Oracle® Banking Enterprise Originations

Localization Installation Guide - Silent Installation

Release 2.12.0.0.0

F42013-01

May 2021

ORACLE®

Oracle Banking Enterprise Originations Localization Installation Guide - Silent Installation, Release 2.12.0.0.0

F42013-01

Copyright © 2017, 2021, 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 **17**
Audience 17
Documentation Accessibility 17
Organization of the Guide 17
Related Documents 18
Conventions 19
1 Getting Started **22**
1.1 About Oracle Banking Enterprise Originations 22
1.2 About This Document 22
1.3 Assumptions 23
1.4 Limitations 23
1.5 Exclusions 23
2 Pre-Installation Configuration **24**
2.1 Setup Prerequisites 24
2.1.1 Hardware Environment 24
2.1.2 Software Environment 25
2.1.2.1 Certification Details 25
2.1.2.2 Optional 28
2.1.2.3 Patching 28
2.2 Configure Variables 29
2.3 Installation Process Overview 30
2.4 Installation Checklist 30
2.4.1 XD Components 31
2.4.2 Updating installobp***.properties 31

2.4.3 Database and WebLogic Domain Configuration 69
2.5 OID Schema Setup – Custom OBEO Schema 70
2.5.1 Prerequisite – OID setup 70
2.5.2 Verify the OID installation 70
2.5.2.1 Start and Verify the OID processes 71
2.5.2.2 OPSS/OID Performance Tuning 71
2.5.2.3 Import OBEO Specific LDIF files 77
2.5.2.4 Verify the import using ODSM or JXplorer 79
3 OBEO Localization SOA Media Pack Installation 82
3.1 Installation and Configuration Procedure 82
3.1.1 Preparatory Steps 82
3.1.2 Pre-Installation Steps 82
3.1.3 Installation Steps 83
3.2 Post Installation Configuration 87
4 OBEO Localization Host Media Pack Installation 94
4.1 Installation and Configuration Procedure 94
4.1.1 Preparatory Steps 94
4.1.2 Pre-Installation Steps 94
4.1.3 Installation Steps 97
4.1.4 Front End Processing Interface (FEPI) Installation Steps 110
4.2 Post Installation Configuration 112
4.3 REST (SWAGGER) Deployment Check 119
5 OBEO Localization Presentation Media Pack Installation 122
5.1 Installation and Configuration Procedure 122
5.1.1 Preparatory Steps 122
5.1.2 Pre-Installation Steps 122

5.1.3 Installation Steps 123
5.2 Post Installation Configuration 130
6 BAM Installation using OBEO Localization SOA Media Pack 138
6.1 Installation and Configuration Procedure 138
6.1.1 Preparatory Steps 138
6.1.2 BAM Domain Creation Steps 138
6.2 Post Installation Configuration 164
7 Standalone Database Setup 168
7.1 Pre-Installation Steps 168
7.2 OBEO Database Setup – RCU Installation 168
7.3 OBEO Database Installation 169
7.3.1 Host DB Schema Creation and Verification 169
7.3.2 HOST DB schema ddl execution 169
7.3.3 HOST DB Schema Seeding 170
7.3.4 System Configuration DB Update Script Execution 170
7.3.5 Removing Preference Refresh Level 171
7.3.6 Database Table Partitioning 171
8 OBEO and IPM Integration 172
8.1 IPM Application Setup for OBEO Content Management 172
8.1.1 UCM Connection 172
8.1.2 Main Application Configuration 179
8.1.2.1 Manage Application Configuration 179
8.1.2.2 Manage Searches 185
8.1.3 Temp Application Configuration 192
8.1.3.1 Manage Application Configuration 192
8.1.3.2 Manage Searches 198

8.2 IPM Configuration for Bulk Upload Process Setup 206
8.2.1 Prerequisites 206
8.2.2 Setting up the Connection Name 206
8.2.3 Setting up Input Agent Path 212
8.2.4 Create SOA Connection 214
8.2.5 Manage Workflow Configuration 219
8.2.6 Manage Inputs for Input Agents 226
8.2.7 Additional Steps 231
8.2.8 SSL Handshake Resolution 232
8.3 IPM Report Upload Setup 233
8.3.1 Prerequisites 233
8.3.2 Setting up the Connection Name 234
8.3.3 Setting up Input Agent Path 239
8.3.4 Create SOA Connection 241
8.3.5 Manage Application Configuration 246
8.3.6 Manage Inputs for Input Agents 255
8.3.7 Manage Searches 260
8.3.8 Additional Steps 267
9 OAS (BIP) Datasource Creation 270
9.1 OAS (BIP) Datasource Creation 270
10 ODI Configuration 274
10.1 Configuration Procedure 274
11 Monitoring Servers Using Oracle Enterprise Manager 276
12 Post Installation Verification 278
12.1 UI Domain Verification 278
12.2 Host Domain Verification 281

12.3 SOA Domain Verification 289
12.4 BAM Installation Verification 290
12.5 BPM Worklist Window Setting 292
13 Errors and Remedies 294
13.1 OBEO Domain Installation 294
13.2 OBEO Security Policy Seeding 294
13.3 OBEO Domain Post Installation 294
13.4 Error on First Log in 295
13.5 Log in Issues 296
13.6 SOA Setup in Cluster 296
13.6.1 "COMPONENTTYPE": invalid identifier error 296
13.7 BIP Report Data Model Linkage Problem after Host Post Installation Step 297
13.8 Oracle BAM Command Utility Issue 298
13.9 BPM Worklist Task Issue 298
13.10 Artifacts Issue for SM500 page 299
13.11 ra/FCRJConnectorSOA connector issue 300
13.12 Humantask Startup Issue 300
13.13 Collection Mocking 301
13.14 DDA, Party and LOAN Mocking for OBEO installer 301
14 Uninstalling the Application 304
14.1 Manual Uninstall 304

