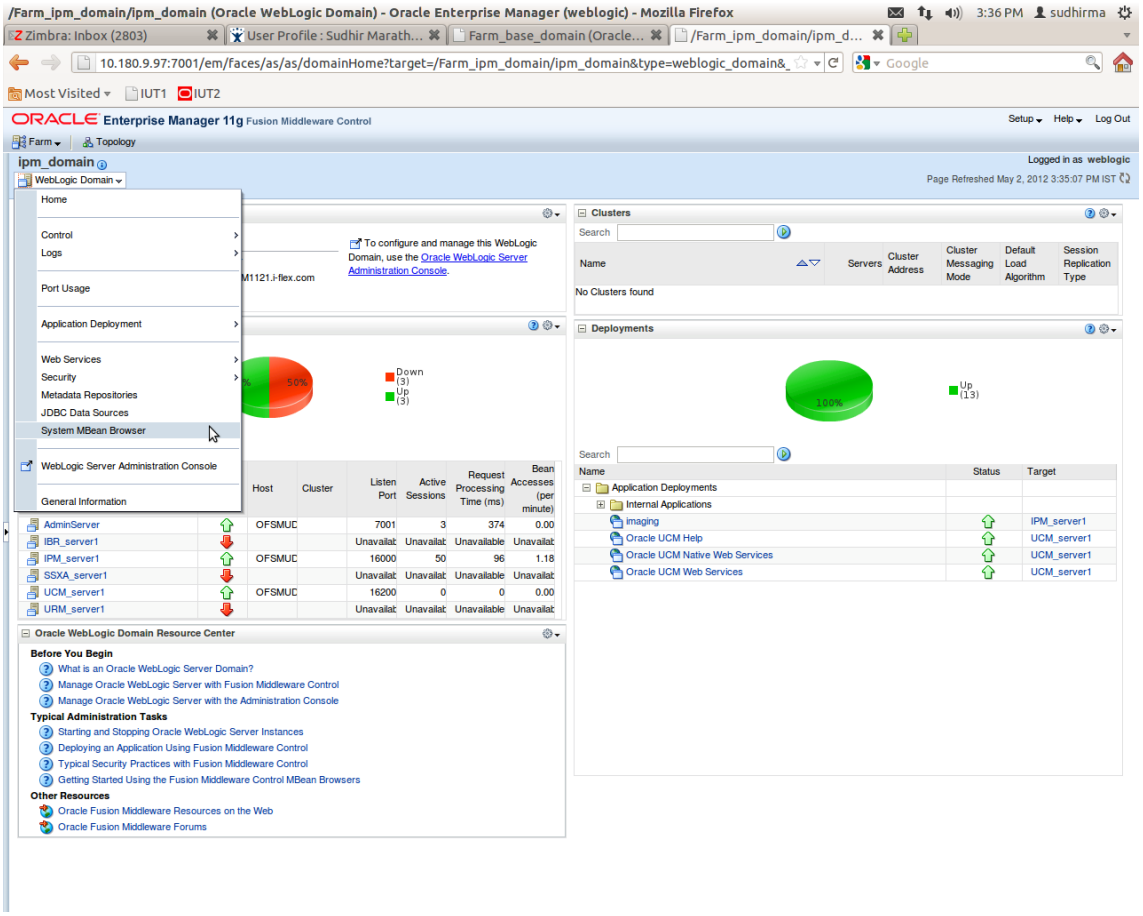


7.3.3 Setting up Input Agent Path

To set up input agent path:

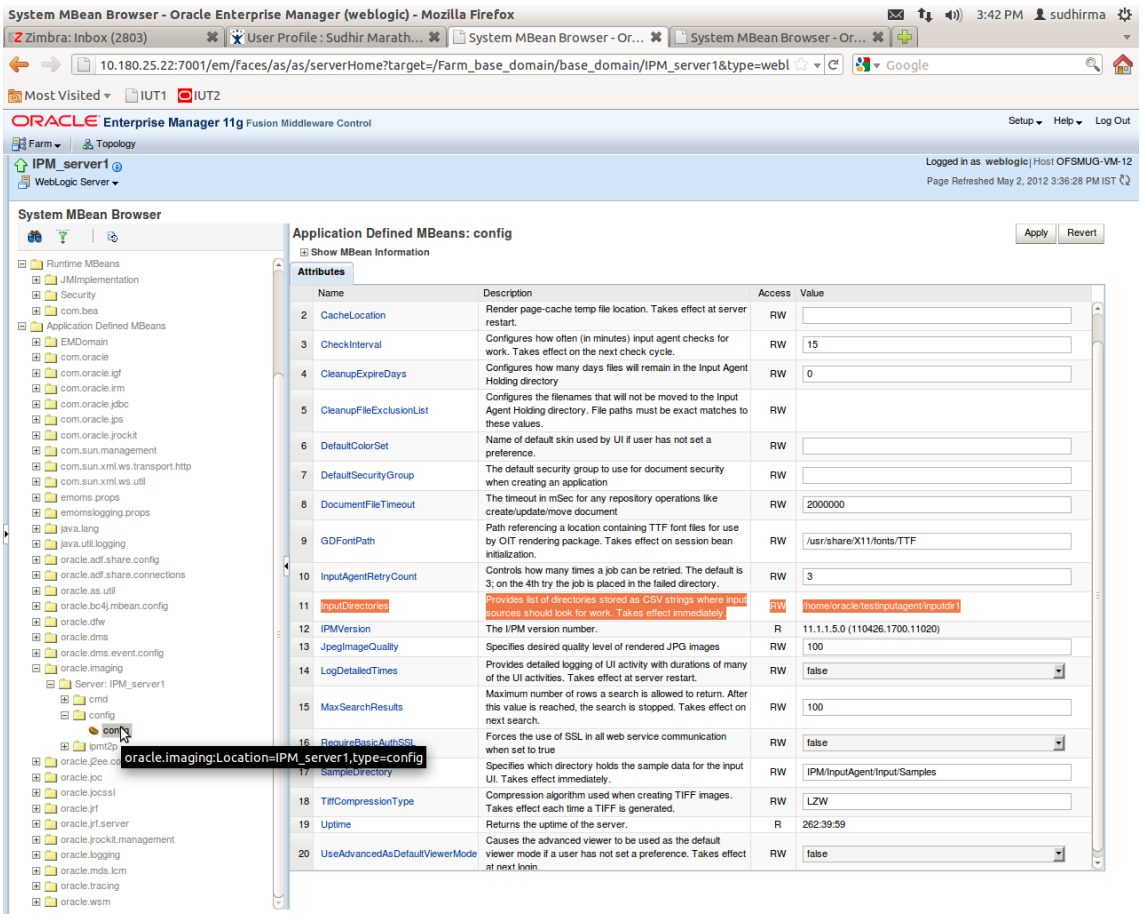
1. Log in to Enterprise Manager (EM) console.
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain**.
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

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



5. In the left hand pane, navigate to **Application Defined MBeans > oracle.imaging > Server: IPM_ server1 > config.**
6. For the attribute InputDirectories, in the **Value** column enter the value to set the path for input agents.
7. Change the highlighted path value to /scratch/ofssobp/testinputagent/inputdir1.

Figure 7–69 InputDirectories: Enter Input Agent Path



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

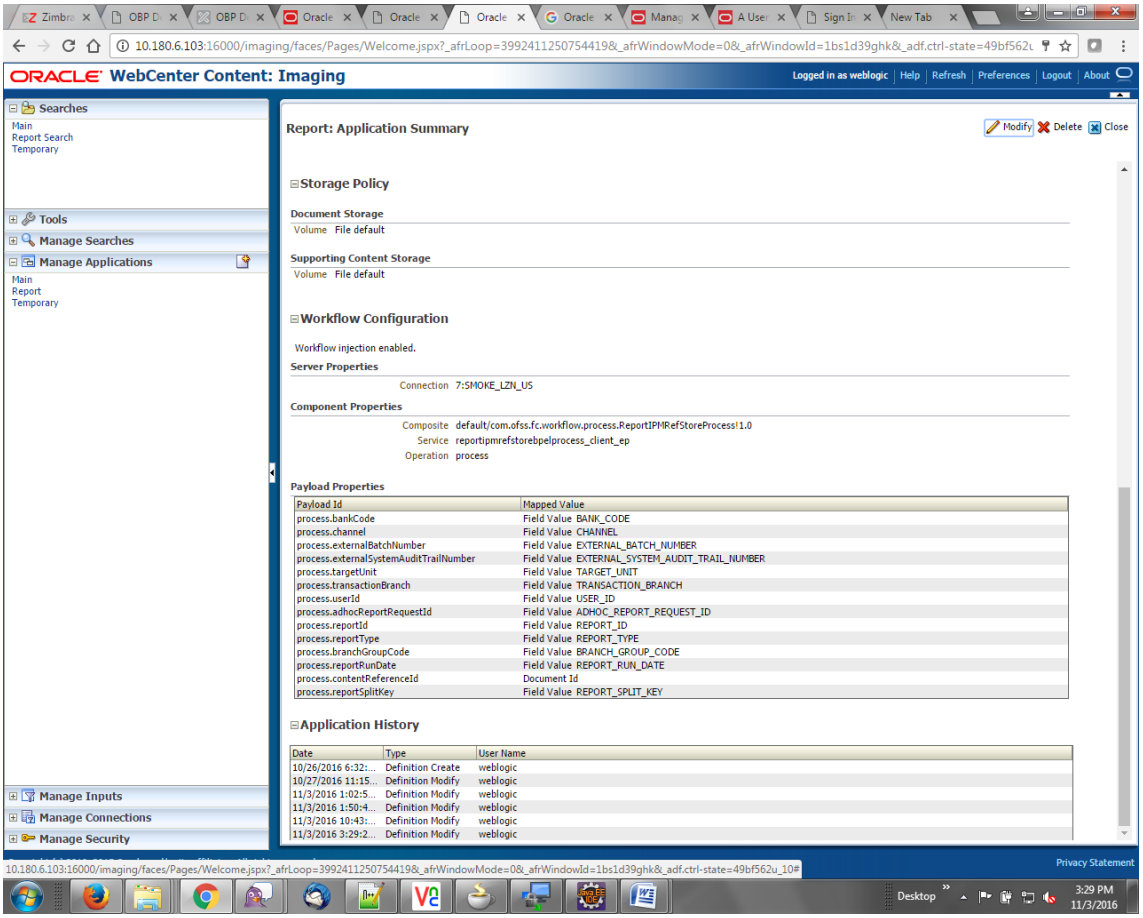
8. Restart IPM server.

7.3.4 Create SOA Connection

To create a SOA Connection:

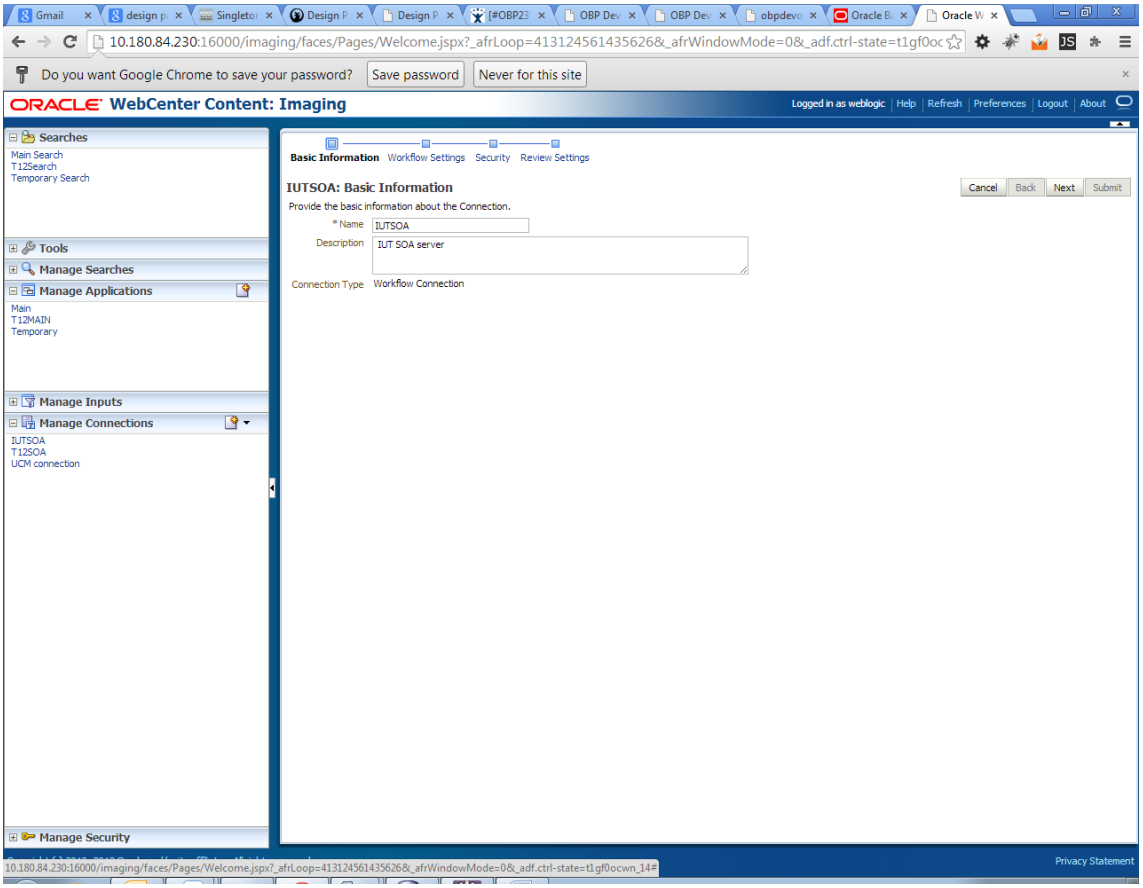
1. Log in to Image Processing Management (IPM).
2. Navigate to the Manage Connections section.

Figure 7–70 Manage Connections: Create Workflow Connection



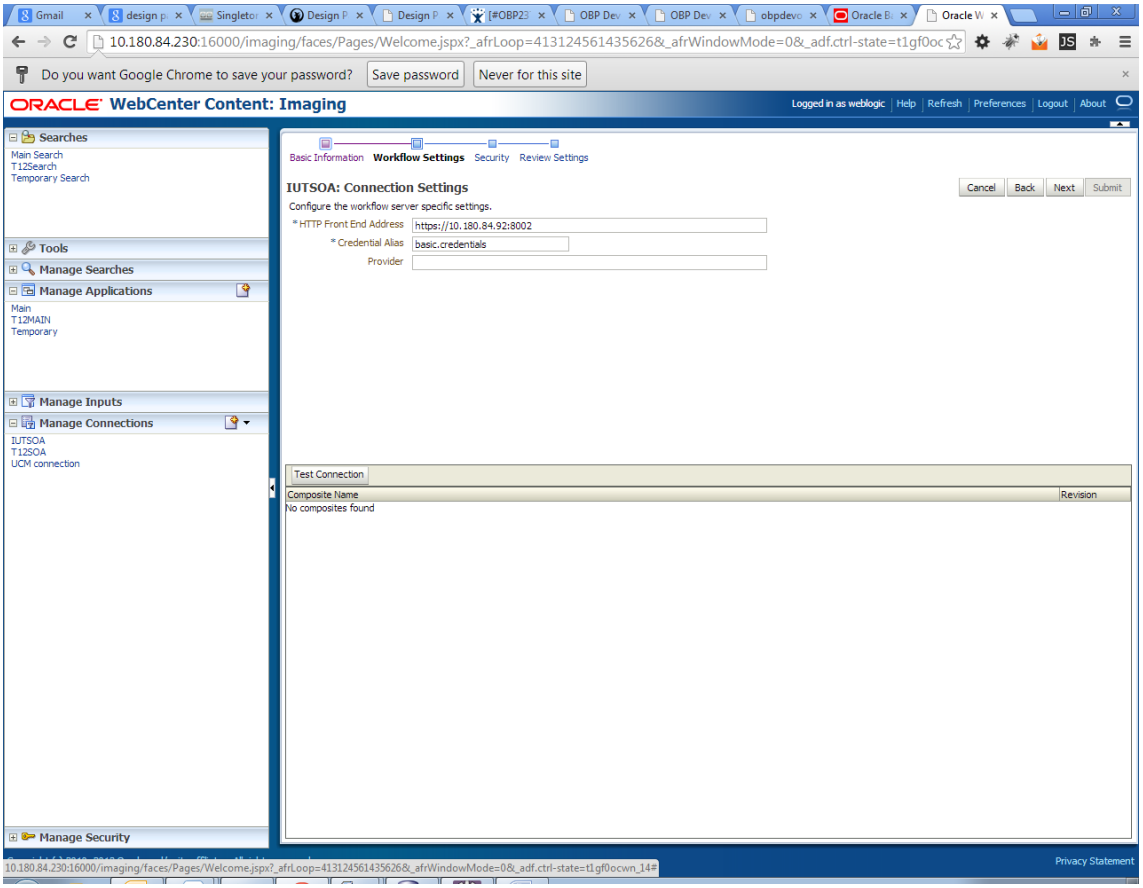
3. Click **Create Workflow Connection.**
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 7–71 IUTSOA: Basic Information