List of Figures

Figure 2–1 Installation Overview 30
Figure 2–2 JXplorer 80
Figure 3–1 Steps in installobpsoa.sh script 84
Figure 3–2 Verification of Properties 84
Figure 3–3 Verification of Properties 85
Figure 3–4 Confirmation to Proceed Domain Installation (cont.) 85
Figure 3–5 Copying and Extraction of obpinstall-ui-soa.zip 86
Figure 3–6 Copying and Extraction of obpinstall-ui-soa.zip 86
Figure 3–7 Copying and Extraction of obpinstall-ui-soa.zip 87
Figure 3–8 Domain Creation Confirmation 87
Figure 3–9 Starting Post Installation 88
Figure 3–10 Starting Post Installation (contd) 89
Figure 3–11 Starting Post Installation (contd) 89
Figure 3–12 Starting Post Installation (contd) 90
Figure 3–13 SOA Post Installation Completion 90
Figure 3–14 Go to BPEL Config 91
Figure 3–15 Go to Web Services Configuration 92
Figure 3–16 Attach Policy 92
Figure 4–1 Steps in installobphost.sh script 98
Figure 4–2 Verification of Properties 99
Figure 4–3 Verification of Properties (contd) 99
Figure 4–4 Verification of Properties (contd) 100
Figure 4–5 Verification of Properties (contd) 100
Figure 4–6 Confirmation and Copying of Installables to Target Machine 101

Figure 4–7 Confirmation and Copying of Installables to Target Machine (contd) 102
Figure 4–8 Confirmation and Copying of Installables to Target Machine (contd) 102
Figure 4–9 Domain Installation Confirmation 103
Figure 4–10 Untar the policyStoreSetup and Copy on destination location 103
Figure 4–11 Untar the policyStoreSetup and Copy on destination location (contd) 104
Figure 4–12 Untar the policyStoreSetup and Copy on destination location (contd) 105
Figure 4–13 Policy Seeding 106
Figure 4–14 Policy Seeding (contd) 107
Figure 4–15 BIP Reports Upload 108
Figure 4–16 BIP Reports Upload (contd) 109
Figure 4–17 BIP Reports Upload (contd) 110
Figure 4–18 Host Domain Admin Server Credentials 112
Figure 4–19 Host Domain Post Installation Script Execution 114
Figure 4–20 Host Domain Post Installation Script Execution (contd) 115
Figure 4–21 Host Domain Post Installation Script Execution (contd) 116
Figure 4–22 Host Domain Post Installation Script Execution (contd) 117
Figure 4–23 Host Domain Post Installation Script Execution Summary 118
Figure 4–24 Navigate to Keystore 119
Figure 4–25 Create Keystore 120
Figure 4–26 Generate Keypair 120
Figure 4–27 OBPAPI deploy on obphost_cluster1 121
Figure 4–28 REST API 121
Figure 5–1 Steps in installobpui.sh script 124
Figure 5–2 Confirmation to Proceed Domain Installation 125
Figure 5–3 Confirmation to Proceed Domain Installation (contd) 126
Figure 5–4 Confirmation to Proceed Domain Installation (contd) 127

Figure 5–5 Copying and Extraction of obpinstall-ui-soa.zip 128
Figure 5–6 Copying and Extraction of obpinstall-ui-soa.zip (contd) 129
Figure 5–7 Domain Creation Confirmation 130
Figure 5–8 UI Admin Server Credentials 131
Figure 5–9 UI Admin Server Running 131
Figure 5–10 UI Admin Server Running (contd) 132
Figure 5–11 Starting Post Installation 133
Figure 5–12 Starting Post Installation (contd) 134
Figure 5–13 Continuation of Post-Installation 135
Figure 5–14 Continuation of Post-Installation (contd) 136
Figure 6–1 Configuration Type page 139
Figure 6–2 Templates page 140
Figure 6–3 High Availability Options page 141
Figure 6–4 Application Location page 142
Figure 6–5 Administrator Account page 143
Figure 6–6 Domain Mode and JDK page 144
Figure 6–7 Database Configuration Type page 145
Figure 6–8 Component Datasources page 146
Figure 6–9 JDBC Test page 147
Figure 6–10 Keystore page 148
Figure 6–11 Advanced Configuration page 149
Figure 6–12 Administration Server page 150
Figure 6–13 Node Manager page 151
Figure 6–14 Managed Servers page 152
Figure 6–15 Clusters page 153
Figure 6–16 Server Templates page 154

Figure 6–17 Dynamic Servers page 155
Figure 6–18 Assign Servers to Clusters page 156
Figure 6–19 Coherence Clusters page 157
Figure 6–20 Machines page 158
Figure 6–21 Assign Servers to Machines page 159
Figure 6–22 Virtual Targets page 160
Figure 6–23 Partitions page 161
Figure 6–24 Configuration Summary page 162
Figure 6–25 Configuration Progress page 163
Figure 6–26 End of Configuration page 164
Figure 6–27 BAM Composer page 166
Figure 6–28 BAM Composer page (contd) 166
Figure 6–29 BAM Composer page 167
Figure 8–1 IPM Imaging Console - Login page 173
Figure 8–2 IPM - Welcome page 174
Figure 8–3 Create Content Server Connection 175
Figure 8–4 UCM: Basic information 176
Figure 8–5 UCM: Connection Settings 177
Figure 8–6 UCM: Connection Security 178
Figure 8–7 UCM: Review Settings 179
Figure 8–8 Main: General Properties 180
Figure 8–9 Main: Field Definitions 181
Figure 8–10 Field Definitions (cont.) 181
Figure 8–11 Main: Application Security 182
Figure 8–12 Main: Document Security 183
Figure 8–13 Main: Storage Policy 184

Figure 8–14 Main: Review Settings 185
Figure 8–15 Main: Properties 186
Figure 8–16 Main: Results Formatting 187
Figure 8–17 Main: Conditions 188
Figure 8–18 Main: Parameters 189
Figure 8–19 Main: Search Security 190
Figure 8–20 Main: Preview and Test 191
Figure 8–21 Main: Review Settings 192
Figure 8–22 Temporary: General Properties 193
Figure 8–23 Temporary: Field Definitions 194
Figure 8–24 Temporary: Application Security 195
Figure 8–25 Temporary: Document Security 196
Figure 8–26 Temporary: Storage Policy 197
Figure 8–27 Temporary: Review Settings 198
Figure 8–28 Temporary: Properties 199
Figure 8–29 Temporary: Results Formatting 200
Figure 8–30 Temporary: Conditions 201
Figure 8–31 Temporary: Parameters 202
Figure 8–32 Temporary: Search Security 203
Figure 8–33 Temporary: Preview and Test 204
Figure 8–34 Temporary: Review Settings 205
Figure 8–35 EM Console Login 207
Figure 8–36 Click Weblogic Domain: ipm domain 208
Figure 8–37 Navigate to Weblogic Domain --> Security --> Credentials 209
Figure 8–38 Create Map oracle.wsm.security 210
Figure 8–39 Create Key basic.credentials 211

Figure 8–40 ipm_domain: Credentials Created 212
Figure 8–41 Navigate to Weblogic Domain --> System MBean Browser 213
Figure 8–42 InputDirectories: Enter Input Agent Path 214
Figure 8–43 Manage Connections: Create Workflow Connection 215
Figure 8–44 IUTSOA: Basic Information 216
Figure 8–45 IUTSOA: Workflow Settings 217
Figure 8–46 IUTSOA: Connection Security 218
Figure 8–47 IUTSOA: Review Settings 219
Figure 8–48 Main: Application Summary 220
Figure 8–49 Manage Applications - Server Properties 221
Figure 8–50 Manage Applications - Component Properties 222
Figure 8–51 Manage Applications - Payload Properties 223
Figure 8–52 Manage Applications - Workflow Configuration 224
Figure 8–53 Field Definitions 225
Figure 8–54 Main: Application Summary 226
Figure 8–55 Input Agent: Basic Information 227
Figure 8–56 Input Agent: Input Mask 228
Figure 8–57 Input Agent: File Parameters 229
Figure 8–58 Input Agent: Fields Mapping 230
Figure 8–59 Input Agent: Summary 231
Figure 8–60 flx_fw_config_all_b table 232
Figure 8–61 SSL Handshake Resolution 233
Figure 8–62 Log in to Enterprise Manager (EM) console 234
Figure 8–63 Click Weblogic Domain: ipm domain 235
Figure 8–64 Navigate to Weblogic Domain --> Security --> Credentials 236
Figure 8–65 Create Map oracle.wsm.security 237

Figure 8–66 Create Key: basic.credentials 238
Figure 8–67 ipm_domain: Credentials Created 239
Figure 8–68 Navigate to Weblogic Domain --> System MBean Browser 240
Figure 8–69 InputDirectories: Enter Input Agent Path 241
Figure 8–70 Manage Connections: Create Workflow Connection 242
Figure 8–71 IUTSOA: Basic Information 243
Figure 8–72 IUTSOA: Workflow Settings 244
Figure 8–73 IUTSOA: Connection Security 245
Figure 8–74 IUTSOA: Review Settings 246
Figure 8–75 Create Application: General Properties 247
Figure 8–76 Report: Field Definitions 248
Figure 8–77 Create Application: Applications Security 249
Figure 8–78 Create Application: Document Security 250
Figure 8–79 Create Application: Storage Policy 251
Figure 8–80 Report: Workflow Configuration - Server Properties 252
Figure 8–81 Report: Workflow Configuration - Component Properties 253
Figure 8–82 Report: Application Summary 254
Figure 8–83 Create Application: Review Settings 255
Figure 8–84 Manage Inputs 256
Figure 8–85 Input Agent Details: Input Mask 257
Figure 8–86 Input Agent Details: Field Mapping 258
Figure 8–87 Input Agent Details: Security 259
Figure 8–88 Input Agent Details: Review Settings 260
Figure 8–89 Create Search: Properties 261
Figure 8–90 Create Search: Results Formatting 262
Figure 8–91 Create Search: Conditions 263

Figure 8–92 Create Search: Parameters 264
Figure 8–93 Create Search: Security 265
Figure 8–94 Create Search: Preview and Test 266
Figure 8–95 Create Search: Review Settings 267
Figure 8–96 Component Properties 269
Figure 9–1 OAS (BIP) Server Console Login 270
Figure 9–2 OAS (BIP) Administration 271
Figure 9–3 OAS (BIP) JDBC Connection 271
Figure 9–4 OAS (BIP) - Add Data Source 272
Figure 9–5 OAS (BIP) Data Source Created 273
Figure 12–1 UI EM Console Status Check 280
Figure 12–2 UI Admin wsm-pm Validator 280
Figure 12–3 UI managed wsm-pm validator 281
Figure 12–4 HOST admin wsm-pm validator 288
Figure 12–5 HOST managed wsm-pm validator 288
Figure 12–6 BAM Composer 291
Figure 12–7 BAM Composer 291
Figure 12–8 BAM Composer 292
Figure 12–9 BPM Worklist Window Settings 292
Figure 13–1 SOA Domain Error 294
Figure 13–2 Error on First Log In 296
Figure 13–3 Selecting the Data model 297
Figure 13–4 BPM Worklist Task issue 299
Figure 13–5 Artifacts Issue for SM500 page 299
Figure 13–6 Settings for javax.resource.cci.ConnectionFactory page 300

List of Tables

Table 2–1 Hardware and OS 24
Table 2–2 List of Software 25
Table 2–3 Notes 26
Table 2–4 XD Components 31
Table 2–5 Values for updating installobp***.properties - FOR HOST 32
Table 2–6 Values for updating installobp***.properties - For SOA 47
Table 2–7 Values for updating installobp***.properties - For UI 59
Table 2–8 DB and WebLogic Domain Configuration 69
Table 2–9 Parameter Values to be Changed 71
Table 2–10 Suggested values for Tuning and Alter Command 72
Table 2–11 Properties 76
Table 2–12 Order of Execution 78
Table 4–1 XD Components 95
Table 4–2 Examples of FMW Dir Name, Domain Name, Server Name and Memory Parameters 95
Table 4–3 Properties 111
Table 4–4 Examples of files 112
Table 8–1 PROP ID Values 232
Table 8–2 PROP ID Values 267
Table 9–1 Data Source Details 272

Preface

The Oracle Banking Enterprise Originations Localization Installation Guide - Silent Installation contains information on silent installation and configuration of Oracle Banking Enterprise Originations 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 Originations AU or 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/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=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 Originations 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 Originations.