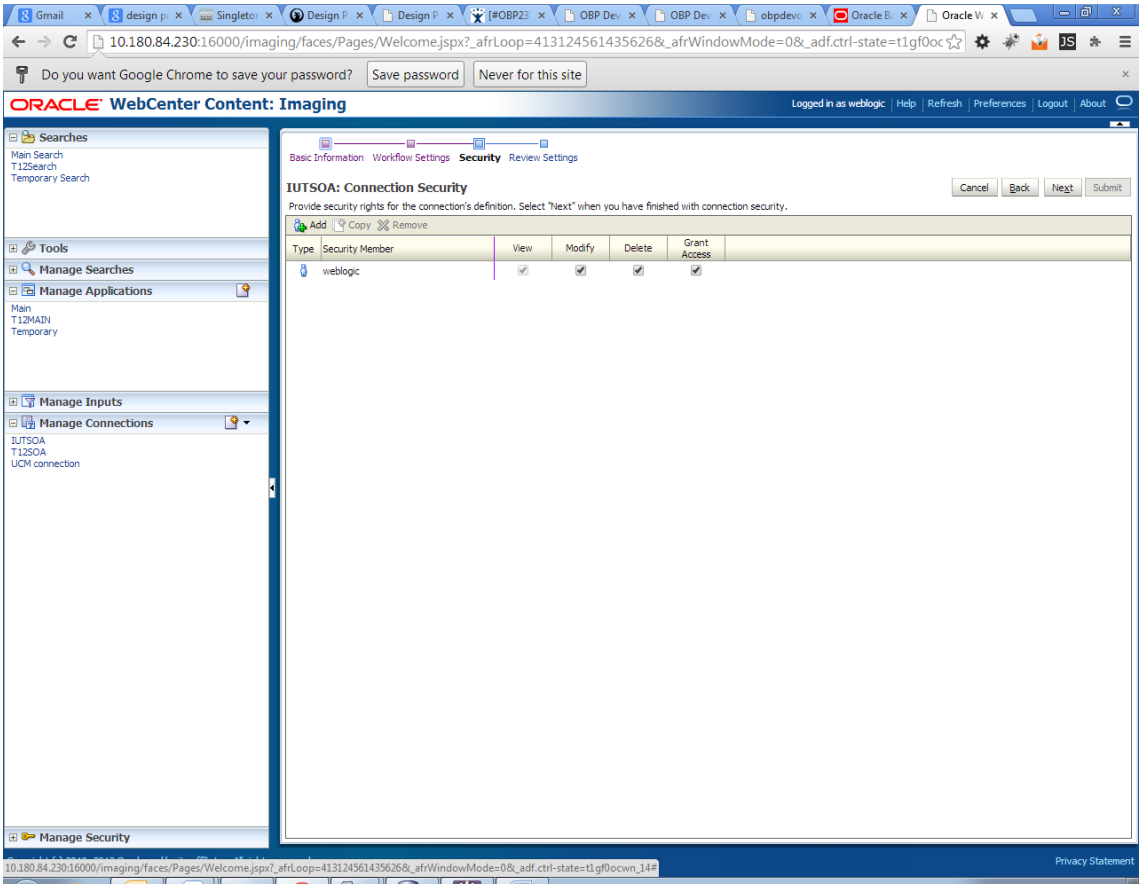
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 7–72 IUTSOA: Workflow Settings



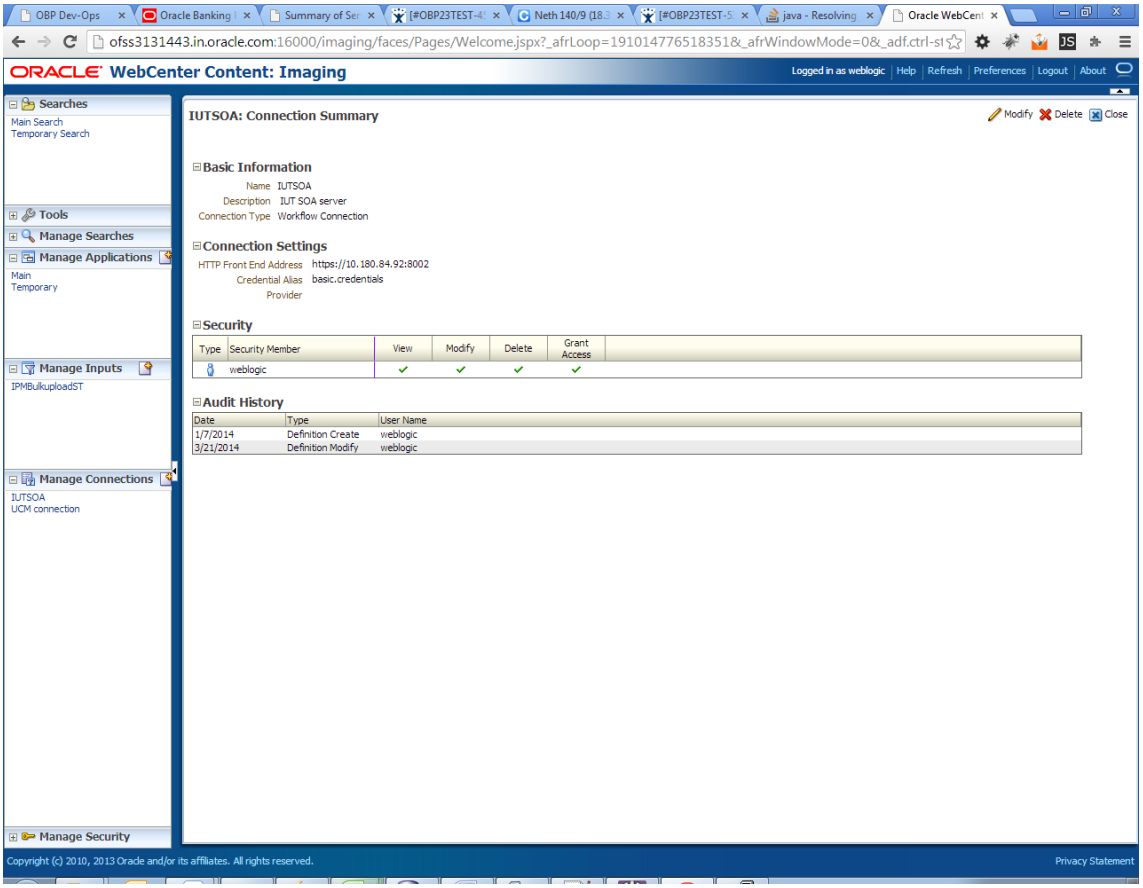
6. In the **Credential Alias** field, enter the value as basic.credentials.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 7–73 IUTSOA: Connection Security



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

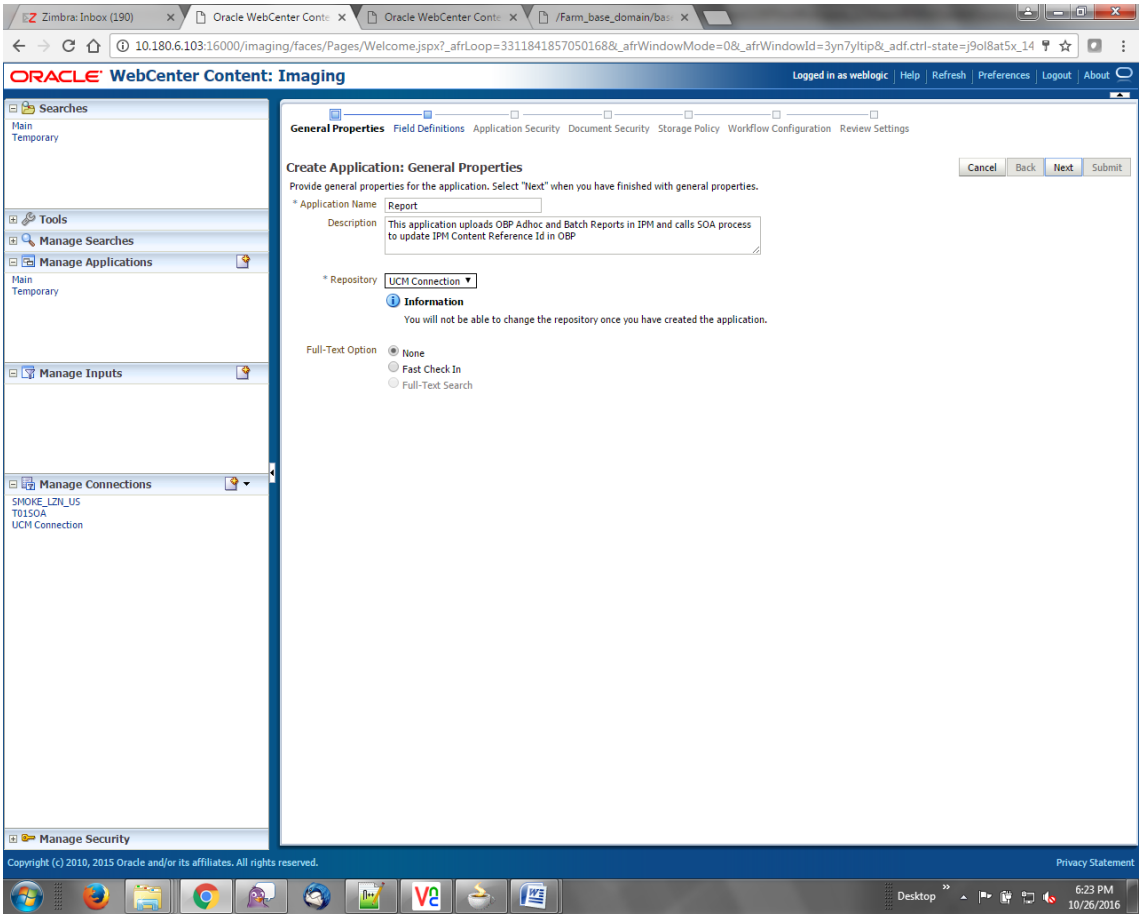
Figure 7–74 IUTSOA: Review Settings



7.3.5 Manage Application Configuration

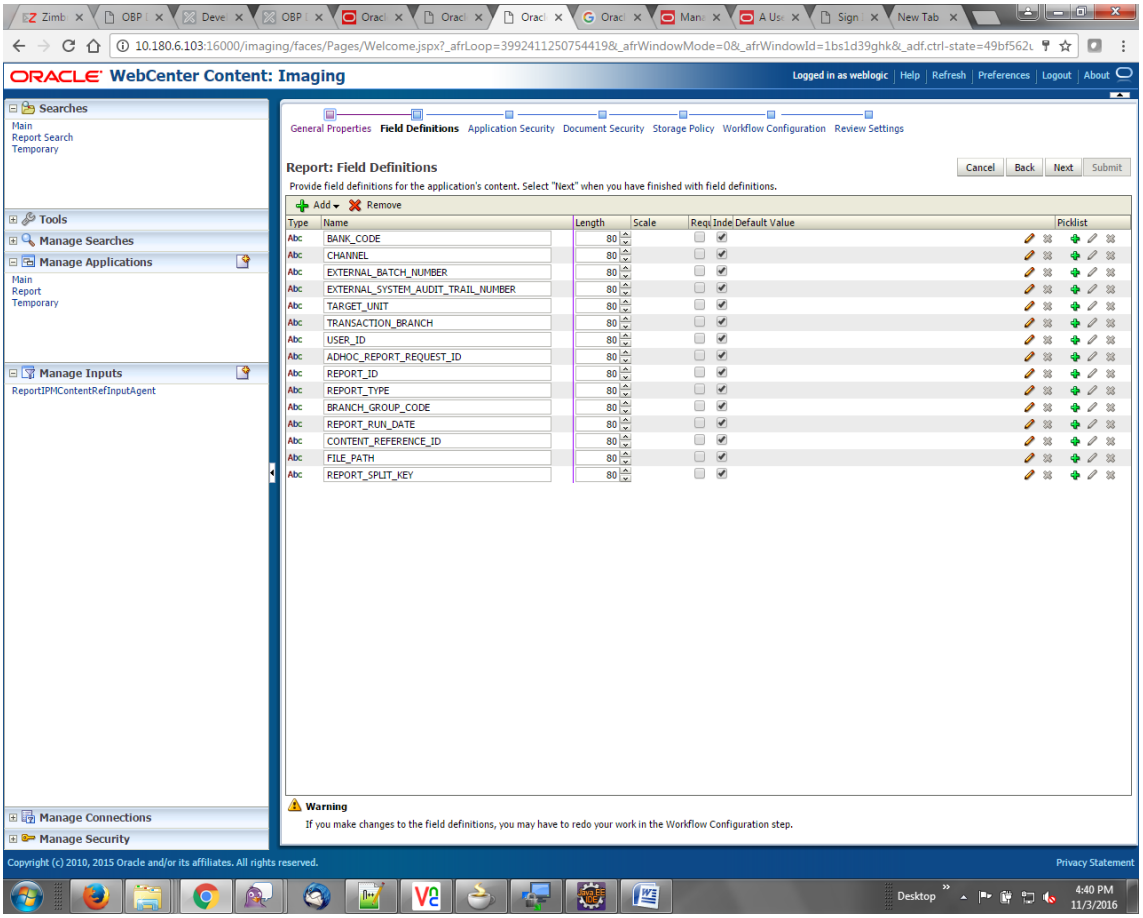
1. Navigate to the Manage Applications section.
2. Select Create New Application option. The Create Application: General Properties page appears.

Figure 7–75 Create Application: General Properties



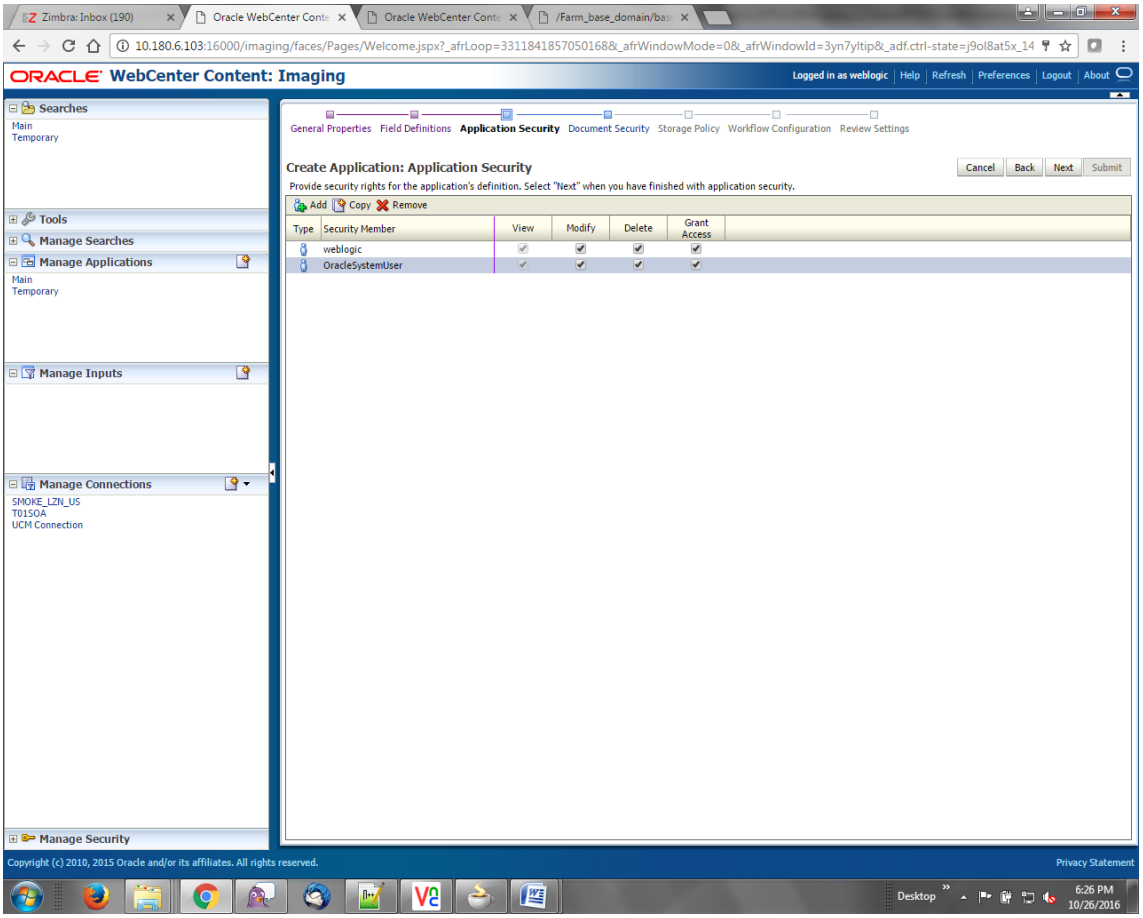
3. Enter the general properties for the application and click **Next.** The Report: Field Definitions page appears.