Chapter 3 OBEO Localization SOA Media Pack Installation

This chapter explains the steps involved in the installation, and post installation and configuration of Oracle Banking Enterprise Originations SOA (Integration Server) Media pack.

Chapter 4 OBEO Localization Host Media Pack Installation

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

Chapter 5 OBEO Localization Presentation Media Pack Installation

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

Chapter 6 BAM Installation using OBEO Localization SOA Media Pack

This chapter explains the steps involved in the installation of Oracle Business Activity Monitoring (BAM) using OBEO SOA (Integration Server) Media Pack.

Chapter 7 Standalone Database Setup

This chapter explains the steps involved in Oracle Banking Enterprise Originations database.

Chapter 8 OBEO and IPM Integration

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

Chapter 9 OAS (BIP) Datasource Creation

This chapter explains the steps required for Oracle Analytics Server (OAS) (formerly known as BIP or Business Intelligence Publisher) datasource creation.

Chapter 10 ODI Configuration

This chapter explains the steps involved in the configuration of ODI using OBEO Host Media Pack.

Chapter 11 Monitoring Servers Using Oracle Enterprise Manager

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

Chapter 12 Post Installation Verification

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

Chapter 13 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 Originations.

Chapter 14 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Enterprise Originations.

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 Originations and Oracle Documaker, see the installation and configuration guides at https://docs.oracle.com/cd/F30719_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 Originations Security Guide.

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

Conventions

The following text conventions are used in this document:

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

The following acronyms are used in this document:

Acronym	Meaning
ADF	Application Development Framework
BAM	Business Activity Monitoring
BPEL	Business Process Execution Language
DB or db	Oracle Database
HOST	Middleware Host Tier
IAM	Identity and Access Management
IPM	Imaging and Process Management
LDAP	Lightweight Directory Access Protocol
OAS	Oracle Analytics Server
OAAM	Oracle Adaptive Access Manager
OBEO	Oracle Banking Enterprise Originations
ODI	Oracle Data Integrator

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

1 Getting Started

This chapter presents an overview of Oracle Banking Enterprise Originations 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 Originations

Oracle Banking Enterprise Originations (OBEO) enables banks to move from product-centric to customer-centric services, simplifying complex origination processes and delivering frictionless customer experiences across the originations lifecycle. Banks can consider deploying Oracle Banking Enterprise Originations, both as an independent standalone project or as a starting point for a broader progressive modernization program. The solution is built using standard enterprise components, provides efficient process automation, and is available on premise, on the cloud, or through a hybrid model. Oracle Banking Enterprise Originations enables banks to deliver cross-channel consistent origination experience wherein the customers can use any channel they prefer. The solution operates across channels, providing a common origination process for both assisted- and self-service customers. The process also allows customers to utilize different access points, so they may begin the process in one channel, yet use alternative channels to complete the process.

1.2 About This Document

This document guides you through the installation of the core banking application Oracle Banking Enterprise Originations along with AU or 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 Originations Integration and Approval Processes hosted on Oracle SOA)
- Security Configuration (Seeding security to OID)
- Seed Data Configuration (Seeding data to Core banking OLTP Database Server)

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

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

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

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

1.3 Assumptions

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

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

- The Oracle Banking Enterprise Originations AU or US localization installables are downloaded and copied onto a Linux machine or Linux VM.
- The reader has taken a remote connection to the Linux machine via Windows box.
- The reader is able to take an 'ssh' connection to the servers on which various OBEO 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 OBEO AU or US localization installation.

1.4 Limitations

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

1.5 Exclusions

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

2 Pre-Installation Configuration

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

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 Originations 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 Originations 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	Oracle Banking Enterprise Originations Oracle Database
2	4	32	200	OEL 7.5 64 bit	Oracle Banking Enterprise Originations ADF UI Presentation Server
3	4	32	200	OEL 7.5 64 bit	Oracle Banking Enterprise Originations Services Middleware Host Server
4	2	16	200	As per OID certification matrix.	Oracle OID Server
5	2	16	200	As per IPM certification matrix.	Oracle IPM Server
6	2	16	200	As per OAS certification matrix.	Oracle Analytics Server
7	4	32	200	As per SOA certification matrix.	Oracle SOA Server
8	4	16	200	As per BAM certification matrix.	Oracle BAM Server

2.1.2 Software Environment

It is assumed that the following products are installed and are available on the server on which the Oracle Banking Enterprise Originations 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	OBEO UI Presentation	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
2	SOA	Banking App	Oracle SOA Suite 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
3	OBEO HOST	Banking App	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Oracle Database 19c Enterprise Edition Release 19.8 Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
4	OID	Security	Oracle Internet Directory 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
5	OAS	Document	Oracle Analytics Server (5.5) Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
6	IPM	Document	Oracle WebCenter - Content 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
7	OSB	Integration	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Oracle Service Bus 12c (12.2.1.4.0). Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
8	ODI	Integration	Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Oracle Data Integrator 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
9	OIM	Security	Oracle Identity Manager 12.2.1.4.0

Sr. No.	Components	Zone	Software
			Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
10	OAM	Security	Oracle Access Manager 12.2.1.4.0 Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281) Oracle Linux 7.5 64-bit
11	OEM	Management	Oracle Enterprise Manager 13.2.0.0.0 As per certification matrix of Oracle Enterprise Manager 13.2.0.0.0
12	EM Agent Installation	Management	Push from OEM Console
13	OBEO Database	Database	Oracle Database 19c Enterprise Edition Release 19.8 Oracle Linux 7.5 64-bit
14	HTTP Server	Web Server	Oracle HTTP Server 12.2.1.4.0.
15	BAM	Banking App	Oracle SOA Suite and Business Process Management 12c (12.2.1.4.0) Java Version jdk1.8.0_xx (jdk1.8.0_281)

The following are some notes related to the software.

Table 2–3 Notes

Serial Number	Description
1	OBEO 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	Oracle Business Intelligence Publisher is required at the time of OBEO installation. It is required to use the actual BIP property values during the installation. This is required as the installer uploads the OBEO reports as onto the BIP server as part of the middleware host installation process.
3	ODI_OUTBOUND_USERNAME and ODI_OUTBOUND_PASSWORD The OBEO 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.
4	The OBEO installer will not abort the installation if this component is not present. It can be installed later.

Serial Number	Description
	It is strongly recommended to use the actual property values instead of default property values during the installation. Else, these properties have to be manually updated in Host Database after the entire installation completes.
5	OIM_OUTBOUND_USERNAME and OIM_OUTBOUND_PASSWORD The OBEO installer will not abort the installation if this component is not present. It can be installed later. It is recommended to use the actual property values instead of default property values during the installation. Else, these properties have to be manually updated in Host Database. Also, actual values for OIM_OUTBOUND_USERNAME and OIM_OUTBOUND_PASSWORD once available have to be manually updated in the 'ra/FCRJConnectorOIM' jndi property of com.ofss.fc.app.connector.ear application inside middleware host server after the entire installation completes.
6	Oracle Access Manager can be installed later.
7	During installation, password of unix user will be asked multiple times for "scp" "ssh". There is a time limit for entering password. If not entered within specified limit, the installation is likely to exit. User should take care of this.
8	It is mandatory for machine nodes on which OBEO UI, Host, and SOA Media pack installation is planned, to install the Java Cryptography Extensions Unlimited Strength Jurisdiction Policy Files, to enable additional encryption strengths.
9	Download the jce_policy.zip from Oracle website for the current Java version being used. For jdk1.8.0_xx, download Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 jce_policy-8.zip from the following link: http://www.oracle.com/technetwork/java/javase/downloads/jce-all-download-5170447.html Copy "local_policy.jar" and "US_export_policy.jar" from this zip file in the path mentioned below: JAVA_HOME/jre/lib/security/
10	It is mandatory that the team installing OBEO reads and understands the system requirements and specifications for the fusion middleware specified in the following link: https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-B648EA24-ABB4-42CA-B8F2-4B535D5EC8DB The url details the system and platform-specific information for Oracle Fusion Middleware 12c Release 1 (12.2.1.4.0) products. Changes necessary at a system level for the fusion middleware should be made prior to executing OBEO media packs. For example, the number of open files should be increased from the default value as specified in the following link: https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-F800C79F-A8CA-4A80-A4E9-97BC8E264889
11	SOA managed servers may need the default value raised at operating system level to run, as it needs to load a large number of OBEO application binaries.
12	It is mandatory for SOA Suite to be installed in machine nodes on which OBEO BAM Installation is planned.
13	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

Serial Number	Description
	conventions, should be added after the media pack installation is complete.
14	Oracle SOA Suite 12.2.1.4.0 patches - p30995852_122140_Generic.zip, p31199221_ 12214200304_Generic.zip, p30970477_122140_Generic.zip, p30729380_122140_ Generic.zip have to be applied on SOA machine only. This can be downloaded from the following link: https://support.us.oracle.com/

2.1.2.2 Optional

The following software is optional:

- Oracle VM server release 2.2.0

2.1.2.3 Patching

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

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

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

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

The installation steps are as follows:

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

   tar -xvzf suds-0.4.tar.gz

   tar -xvzf docutils-0.12.tar.gz

   tar -xvzf wstools-0.4.3.tar.gz

   tar -xvzf SOAPpy-0.12.5.tar.gz

   tar -xvzf PyYAML-3.11.tar.gz

   tar -xvzf JPype1-0.5.7.tar.gz

   chmod -R 777 *

   cd suds-0.4

   python setup.py install

   cd ../docutils-0.12

python setup.py install

cd ../wstools-0.4.3

python setup.py install

cd ../SOAPpy-0.12.5

python setup.py install

cd ../PyYAML-3.11

python setup.py install

cd ../JPype1-0.5.7

python setup.py install

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

2.2 Configure Variables

Perform the following steps to configure the variables:

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

   The wsdl details will be as follows:

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

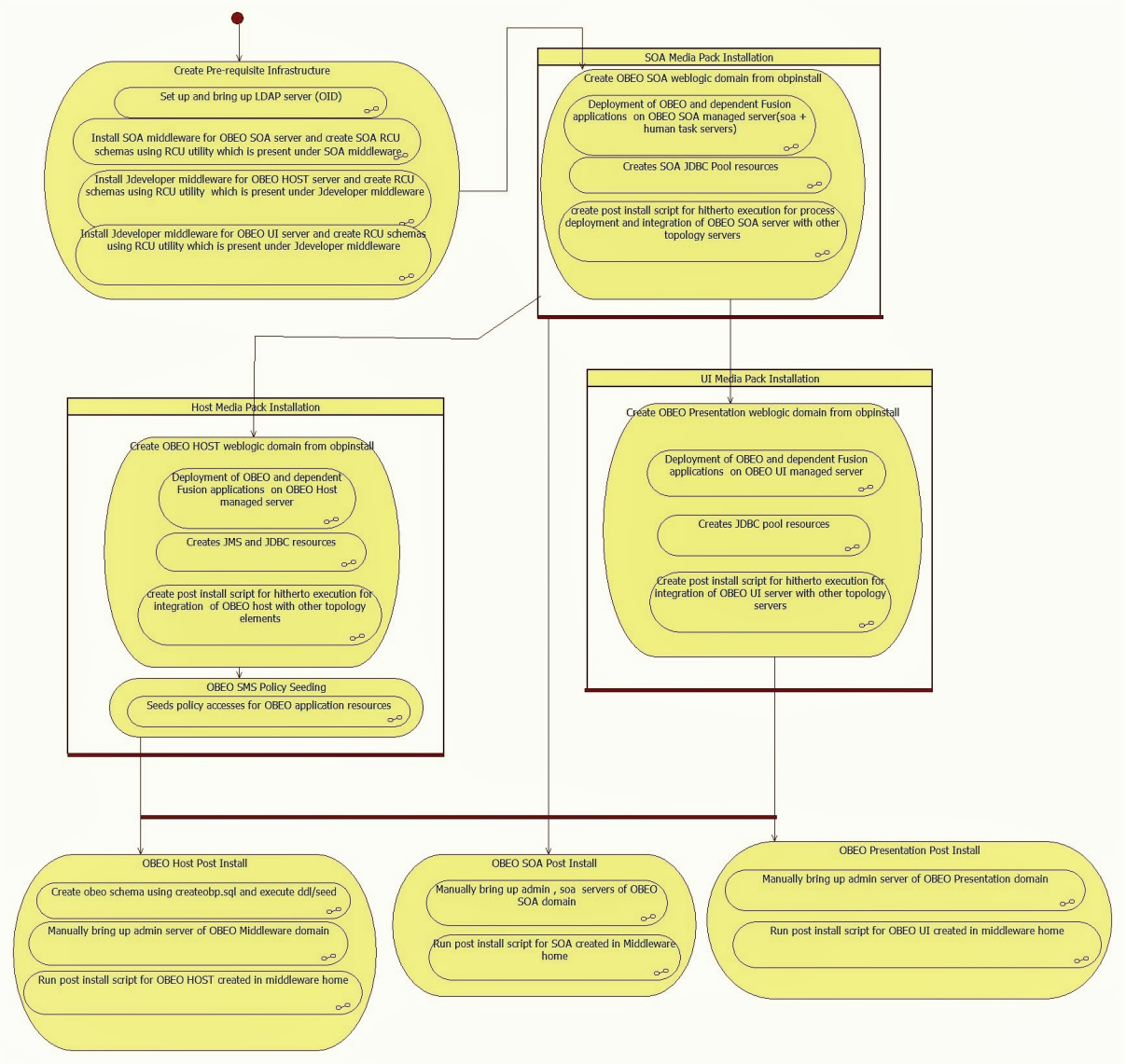
   For example, url: http://<Ip>:<Port>/com.ofss.fc.webservice/services/sms/TransactionBlackoutApplicationServiceSpi?wsdl

5. Modify the PatchConstants.py located at the location <installDir>patching/constants.
   a. The PATCH_HOME should point to the Patching Utility.
   b. The Deployables Path should point to obp.
   c. The FMW_HOME should point to the path till fmw.
   d. The WLST_SCRIPT_LOCATION should point to the wlst.sh (weblogic scripting tool).
   e. The JVM_PATH should point to the libjvm.so.
   f. The PATCH_TEMP_LOCATION should be the path where the zips are to be stored.
   g. The FCServerWithPort is '${protocol}://${hostmanagedserver_ip}:${hostManagedServer_port}'.
   h. The SOAServerWithPort is '${protocol}://${uimanagedserver _ip}:${ uiManagedServer _port}'.
   i. The CENTRAL_PATCH_STAGE_PATH should point to the central patch Staging path.
6. Create folder patchStage and centralPatchStage in location <installDir>/.

2.3 Installation Process Overview

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

Figure 2–1 Installation Overview



2.4 Installation Checklist

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

https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/sysrs/system-requirements-and-specifications.html#GUID-B648EA24-ABB4-42CA-B8F2-4B535D5EC8DB

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 OBEO Localization media packs.

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

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

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

2.4.1 XD Components

The following table provides a list of XD components.

Table 2–4 XD Components

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

2.4.2 Updating installobp***.properties

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

Table 2–5 Values for updating installobp.properties - FOR HOST***

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

Sr.No	Name	Description	Example Value	Value
		Provider .Value will be OID or OVD.		
23	OID_IP	I/P address of the OID server.	10.180.84.113	
24	OID_PORT	Port of the OID process instance.	3060	
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.	ou=obp,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	

Sr.No	Name	Description	Example Value	Value
30	HOST_CLUSTER_NAME	Refers to HOST cluster name	obphost_cluster1	Can give any logical name
31	HOST_SERVER_NAME	Refers to HOST server name	obphost_server1	Can give any logical name
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_231	
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 patching.	/scratch/app/product/jdk1.8.0_231	
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)	

Sr.No	Name	Description	Example Value	Value
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	UI_IP	I/P address of the server on which the OBP presentation or UI layer should be installed.	10.180.84.111	
44	SOA_ORACLE_HOME	Name of Oracle SOA which is present in fusion middleware.	soa	

Sr.No	Name	Description	Example Value	Value
45	SOA_IP	i/p address of SOA machine	10.180.84.112	
46	SOA_UNIX_USER	Unix username of SOA machine	ofssobp	
47	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
48	SOA_DOMAIN_NAME	Refers to the middleware home of the weblogic installation on the SOA server.	base_domain	
49	SOA_MANAGED_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
50	SOA_ADMIN_SERVER_LISTEN_PORT	Listen port of SOA Admin server	7001	
51	SOA_MANAGED_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
52	SOA_WEBLOGIC_USERNAME	Username of the server of SOA domain	weblogic	
53	SOA_WEBLOGIC_PASSWORD	Password of the server of SOA domain	weblogic1	
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	BIP_SERVER_IP	I/P of the BIP server to host OBP reports	10.180.84.115	

Sr.No	Name	Description	Example Value	Value
57	BIP_SERVER_PORT	Port of the BIP server that hosts OBP reports	9502	
58	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
59	BIP_MW_HOME	Oracle BIP Middleware directory on BIP server	/scratch/app/product/fmw	
60	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
61	BIP_JAVA_HOME	Orace JAVA HOME directory on BIP server	/scratch/app/product/jdk1.8.0_281	
62	BIP_SERVER_USER	Oracle BIP server user id	weblogic	
63	BIP_SERVER_PSWD	Oracle BIP server user password	weblogic1	
64	BIP_CATALOG_NAME	OBP BIP Catalog Name will be same as Host database user	OBP2712	
65	BIP_DATASOURCE_NAME	OBP Host database user used by OBP report to fetch data for reports	OBP2712	
66	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
67	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
68	IPM_SERVER_IP	IP of Oracle Image and Processing Server for OBP Content Management	10.180.84.114	
69	IPM_SERVER_PORT	Port of Oracle Image and Processing Server	16000	