Figure 7–76 Report: Field Definitions



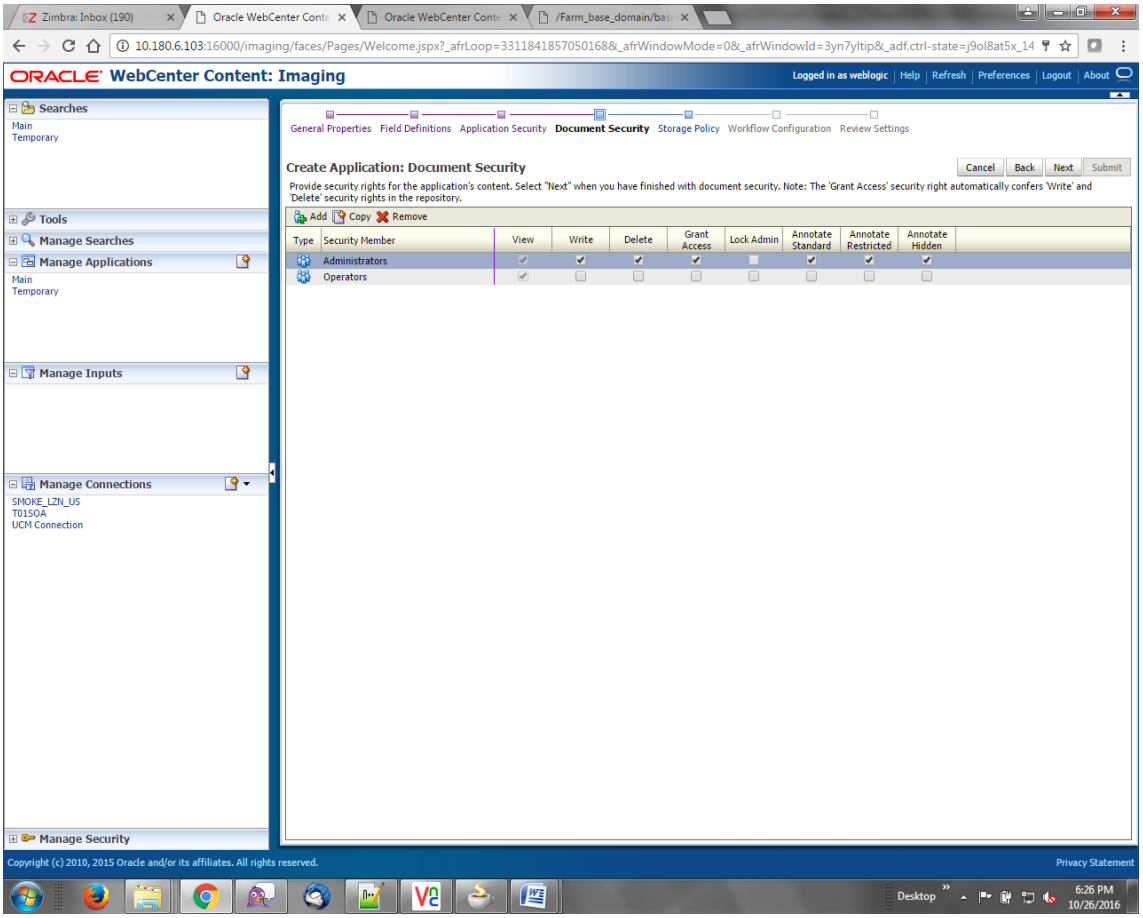
4. Enter the field definition details and click **Next.** The Create Application: Applications Security page appears.

Figure 7–77 Create Application: Applications Security



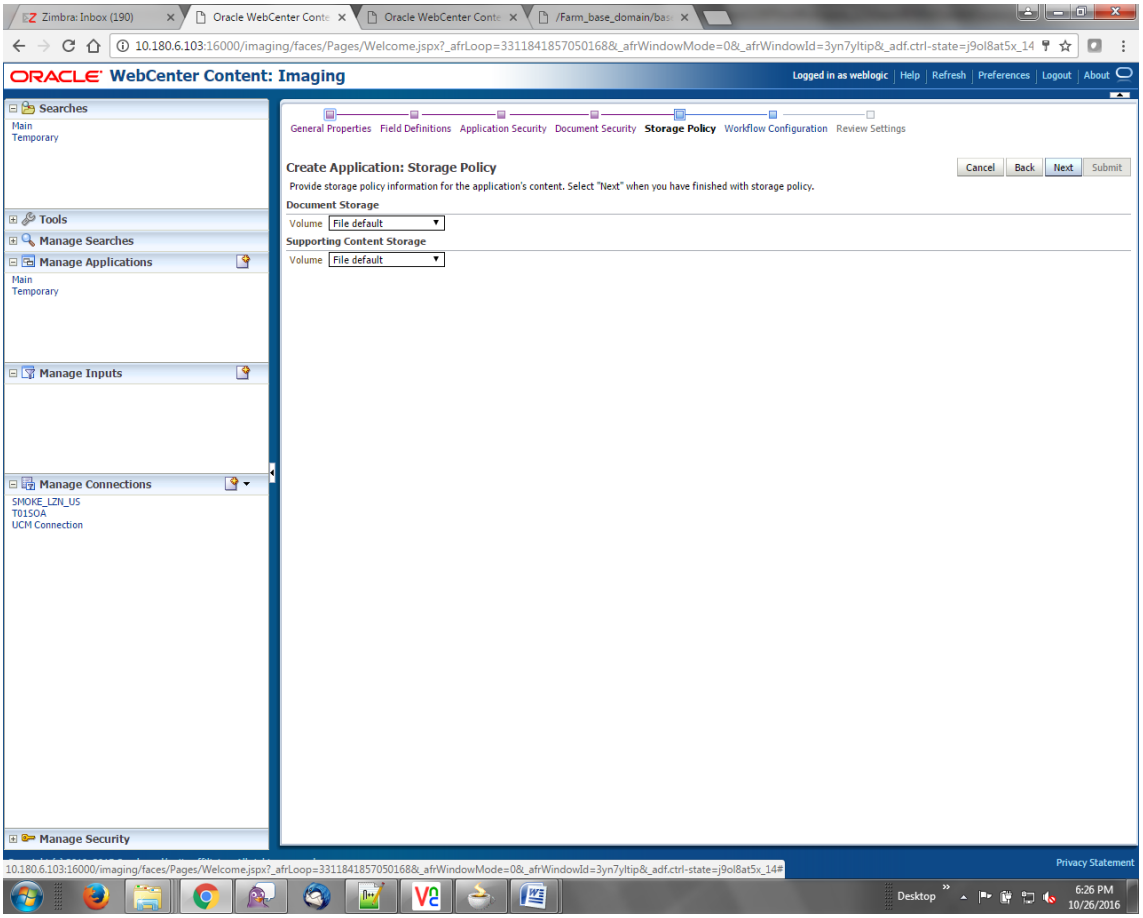
5. In the Application Security section, select the access rights for users and click **Next.** The Create Application: Document Security page appears.

Figure 7–78 Create Application: Document Security



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

Figure 7–79 Create Application: Storage Policy



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

Figure 7–80 Report: Workflow Configuration - Server Properties

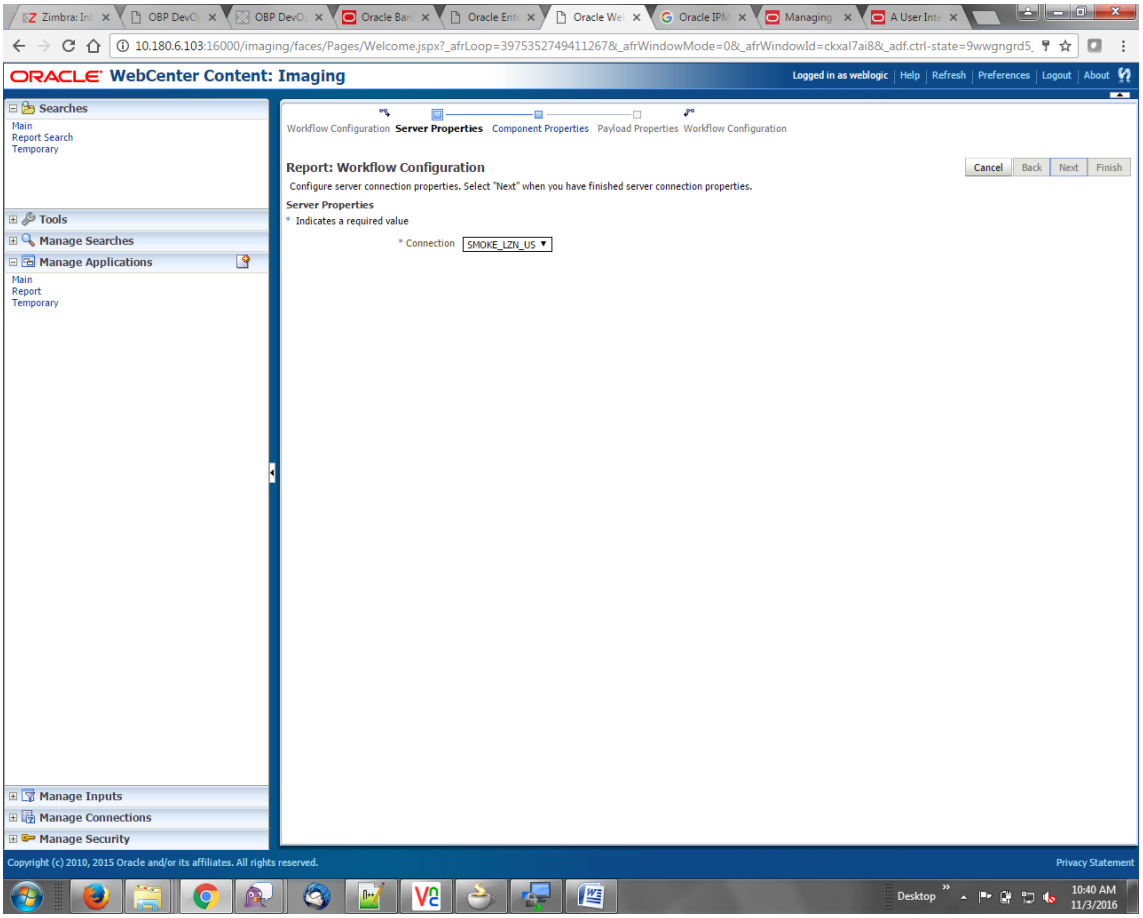


Figure 7–81 Report: Workflow Configuration - Component Properties

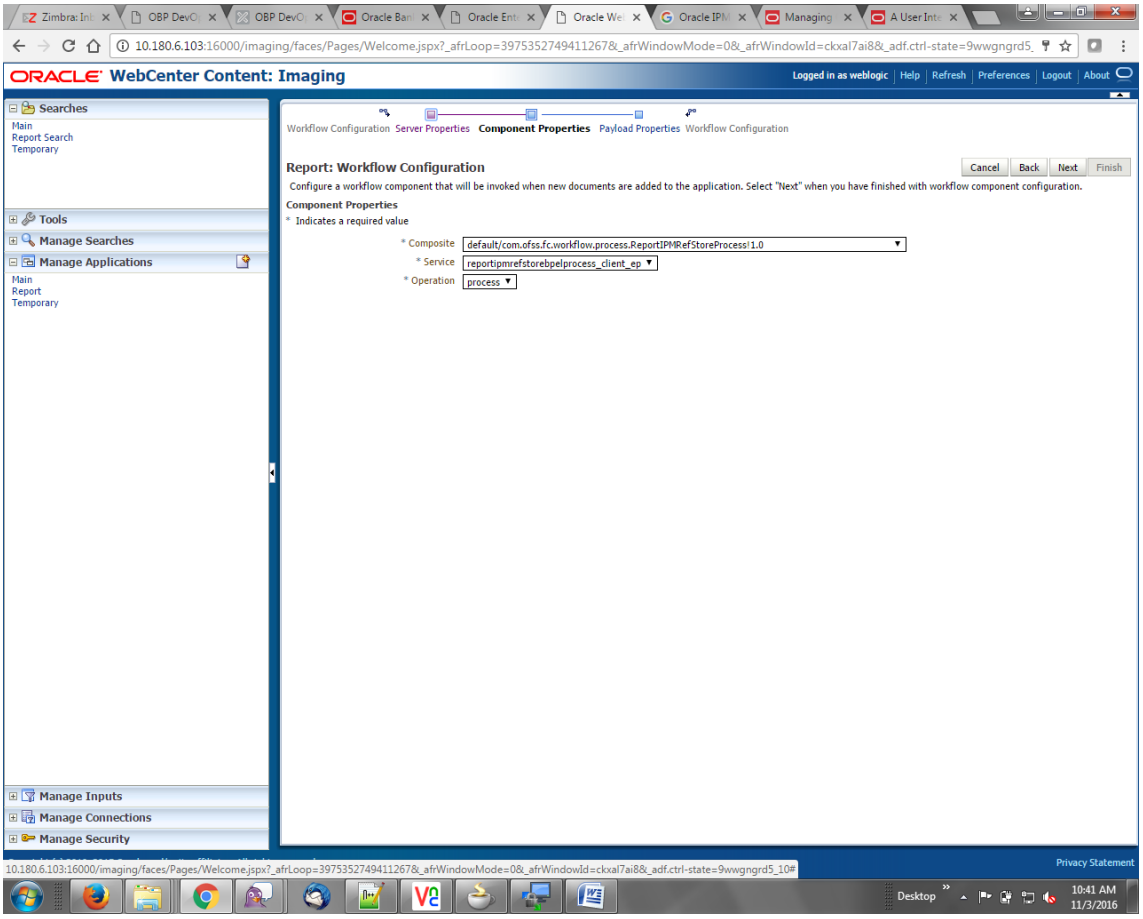
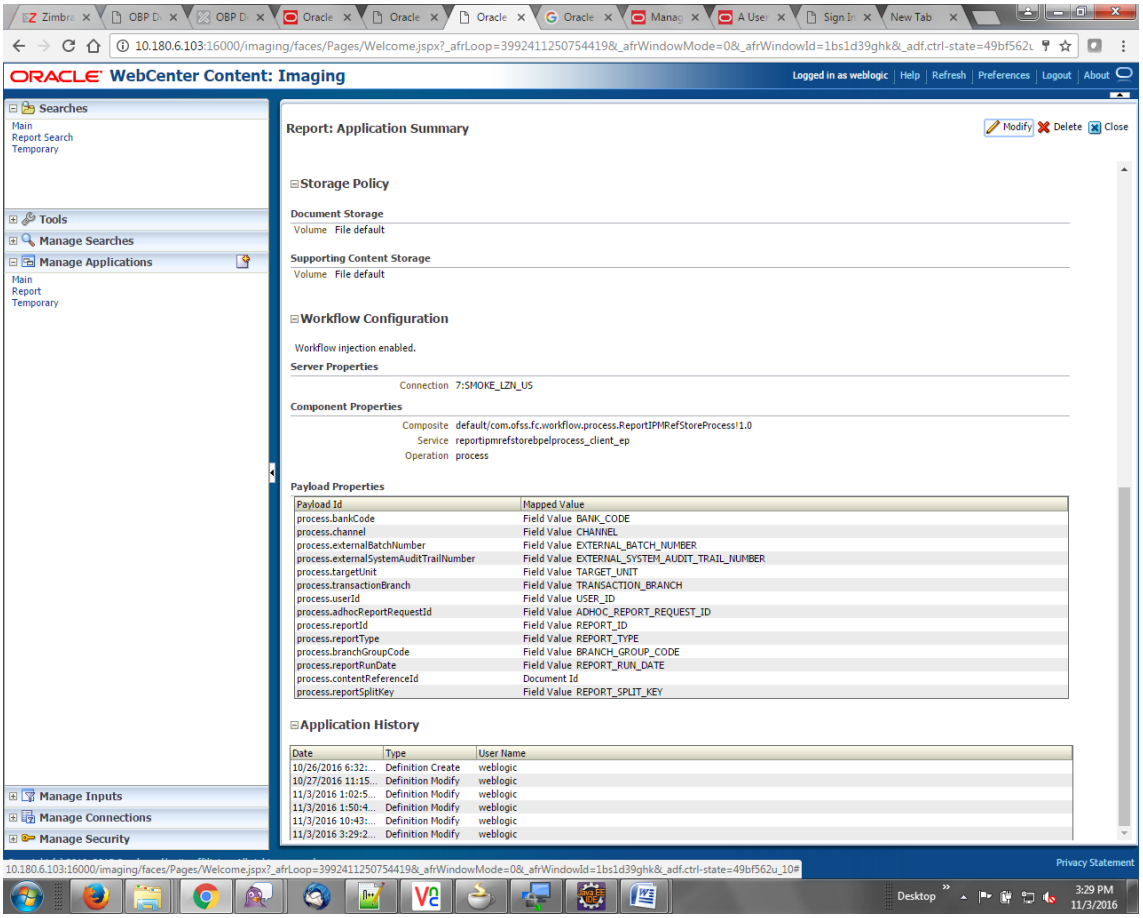
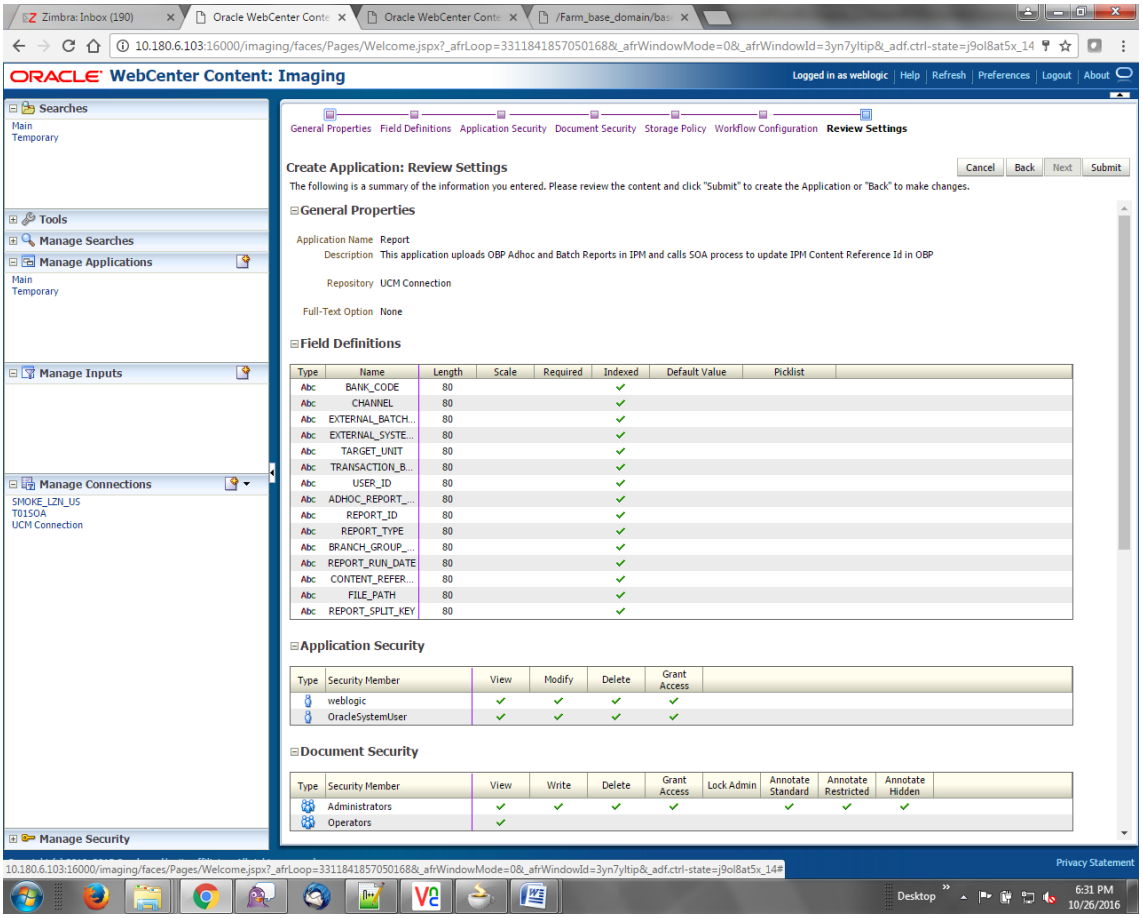


Figure 7–82 Report: Application Summary



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

Figure 7–83 Create Application: Review Settings

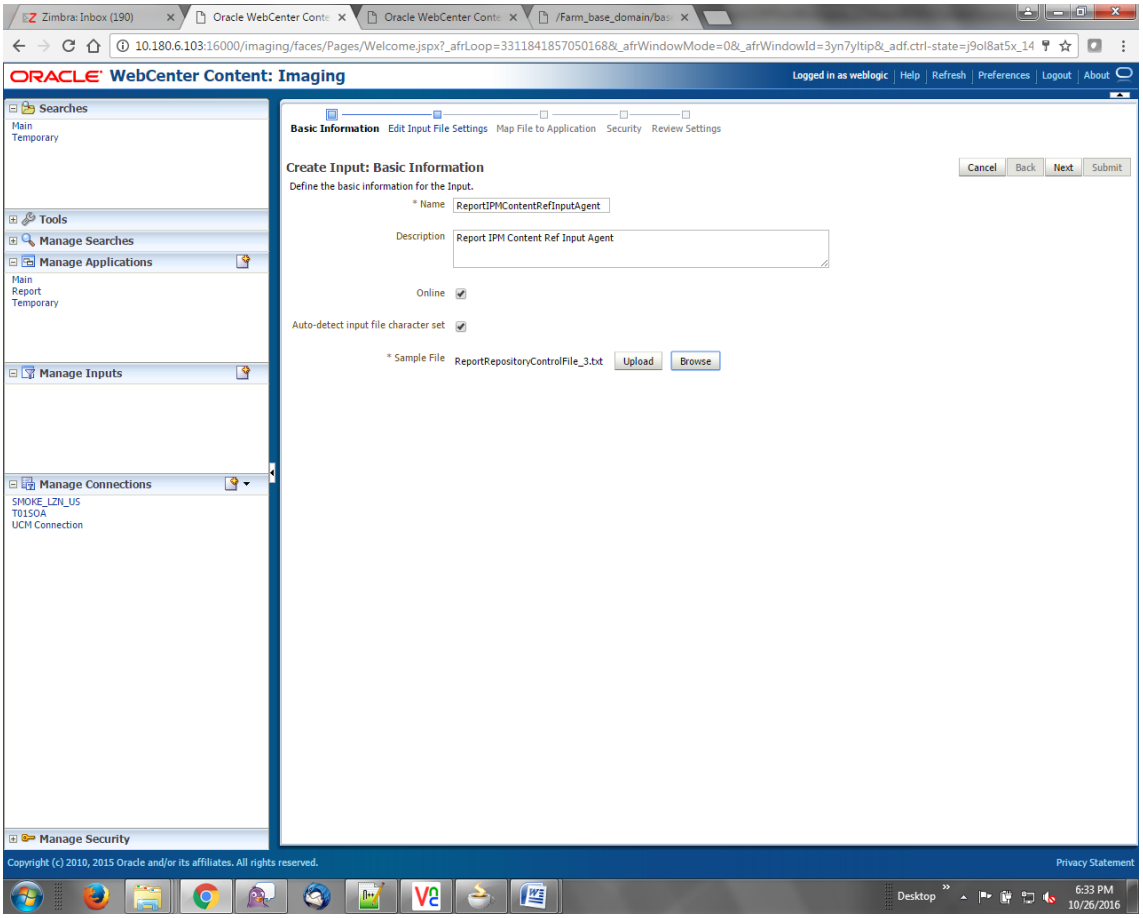


7.3.6 Manage Inputs for Input Agents

To manage workflow configuration:

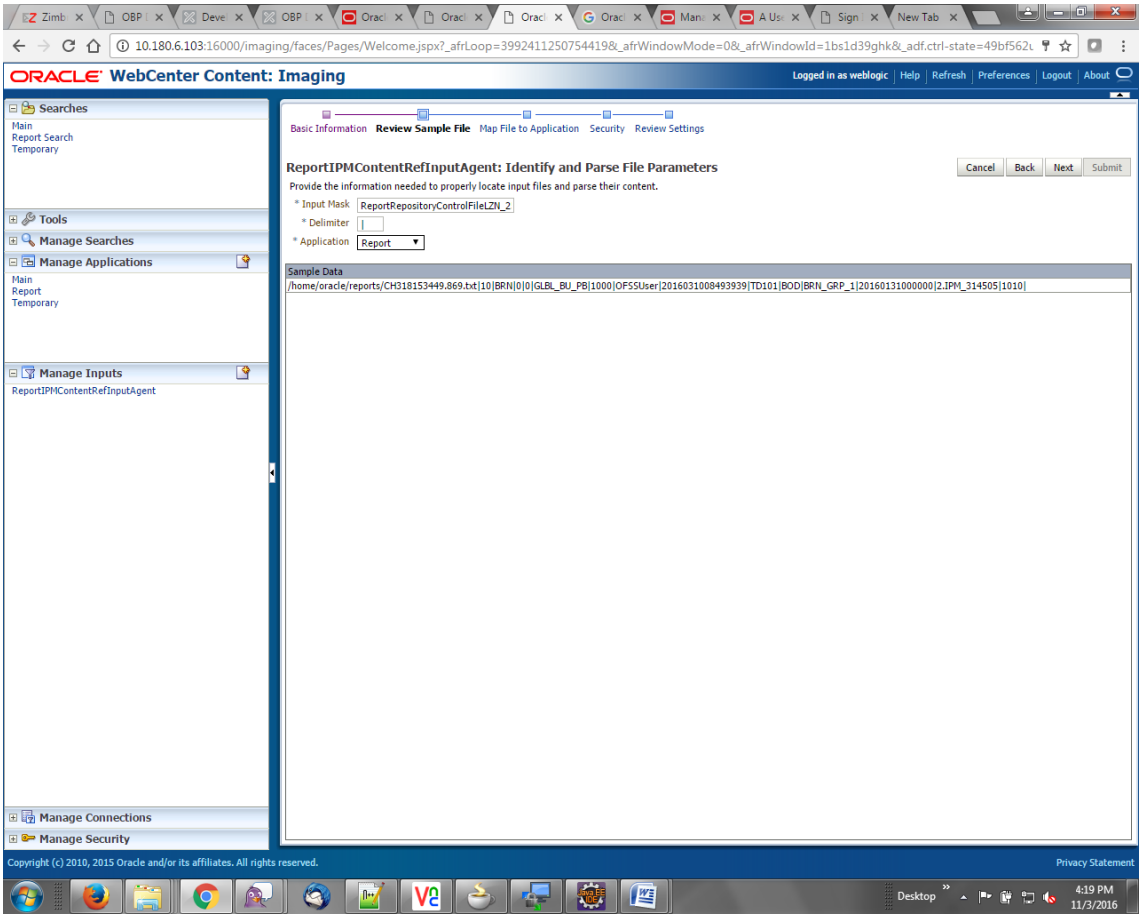
1. Log in to Image Processing Management (IPM).
2. Navigate to Manage Inputs section.

Figure 7–84 Manage Inputs



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

Figure 7–85 Input Agent Details: Input Mask



5. Upload the sample file.

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

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

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

   flx_fw_config_all_b

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

   appended with name given in table flx_fw_config_var_b

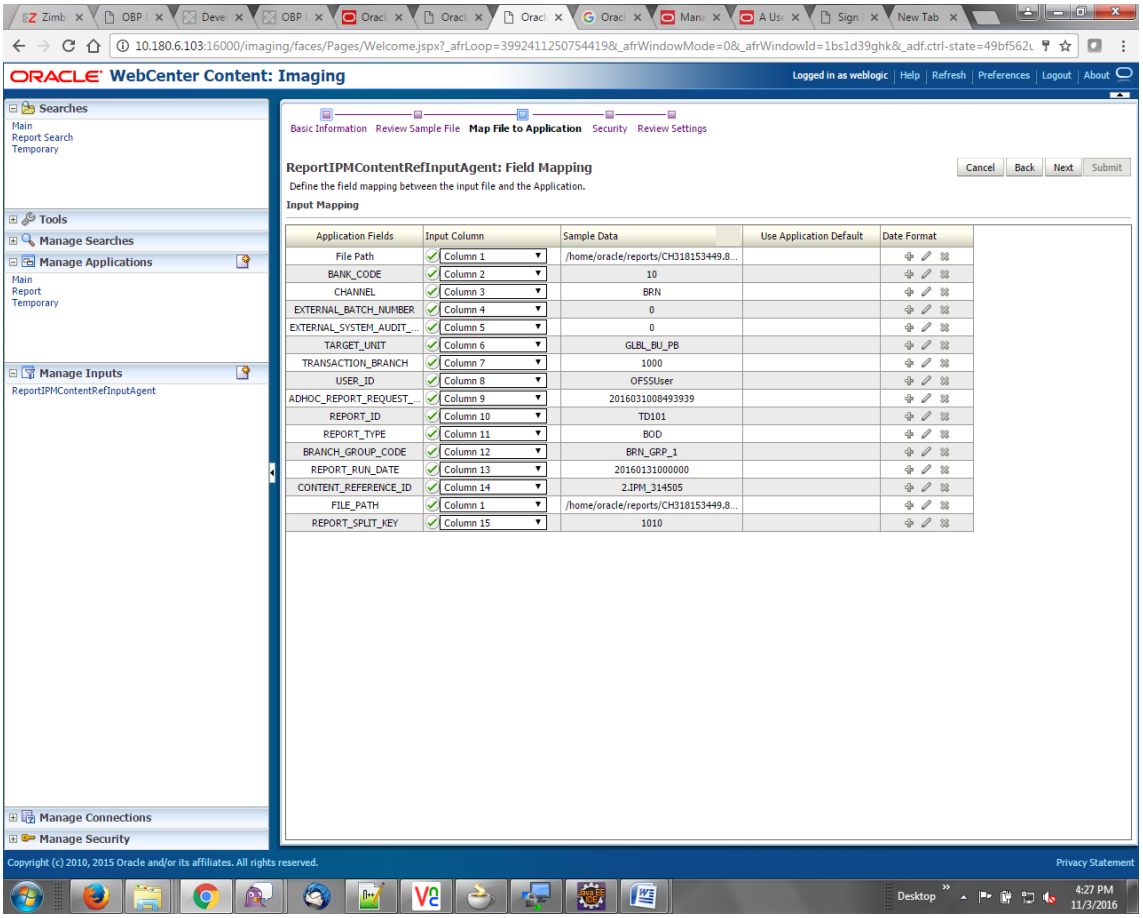
   select prop_value from flx_fw_config_var_b where prop_id = env.name;

Note

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

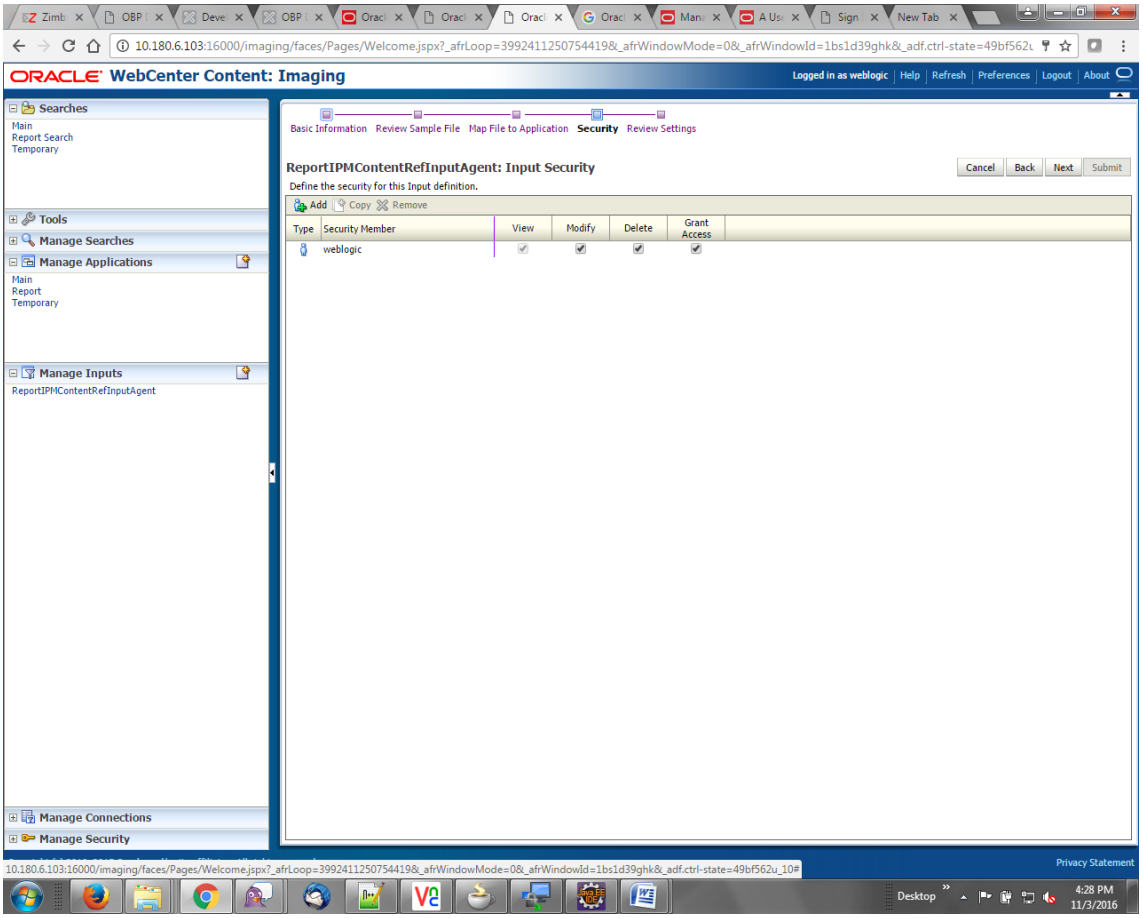
7. In the **Delimeter** field, enter the delimiter value as | (vertical bar character).
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 7–86 Input Agent Details: Field Mapping