Sr.No	Name	Description	Example Value	Value
		for OBP Content Management		
70	IPM_MW_HOME	Oracle weblogic Home directory on IPM server	/scratch/app/product/fmw	
71	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ECM1	
72	OBP_HOST_DB_USER	OBP Host database user/schema	OBEDMUS211	
73	OBP_HOST_DB_PASSWORD	OBP Host database password	welcome1	
74	OBP_HOST_DB_IP	OBP Host database i/p address	10.180.84.113	
75	OBP_HOST_DB_PORT	OBP Host database port	1521	
76	OBP_HOST_DB_SERVICE_NAME	OBP Host database service name	P84113A	
77	ONS_NODE	i/p address of ONS service	10.180.84.113	
78	ONS_PORT	Listen port of ONS service	6200	
79	OPSS_HOST_SCHEMA_USER	HOST OPSS Host schema user	COLLMW_OPSS	
80	OPSS_HOST_SCHEMA_PASSWORD	OPSS Host schema password	welcome1	
81	OPSS_HOST_DB_IP	OPSS Host DB IP	10.180.84.113	
82	OPSS_HOST_DB_PORT	OPSS Host DB Port	1521	
83	OPSS_HOST_DB_SERVICE_NAME	OPSS Host database service name	P84113A	

Sr.No	Name	Description	Example Value	Value
84	LOCAL_ DATASOURCE	STB datasource schema name	COLLMW_STB	
85	WLS_RUNTIME_ SCHEMA_USER	WLS runtime datasource schema name	COLLMW_WLS_RUNTIME	
86	MDS_HOST_DB_ USER	MDS schema user to be used by UI and Host domain	COLLMW_MDS	
87	MDS_HOST_DB_ PASSWORD	MDS schema Password of MDS schema user to be used by UI and Host domain	welcome1	
88	MDS_HOST_DB_IP	MDS DB IP address of MDS schema user to be used by UI and Host domain	10.180.84.113	
89	MDS_HOST_DB_ PORT	MDS db port of MDS schema user to be used by UI and Host domain	1521	
90	MDS_HOST_DB_ SERVICE_NAME	MDS db service name of MDS schema user to be used by UI and Host domain	P84113A	
91	OPSS_SOA_ SCHEMA_USER	SOA OPSS schema name	SOA27_OPSS	
92	OPSS_SOA_ AUDIT_DBDS	SOA OPSS Audit schema name	SOA27_IAU_APPEND	
93	OPSS_SOA_ AUDIT_VIEWDS	SOA OPSS Audit View schema name	SOA27_IAU_VIEWER	
94	OPSS_SOA_ SCHEMA_	Password of SOA OPSS schema	welcome1	

Sr.No	Name	Description	Example Value	Value
	PASSWORD	name		
95	OPSS_SOA_DB_IP	IP address of SOA OPSS DB machine	10.180.84.113	
96	OPSS_SOA_DB_PORT	Port of SOA OPSS DB	1521	
97	OPSS_SOA_DB_SERVICE_NAME	Service name of SOA OPSS DB	P84113A	
98	HOST_ADMIN_JVM_PARAMS	Host domain admin JVM startup parameters	-Xms1024m -Xmx4096m	
99	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	
100	KEYSTORE_PASSWORD	Password for generating certificate	welcome1	
101	IPM_OUTBOUND_USERNAME	IPM Username created in connector	weblogic	
102	IPM_OUTBOUND_PASSWORD	Password for the IPM user in connector	weblogic1	
103	BIP_OUTBOUND_USERNAME	BIP Username created in	weblogic	

Sr.No	Name	Description	Example Value	Value
		connector		
104	BIP_OUTBOUND_PASSWORD	Password for the BIP user in connector	weblogic1	
105	ODI_OUTBOUND_USERNAME	ODI Username created in connector	weblogic	
106	ODI_OUTBOUND_PASSWORD	Password for the ODI user in connector	weblogic1	
107	OIM_OUTBOUND_USERNAME	OIM Username created in connector	weblogic	
108	OIM_OUTBOUND_PASSWORD	Password for the OIM user in connector	weblogic1	
109	WCM_OUTBOUND_USERNAME	WCM Username created in connector	weblogic	
110	WCM_OUTBOUND_PASSWORD	Password for the WCM user in connector	weblogic1	
111	OFFLINE_CHANNEL_OUTBOUND_USERNAME	Offline Username created in connector	offlineuser	
112	OFFLINE_CHANNEL_OUTBOUND_PASSWORD	Password for the Offline user in connector	welcome1	
113	SAML_ISSUER_OUTBOUND_USERNAME	SAML ISSUER Username created in connector	weblogic	
114	SAML_ISSUER_OUTBOUND_PASSWORD	Password for the SAML ISSUER user in connector	weblogic1	
115	BPEL_ENCRYPTION_OUTBOUND_USERNAME	BPEL_ENCRYPTION Username created in connector	weblogic	
116	BPEL_ENCRYPTION_	Password for the BPEL_	weblogic1	

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

Sr.No	Name	Description	Example Value	Value
130	POSUSER_OUTBOUND_PASSWORD	Password for the POS user in connector	welcome1	
131	DMSHOST_OUTBOUND_USERNAME	DMS HOST Username created in connector	weblogic	
132	DMSHOST_OUTBOUND_PASSWORD	Password for the DMS HOST user in connector	weblogic1	
133	DMSUI_OUTBOUND_USERNAME	DMS UI Username created in connector	weblogic	
134	DMSUI_OUTBOUND_PASSWORD	Password for the DMS UI user in connector	weblogic1	
135	OCH_OUTBOUND_USERNAME	OCH Username created in connector	weblogic	
136	OCH_OUTBOUND_PASSWORD	Password for the OCH user in connector	weblogic1	
137	WS_MFT_OUTBOUND_USERNAME	WS_MFT Username created in connector	weblogic	
138	WS_MFT_OUTBOUND_PASSWORD	Password for the WS_MFT user in connector	weblogic1	
139	OP_OUTBOUND_USERNAME	OP Username created in connector	weblogic	
140	OP_OUTBOUND_PASSWORD	Password for the OP user in connector	weblogic1	
141	ICS_OUTBOUND_USERNAME	Username for ICS connector	weblogic	
142	ICS_OUTBOUND_PASSWORD	Password for ICS connector	Weblogic1	
143	OBDX_OUTBOUND_USERNAME	Username for OBDX connector	1518675030085dean.white@test.com	
144	OBDX_OUTBOUND_PASSWORD	Password for OBDX connector	Welcome@1	