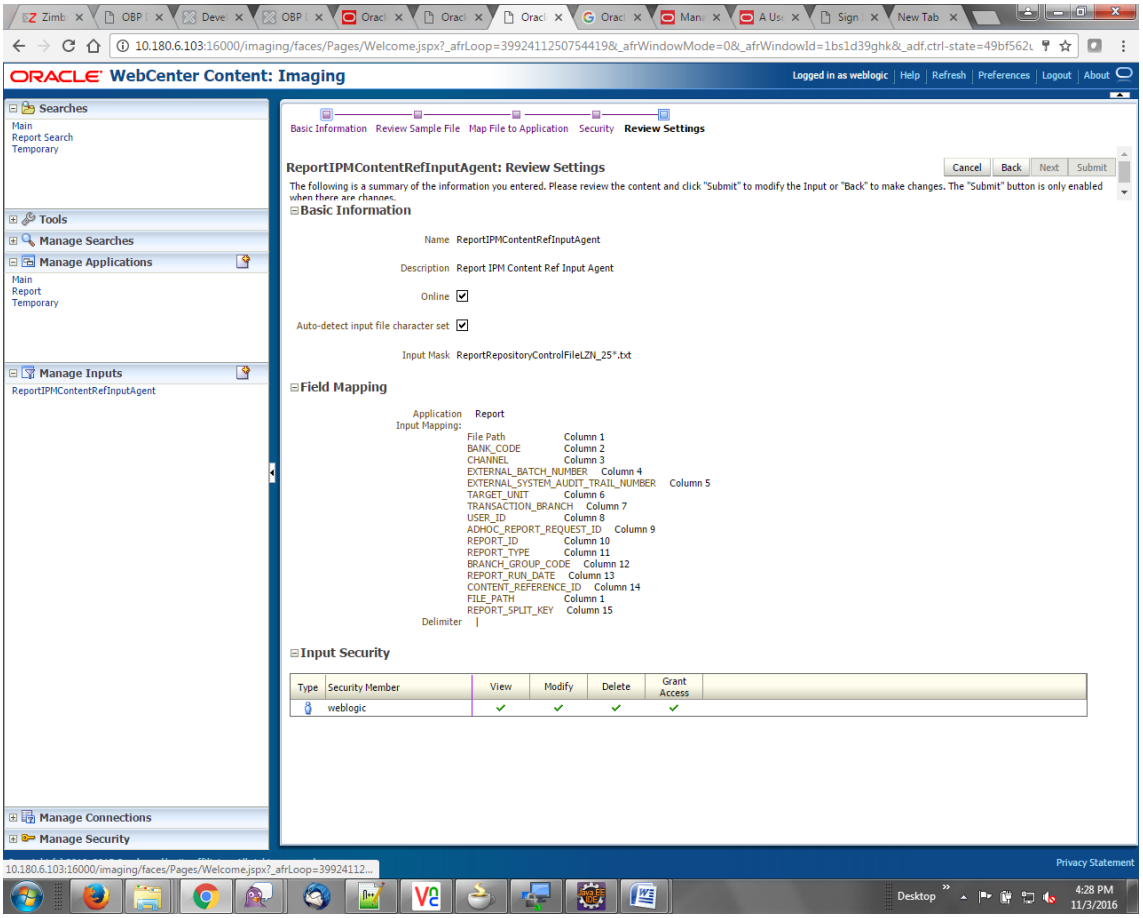
9. Select the access rights for user in the Security section and click **Next.**

Figure 7–87 Input Agent Details: Security



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

Figure 7–88 Input Agent Details: Review Settings



Note

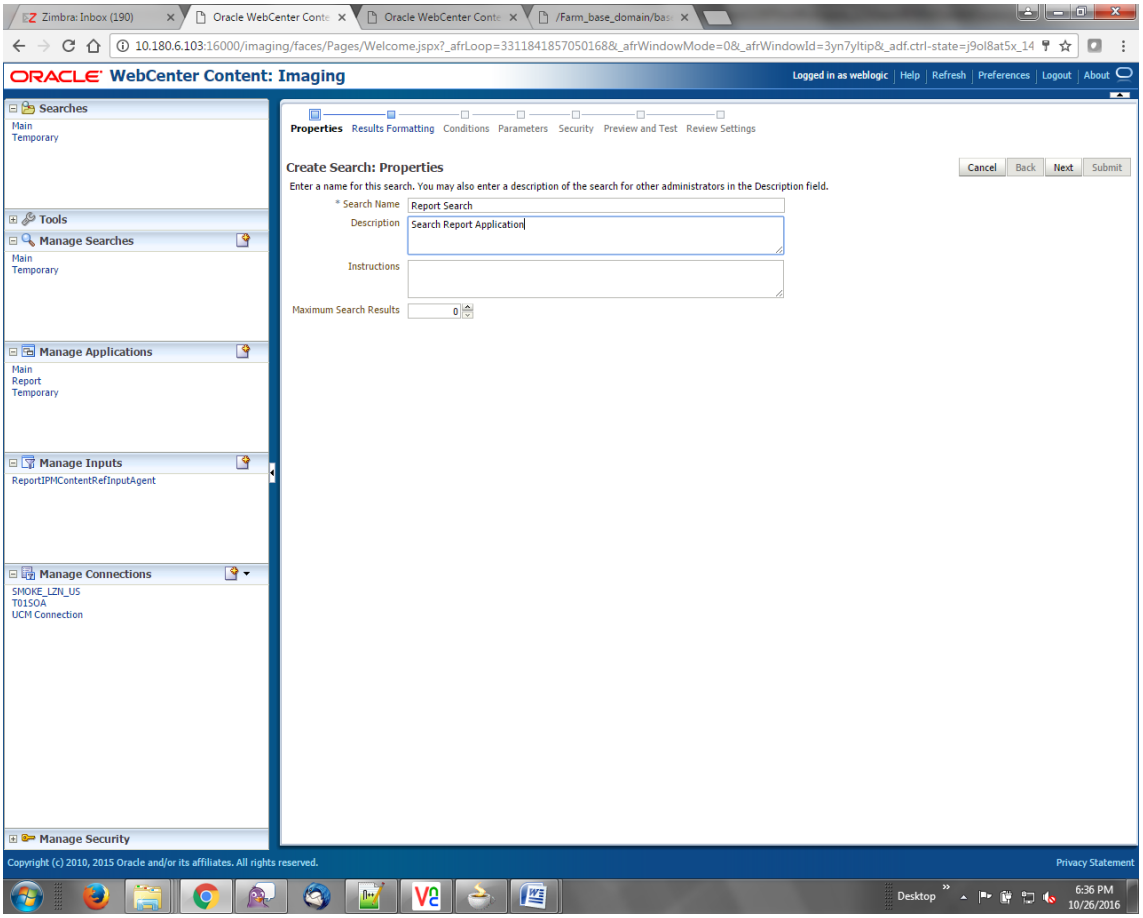
Do not forget to toggle online, else the input agent will not pick up any file for processing.

7.3.7 Manage Searches

To manage searches:

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

Figure 7–89 Create Search: Properties



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

Figure 7–90 Create Search: Results Formatting

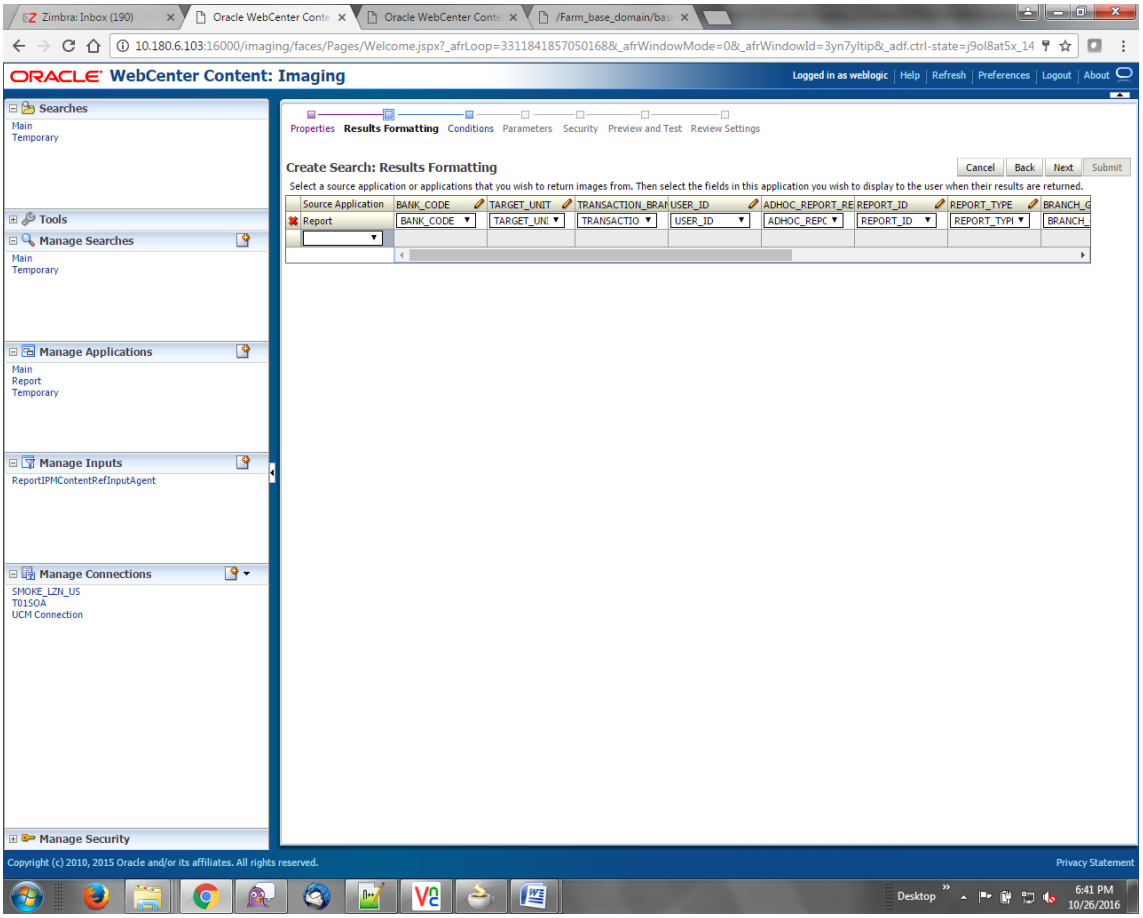


Figure 7–91 Create Search: Conditions

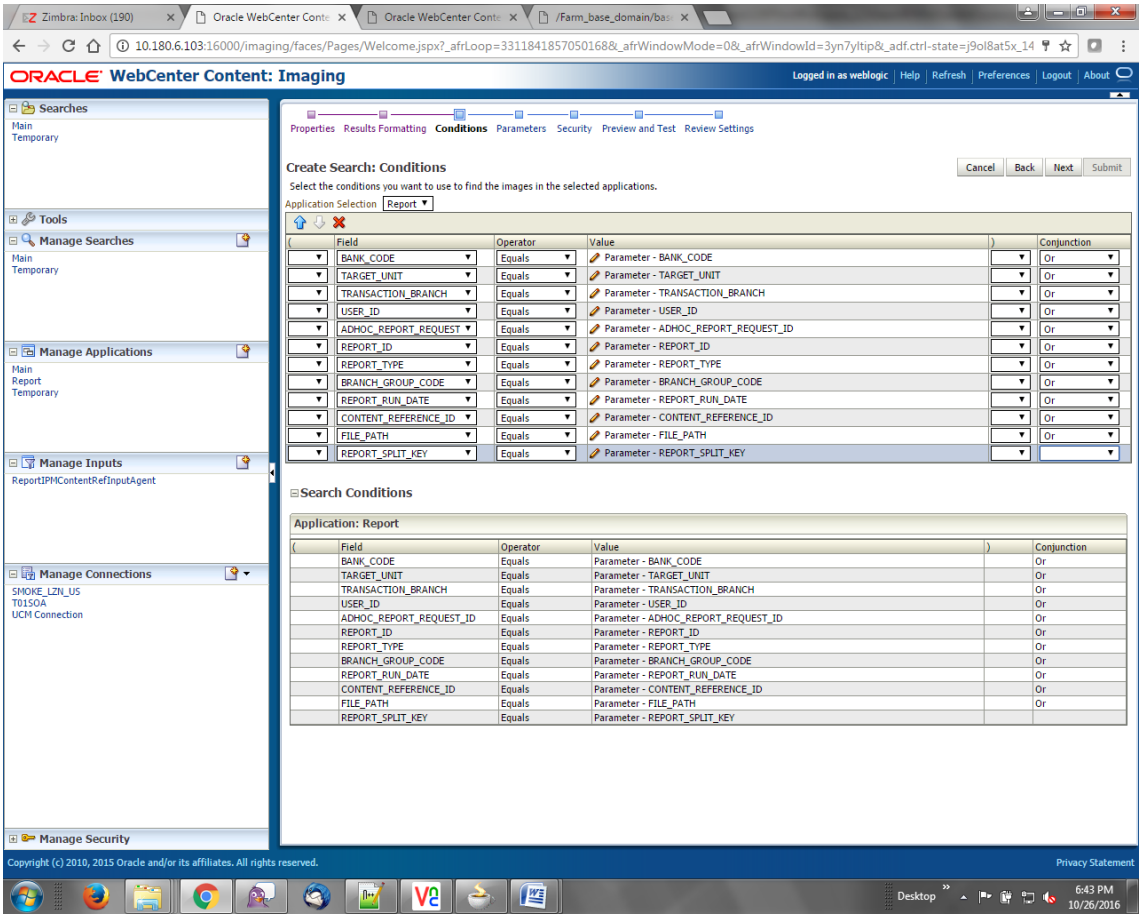
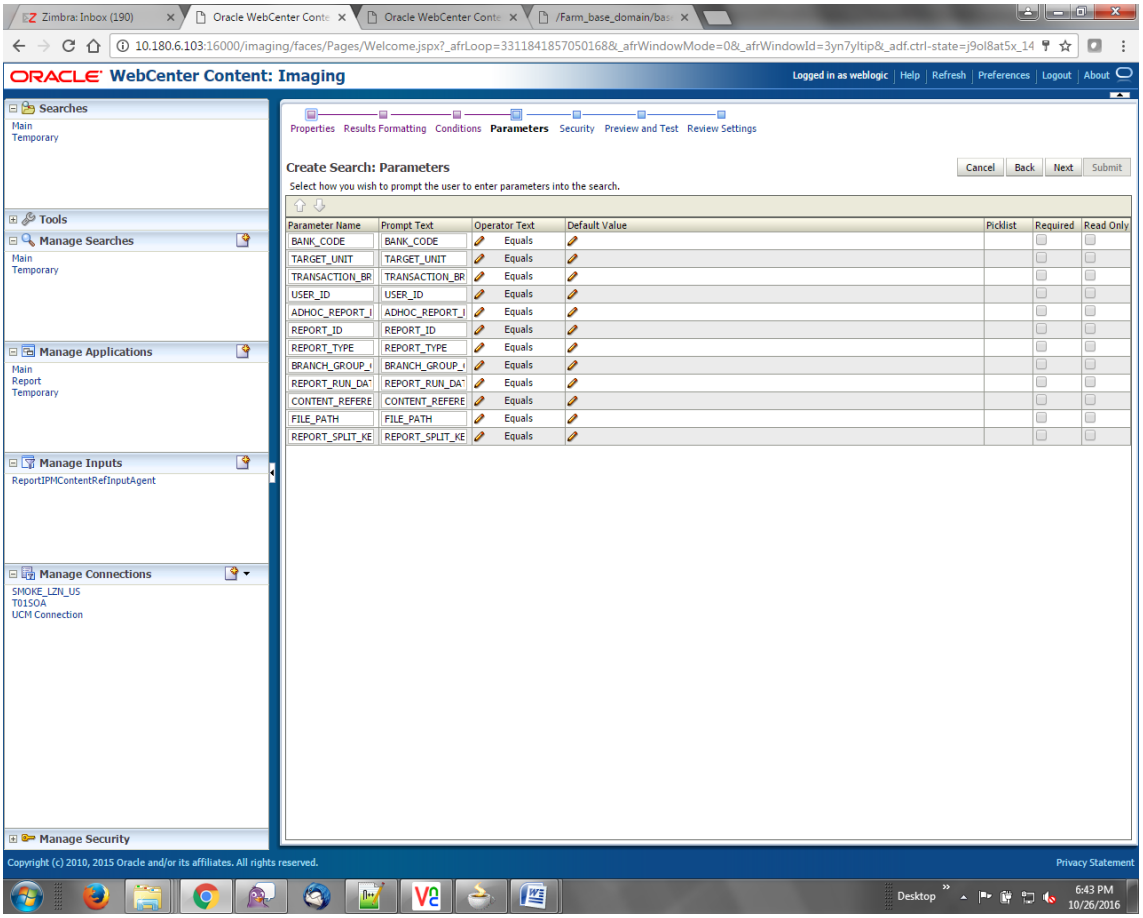
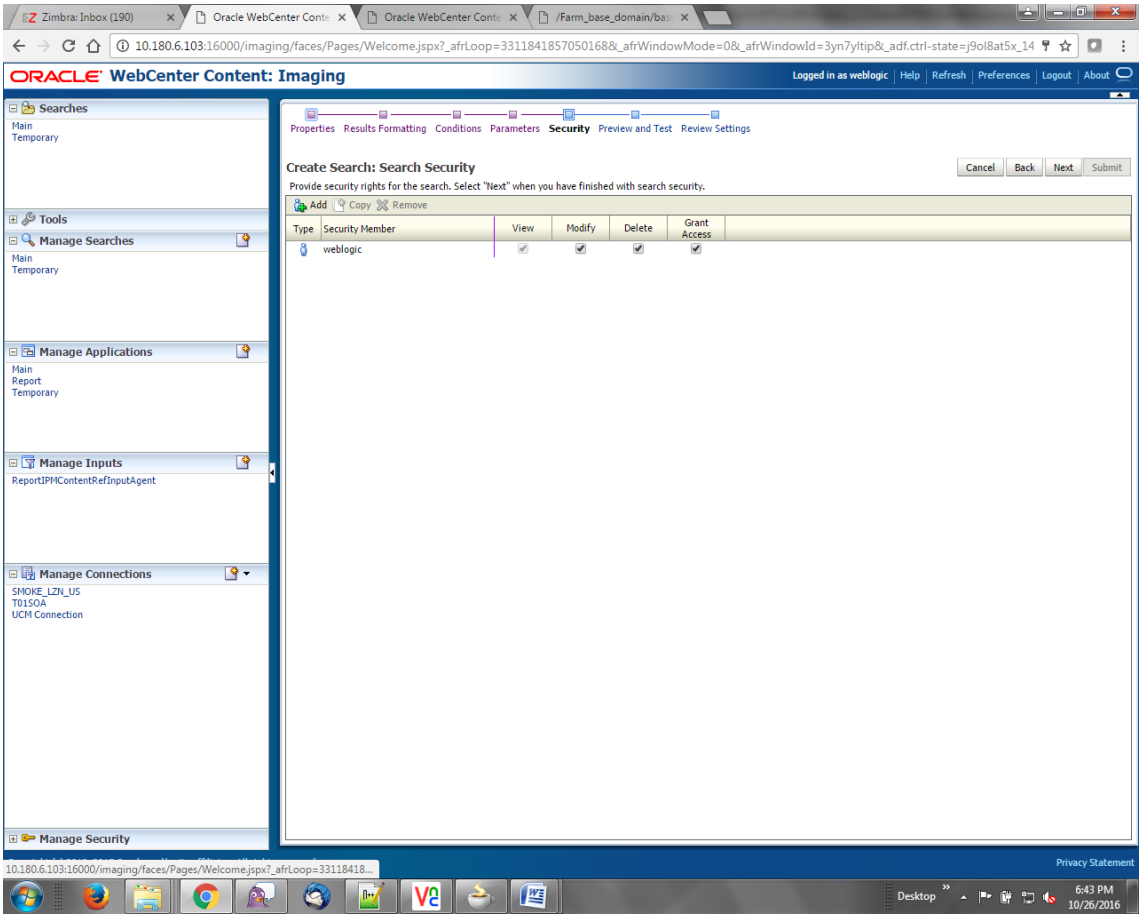


Figure 7–92 Create Search: Parameters



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

Figure 7–93 Create Search: Security



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

Figure 7–94 Create Search: Preview and Test

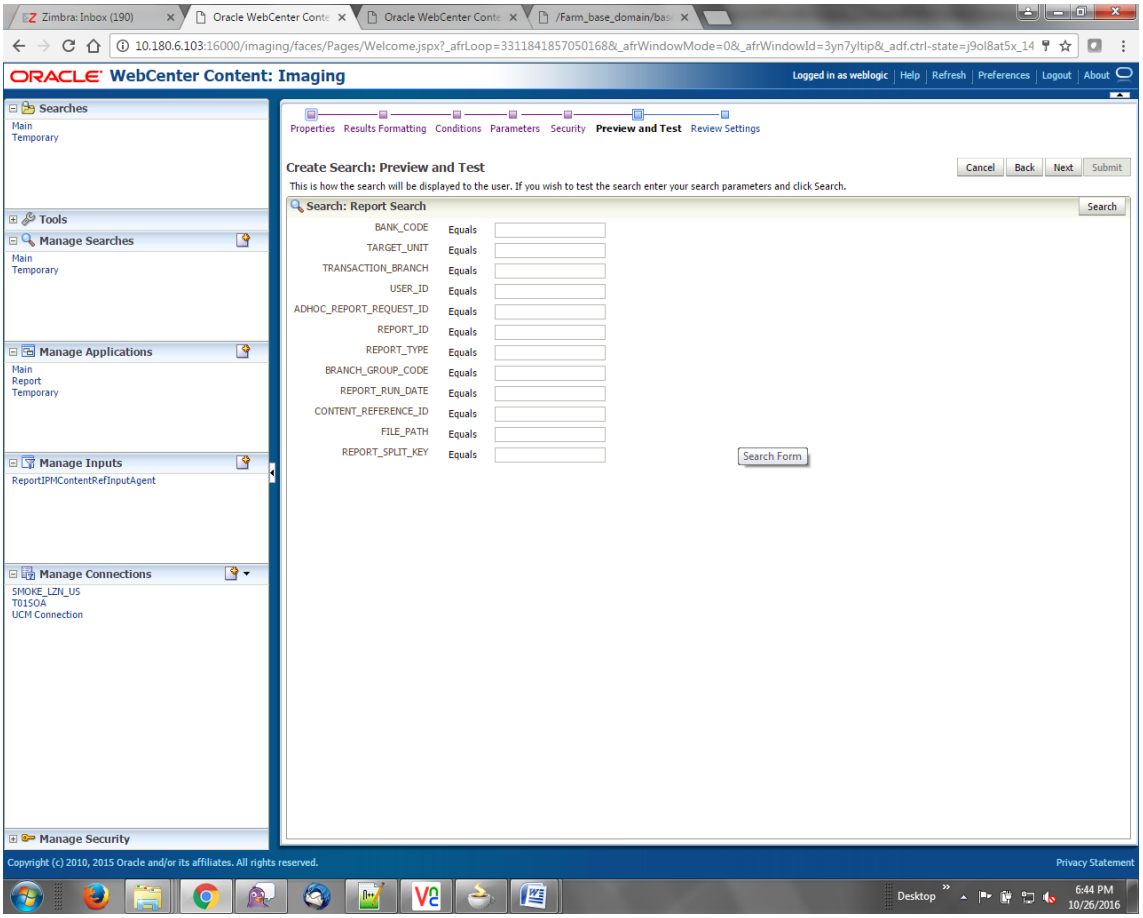
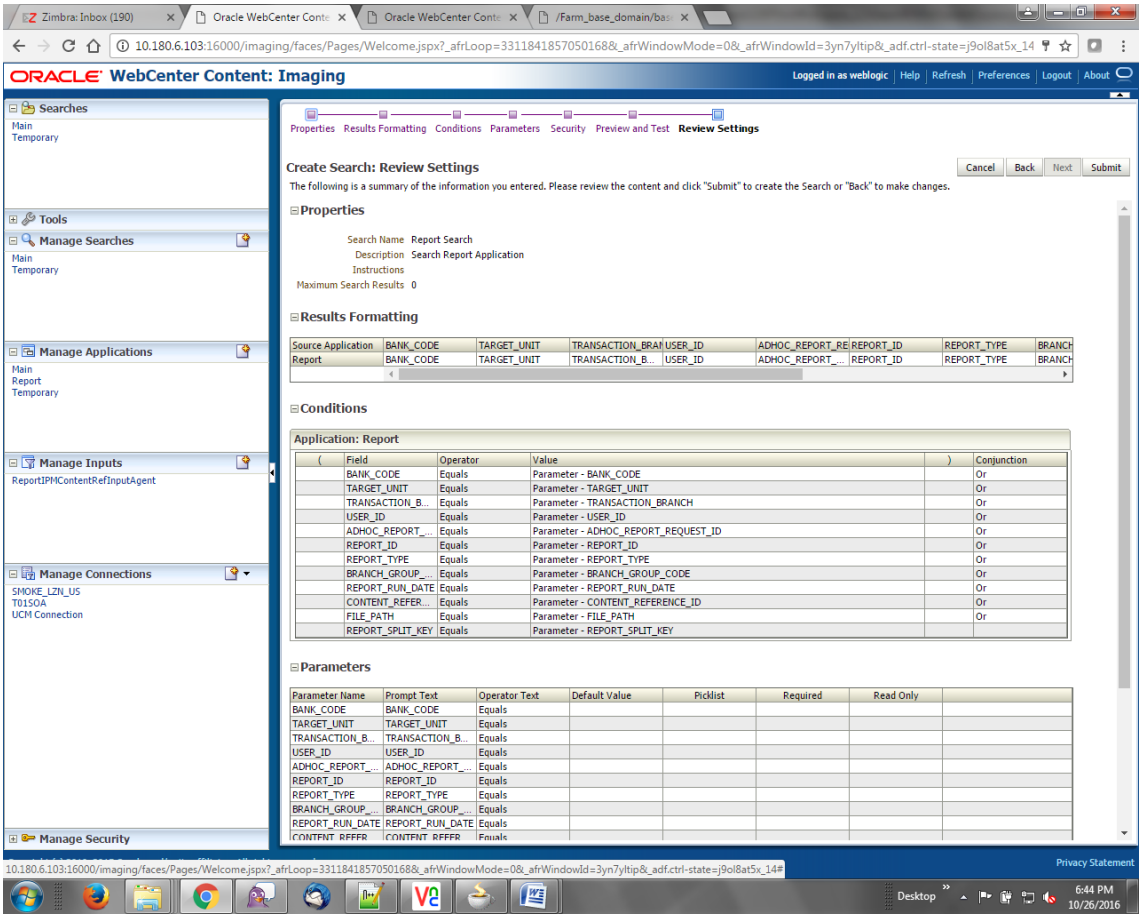


Figure 7–95 Create Search: Review Settings



7.3.8 Additional Steps

1. Update user and bankcode as follows:

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

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

Table 7–2 PROP ID Values

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

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

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

        Copy certificate at the following path on IPM server.

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

        keytool -import -noprompt -trustcacerts -alias UI_SSL_trustself -file SOACert.cer -keystore cacerts -storepass changeit

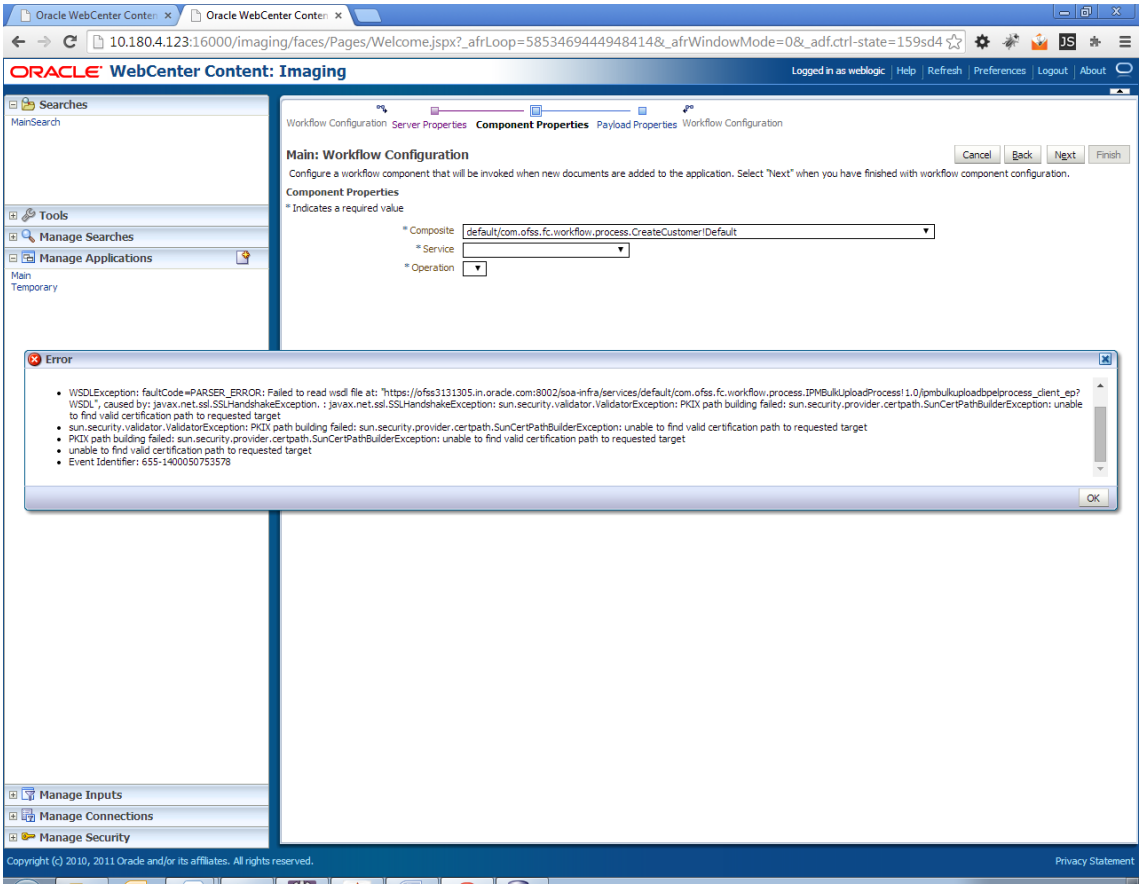
    c. Security policy for ReportIPMRefStoreProcess can been removed (if required).

        Security for called method

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

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

Figure 7–96 Component Properties



8 ODI Configuration

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

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

8.1 Configuration Procedure

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

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

    Example: WSDL_URL =

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

9 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.

10 Post Installation Verification

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

10.1 UI Domain Verification

To verify the UI domain installation:

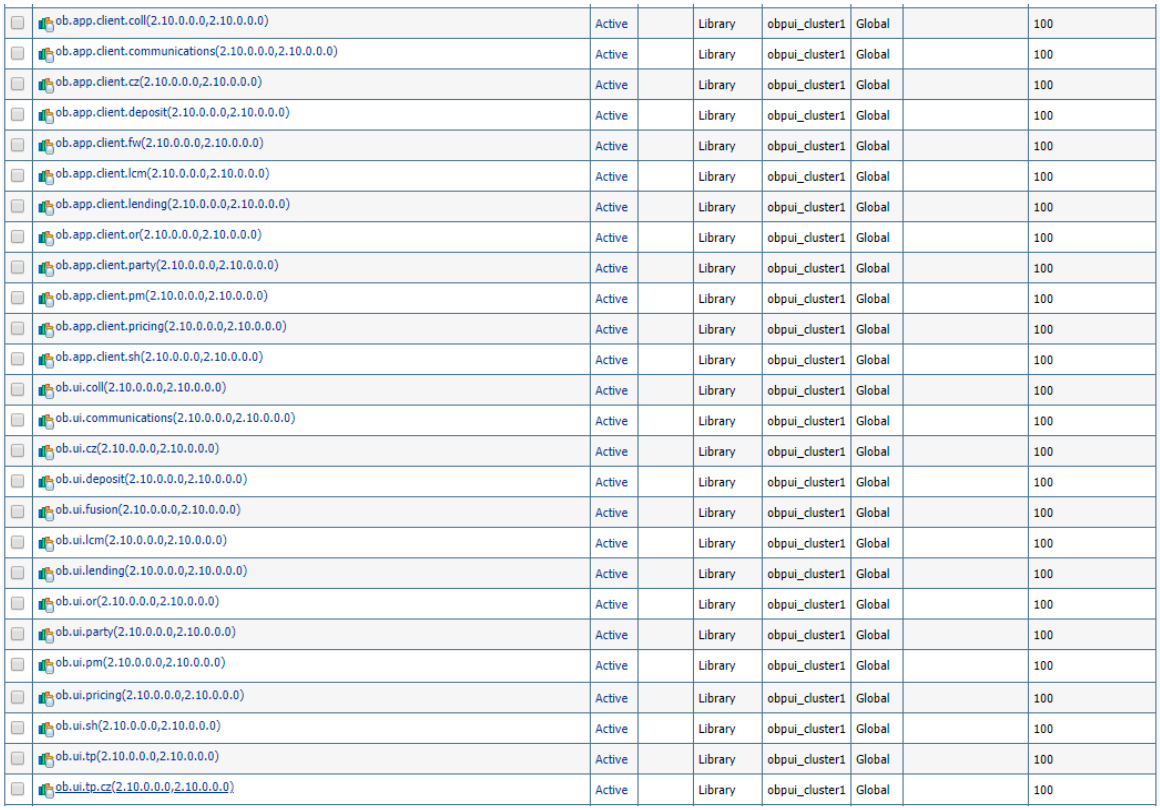
1. Start the UI domain Admin and Managed servers.
2. In the WebLogic console (<UI_IP>:<UI_ADMIN_PORT>/console), navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following OBEDM libraries and applications is *Active*.
    - Shared Libraries
        - ob.app.client.communications
        - 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 10–1 UI Weblogic Console



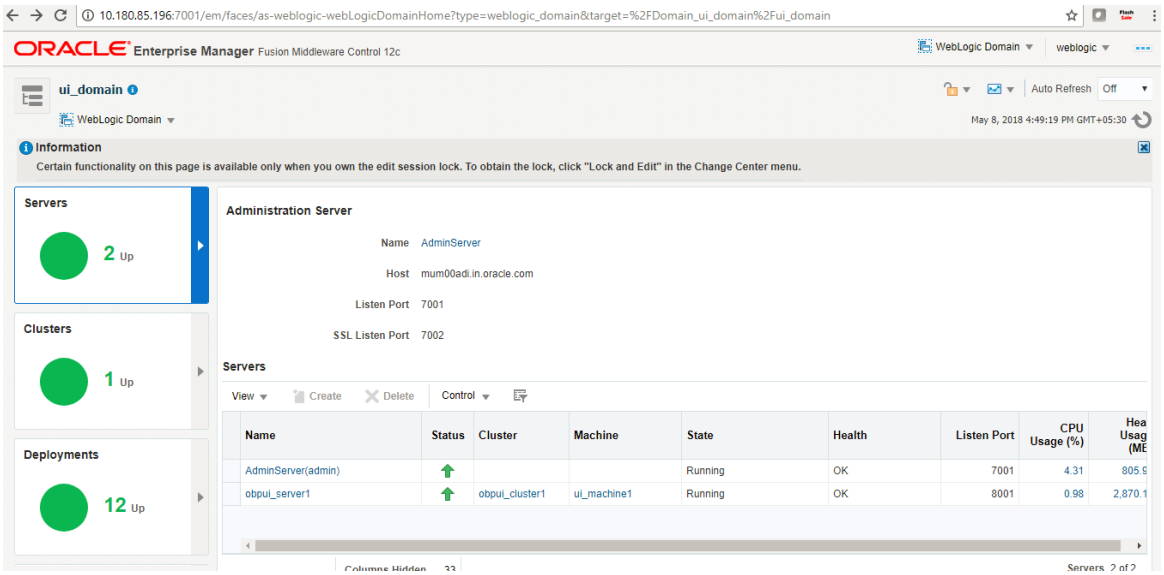
ob.app.client.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
ob.app.client.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
ob.app.client.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obpui_cluster1	Global		100
ob.app.client.deposit(2.10.0.0.0,2.10.0.0.0)	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 10–2 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

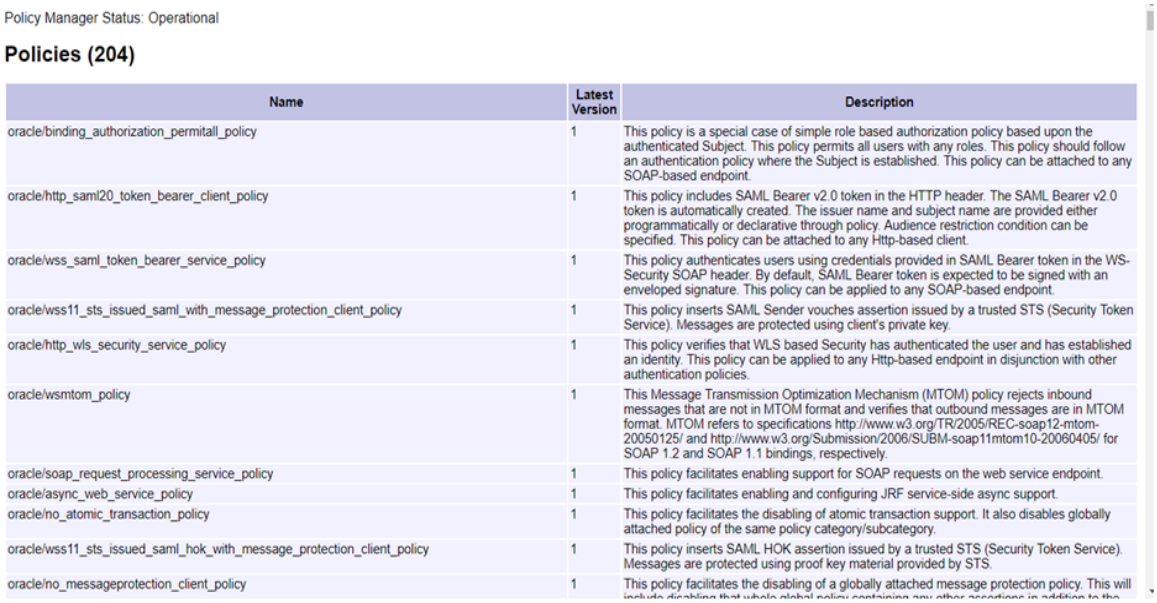
4. In EM console (<UI_IP>:<UI_ADMIN_PORT>/em), check the status of:
   - Cluster
   - Managed Servers
   - Applications

Figure 10–3 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 10–4 UI Admin wsm-pm Validator

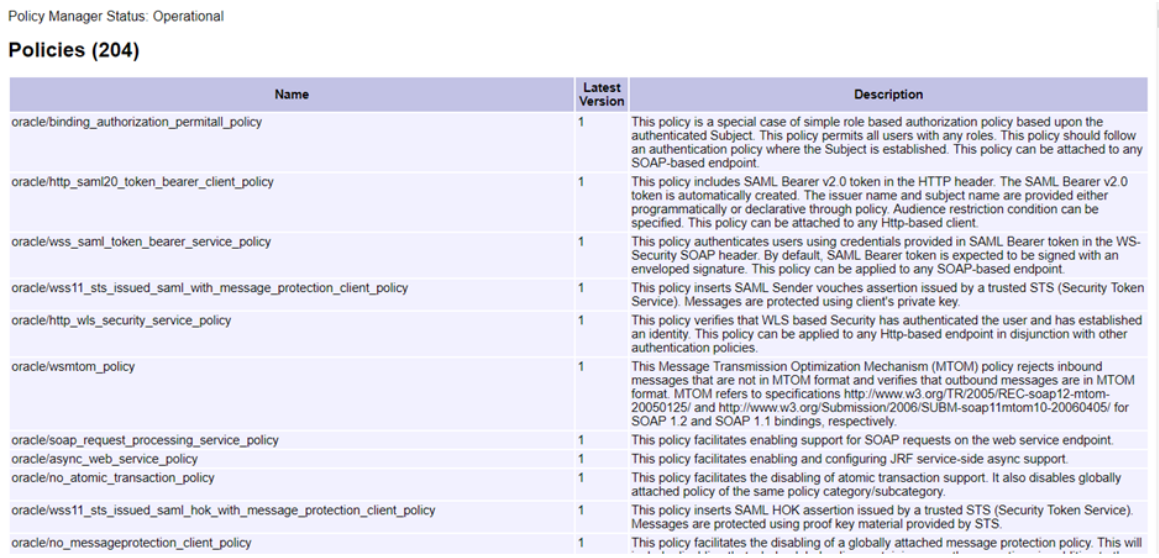


Policy Manager Status: Operational

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 10–5 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

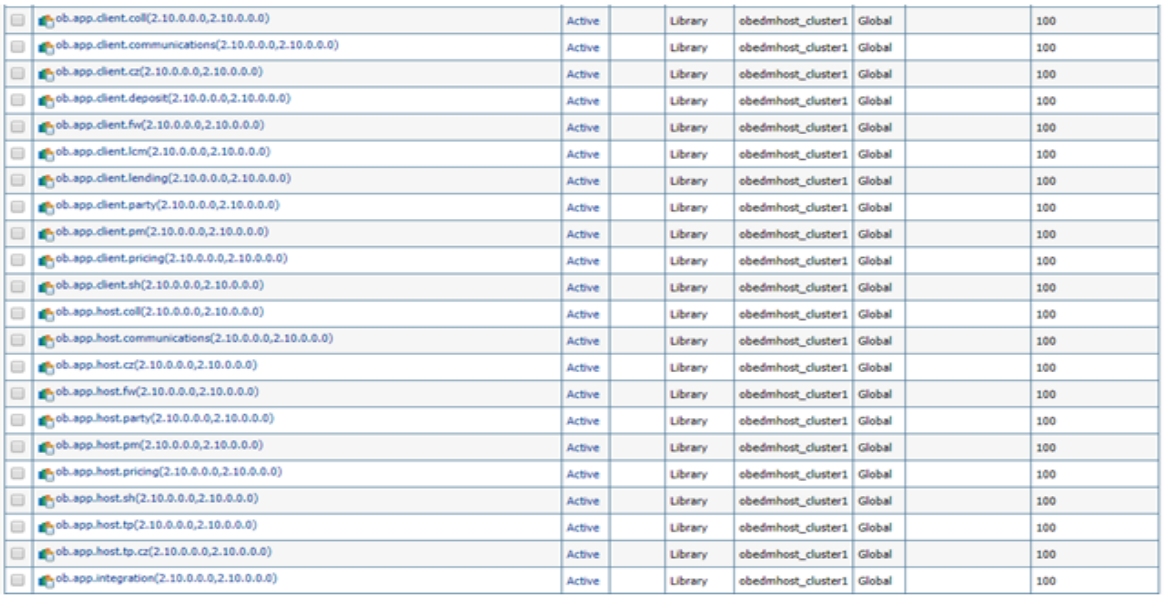
10.2 Host Domain Verification

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*.

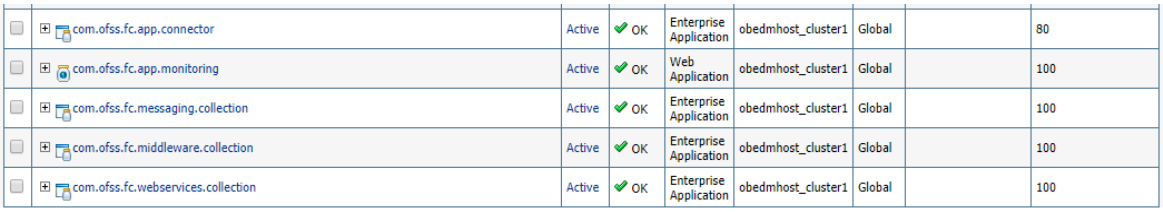
- Shared libraries
  - ob.app.client.communications
  - ob.app.client.coll
  - ob.app.client.cz
  - ob.app.client.deposit
  - ob.app.client.fw
  - ob.app.client.lcm
  - ob.app.client.lending
  - ob.app.client.party
  - ob.app.client.pm
  - ob.app.client.pricing
  - ob.app.client.sh
  - ob.app.host.communications
  - 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 10–6 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 10–7 Host WebLogic Console

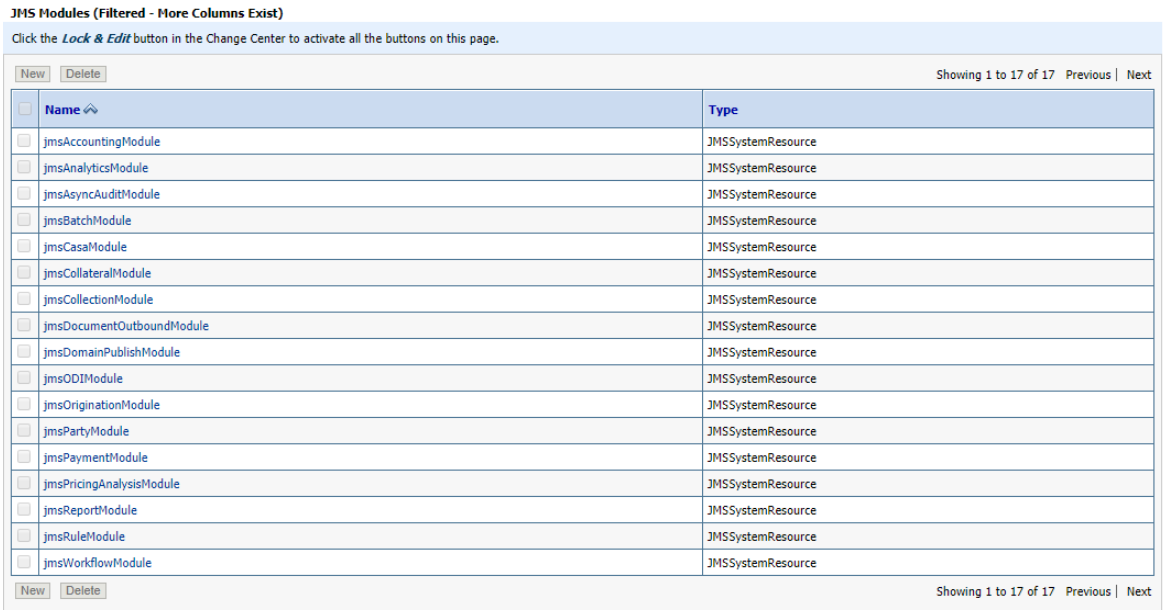


	com.ofss.fc.app.connector	Active	OK	Enterprise Application	obedmhost_cluster1	Global		80
	com.ofss.fc.app.monitoring	Active	OK	Web Application	obedmhost_cluster1	Global		100
	com.ofss.fc.messaging.collection	Active	OK	Enterprise Application	obedmhost_cluster1	Global		100
	com.ofss.fc.middleware.collection	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 10–8 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.

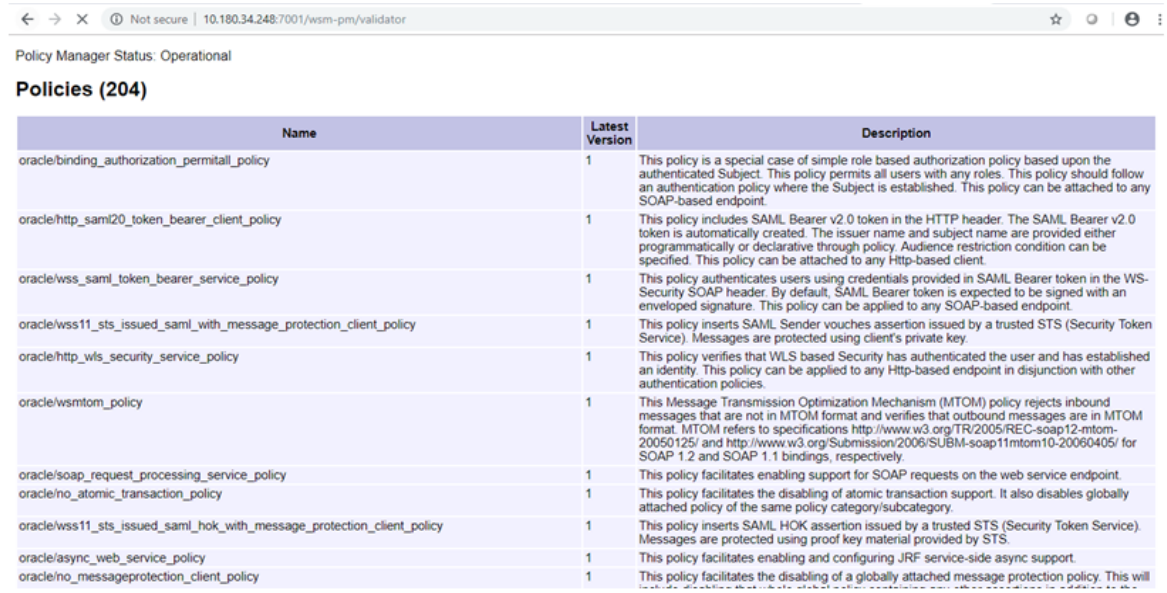
New | Delete — Showing 1 to 17 of 17 Previous | Next

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 10–9 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 10–10 HOST managed wsm-pm validator

Additionally, the installer can verify the following:

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

10.3 SOA Domain Verification

To verify the SOA domain installation:

1. Start the SOA domain Admin and Managed servers (SOA and human task).
2. Navigate to the **Summary of Deployments** page.
3. Verify that the **Status** of the following OBEDM libraries and human task files with .ear extension is *Active*.
   - Shared Libraries
     - ob.app.client.coll
     - ob.app.client.communications

- ob.app.client.cz
- ob.app.client.deposit
- ob.app.client.fw
- ob.app.client.lcm
- ob.app.client.lending
- ob.app.client.or
- ob.app.client.party
- ob.app.client.pm
- ob.app.client.pricing
- ob.app.client.sh
- ob.ui.coll
- ob.ui.communications
- ob.ui.cz
- ob.ui.deposit
- ob.ui.fusion
- ob.ui.lcm
- ob.ui.lending
- ob.ui.or
- ob.ui.party
- ob.ui.pm
- ob.ui.pricing
- ob.ui.sh
- ob.ui.tp
- ob.ui.tp.cz

■ Ears

- com.ofss.fc.app.ui.connector
- com.ofss.fc.ui.view.mds
- com.ofss.fc.workflow.ui.batchexceptionrecovery
- com.ofss.fc.workflow.ui.brop
- com.ofss.fc.workflow.ui.CollectionWorkflowApplication
- com.ofss.fc.workflow.ui.common.approval
- com.ofss.fc.workflow.ui.hardshiprelief
- com.ofss.ob.webservice.soamanagement

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

Figure 10–11 SOA WebLogic Console

	ob.app.client.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.deposit(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.fw(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.lcm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.lending(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.or(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.app.client.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.coll(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.communications(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.deposit(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.fusion(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.lcm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.lending(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.or(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.party(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.pm(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.pricing(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.sh(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.tp(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100
	ob.ui.tp.cz(2.10.0.0.0,2.10.0.0.0)	Active		Library	obphumantask_cluster1	Global		100

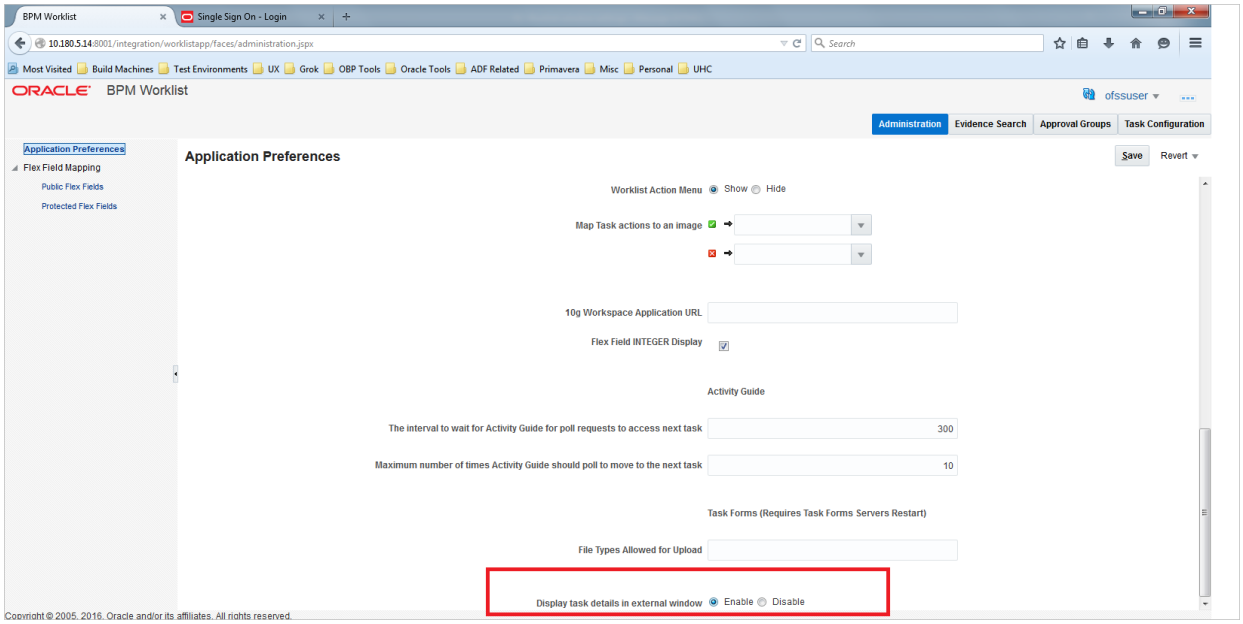
Figure 10–12 SOA WebLogic Console

	com.ofss.fc.app.ui.connector	Active	OK	Enterprise Application	obphumantask_cluster1	Global		80
	com.ofss.fc.ui.view.mds	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.fc.workflow.ui.batchexceptionrecovery	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.fc.workflow.ui.brop	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.fc.workflow.ui.CollectionWorkflowApplicationUI	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.fc.workflow.ui.common.approval	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.fc.workflow.ui.hardshiprelief	Active	OK	Enterprise Application	obphumantask_cluster1	Global		100
	com.ofss.ob.webservice.soamanagement	Active	OK	Web Application	obpsoa_cluster1	Global		100

10.4 BPM Worklist Window Setting

For BPM Worklist window setting, the option **Display task details in external window** must be set to enable mode. This option is present in administration mode of BPM Worklist as shown in Figure 10–13.

Figure 10–13 BPM Worklist Window Settings



11 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.

11.1 OBEDM Domain Installation

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

While creating OBEDM SOA domain, ignore the following error:

Error: No domain or domain template has been read.

Error: No domain or domain template has been read.

Figure 11–1 SOA Domain Error

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

11.2 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.

11.3 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

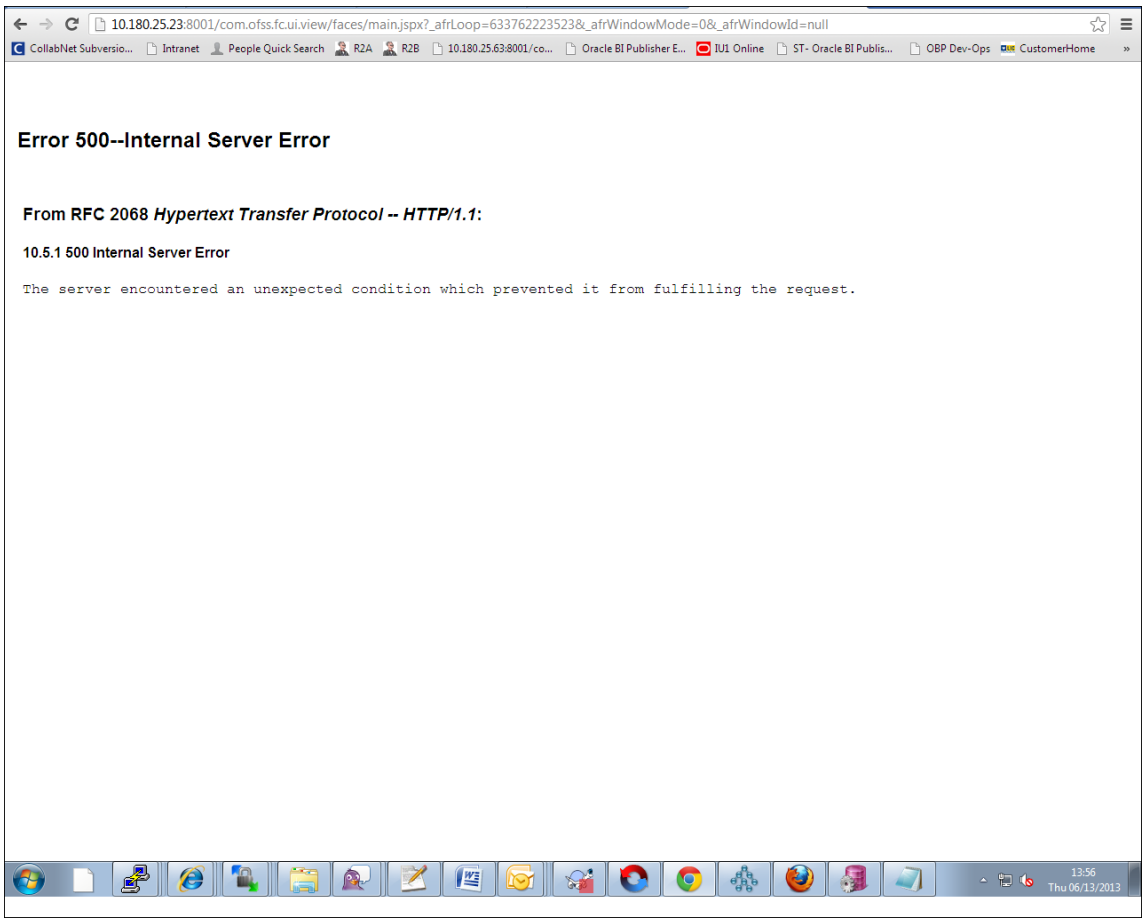
Once the post install script is completed successfully, you can start the domain servers and enter a dummy transaction to check the system correctness. If you face an error you can inspect the stderr log, the WebLogic domain managed server logs as well as the ofss logs under domain directory.

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.

11.4 Error on First Log in

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

Figure 11–2 Error on First Log In



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

11.5 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.

11.6 SOA Setup in Cluster

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

11.6.1 "COMPONENTTYPE": invalid identifier error

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

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

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

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

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

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

11.7 BPM Worklist Task Issue

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

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

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

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

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

   And jps-config.xml

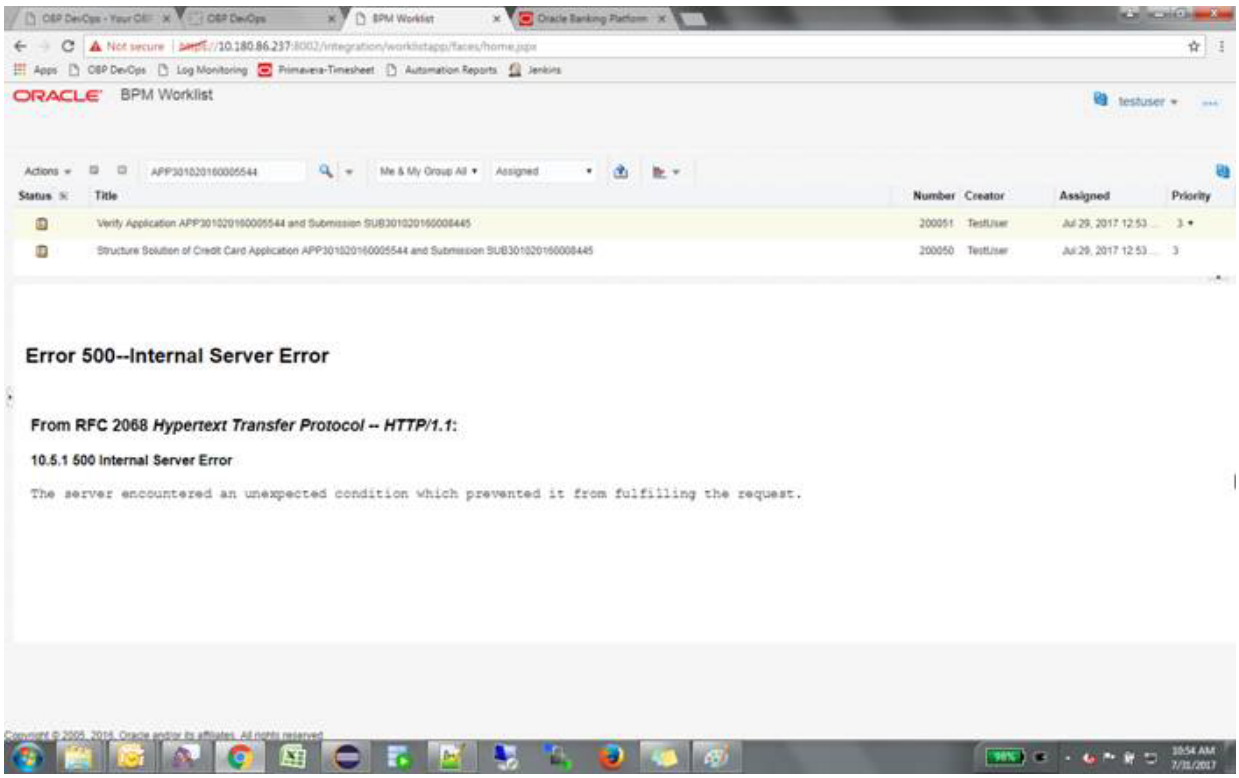
   <property name="trust.keystoreType" value="KSS"/>

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

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

2. Restart it.

Figure 11–3 BPM Worklist Task issue



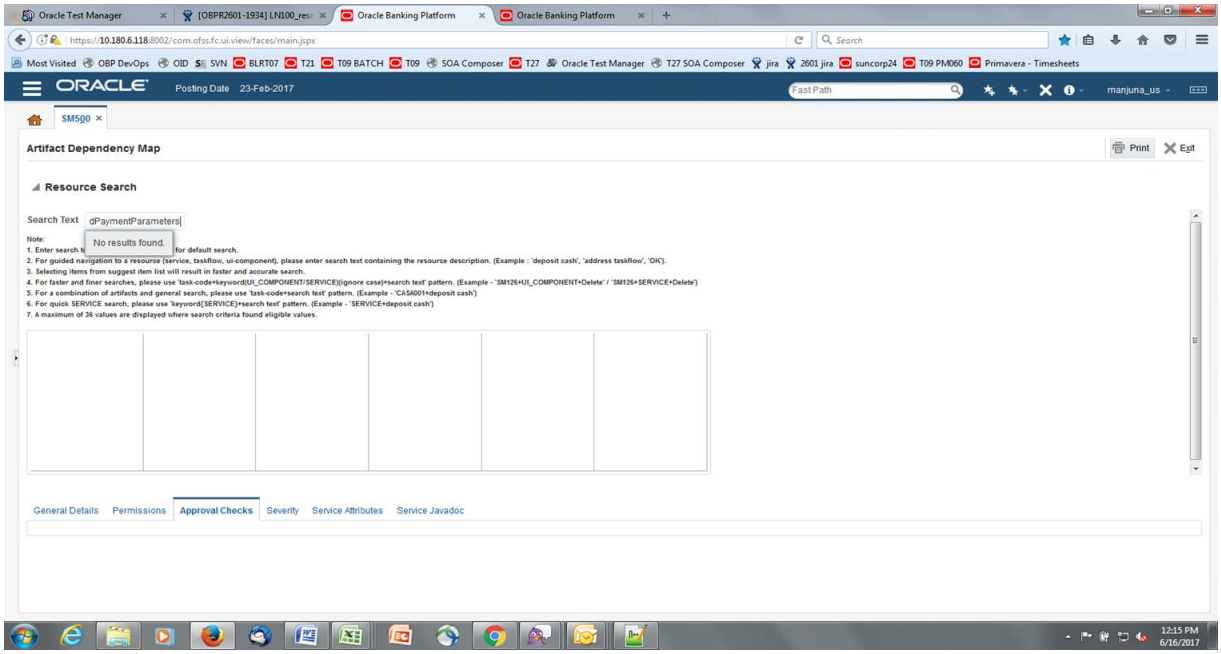
11.8 Artifacts Issue for SM500 page

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 11–4 Artifacts Issue for SM500 page



11.9 ra/FCRJConnectorSOA connector issue

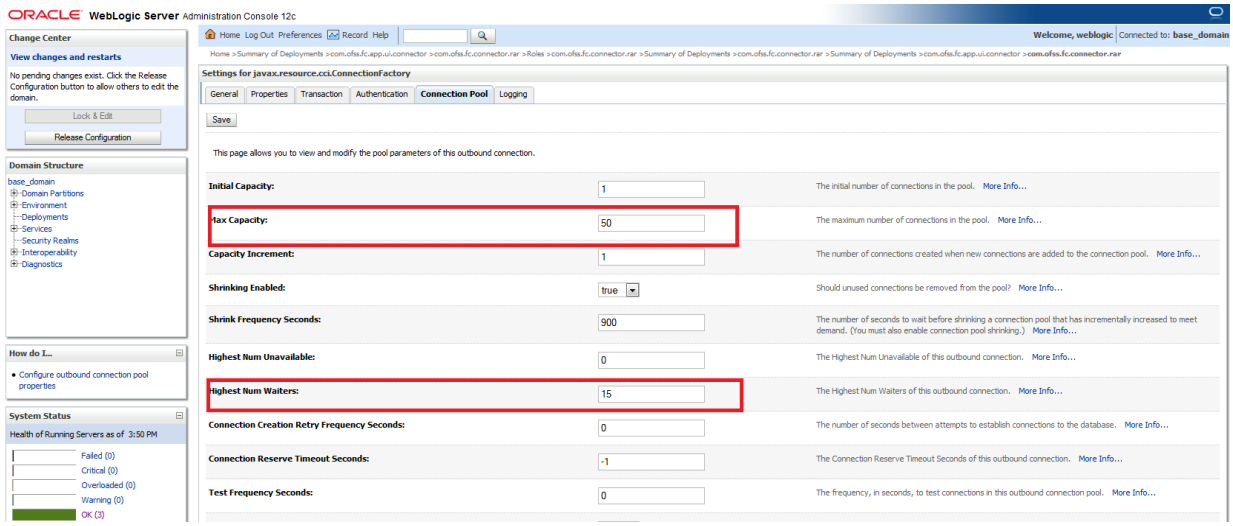
If below mentioned error is faced on Humantask server, configuration shown in the below figure has to be done to resolve issue.

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

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

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

Figure 11–5 Settings for javax.resource.cci.ConnectionFactory page



11.10 Humantask Startup Issue

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

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

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

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

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

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

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

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

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

Truncated. see log file for complete stacktrace

12 Uninstalling the Application

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

12.1 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.