Sr.No	Name	Description	Example Value	Value
145	CARD_ USERNAME	Username of Card connector	orakey	
146	CARD_ PASSWORD	Password of Card connector	welcome1	
147	RULE_USERNAME	Username of Rule connector	orakey	
148	RULE_ PASSWORD	Password of Rule connector	welcome1	
149	BAM_USERNAME	Username of BAM connector	weblogic	
150	BAM_PASSWORD	Password of BAM connector	weblogic1	
151	COMMON_ OUTBOUND_ USERNAME	Username for common connector	Weblogic1	
152	COMMON_ OUTBOUND_ PASSWORD	Password for common connector	Weblogic1	
153	PM_OUTBOUND_ USERNAME	Username for PM connector	weblogic	
154	PM_OUTBOUND_ PASSWORD	Password for PM connector	weblogic1	
155	LENDING_ OUTBOUND_ USERNAME	Username for lending connector	weblogic	
156	LENDING_ OUTBOUND_ PASSWORD	Password for lending connector	weblogic1	
157	DEPOSITS_ OUTBOUND_ USERNAME	Username for deposits connector	weblogic	
158	DEPOSITS_ OUTBOUND_ PASSWORD	Password for deposits connector	weblogic1	
159	FW_OUTBOUND_ USERNAME	Username for FW connector	weblogic	
160	FW_OUTBOUND_ PASSWORD	Password for fw connector	weblogic1	
161	COLLECTION_ OUTBOUND_ USERNAME	Username for collection connector	weblogic	
162	COLLECTION_	Password for	weblogic1	

Sr.No	Name	Description	Example Value	Value
	OUTBOUND_ PASSWORD	collection Connector		
163	OR_OUTBOUND_ USERNAME	Username for OR connector	weblogic	
164	OR_OUTBOUND_ PASSWORD	Password for OR connector	weblogic1	
165	PARTY_ OUTBOUND_ USERNAME	Username for Party connector	weblogic	
166	PARTY_ OUTBOUND_ PASSWORD	Password for Party connector	weblogic1	
167	PRODPROC_ OUTBOUND_ USERNAME	Username for PRODPROC connector	weblogic	
168	PRODPROC_ OUTBOUND_ PASSWORD	Password for PRODPROC connector	weblogic1	
169	RECOVERY_ OUTBOUND_ USERNAME	Username for Recovery connector	weblogic	
170	RECOVERY_ OUTBOUND_ PASSWORD	Password for Recovery connector	weblogic1	
171	PRICING_ OUTBOUND_ USERNAME	Username for Pricing connector	weblogic	
172	PRICING_ OUTBOUND_ PASSWORD	Password for Pricing connector	weblogic1	
173	LCM_OUTBOUND_ USERNAME	Username for LCM connector	weblogic	
174	LCM_OUTBOUND_ PASSWORD	Password for LCM connector	weblogic1	
175	MDM_ OUTBOUND_ USERNAME	Username for MDM connector	weblogic	
176	MDM_ OUTBOUND_ PASSWORD	Password for MDM connector	weblogic1	
177	COMMUNICATIONS_OUTBOUND_ USERNAME	Username for COMMUNICATIONS connector	weblogic	

Sr.No	Name	Description	Example Value	Value
178	COMMUNICATIONS_OUTBOUND_PASSWORD	Password for COMMUNICATIONS connector	weblogic1	
179	APPCAPTURE_OUTBOUND_USERNAME	Username for APPCAPTURE connector	weblogic	
180	APPCAPTURE_OUTBOUND_PASSWORD	Password for APPCAPTURE connector	weblogic1	
181	EDN_OUTBOUND_USERNAME	Username for EDN connector	weblogic	
182	EDN_OUTBOUND_PASSWORD	Password for EDN connector	weblogic1	
183	EJBSUBJECT_USERNAME	Username for EJBSUBJECT connector	weblogic	
184	EJBSUBJECT_PASSWORD	Password for EJBSUBJECT connector	weblogic1	
185	USER_TIMEZONE	Time zone entry	+5:30	
186	HOST_SSL_PASSWORD	Password for configuring SSL in HOST domain	welcome1	

Table 2–6 Values for updating installobp.properties - For SOA***

Sr. No	Name	Description	Example Value	Value
1	SILENT_INSTALL	Flag for executing installer remotely	Y	
2	SECURITY_ENABLED	Flag for security enable	Y	
3	IPM_INSTALLED	Flag for if IPM is installed	Y	
4	BIP_INSTALLED	Flag for if BIP is installed	Y	
5	LOCAL_IP	I/P address	10.180.84.111	

Sr. No	Name	Description	Example Value	Value
		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.		
6	LOCAL_DISPLAY_ VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
7	DOMAIN_NAME	Name of the weblogic domain to be created	Host_domain or ui_domain or base_domain	
8	XD_COMPONENT_ NAME	XD Component name	obpsoa	
9	LOCALIZATION_TYPE	Type of localization	us	
10	DOMAIN_DIRECTORY_ LOCATION	Location where DOMAIN_ NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
11	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
12	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	
13	MDS_SCHEMA_USER	MDS schema user for SOA domain	MPUSSOA_MDS	
14	SOA_ INFRASTRUCTURE_	SOA infrastructure	MPUSSOA_SOAINFRA	

Sr. No	Name	Description	Example Value	Value
	SCHEMA_USER	schema user for SOA domain		
15	LOCAL_SCHEMA_USER	Local schema user for SOA domain	MPUSSOA_STB	
16	UMS_SCHEMA_USER	UMS schema user for SOA domain	MPUSSOA_UMS	
17	WLS_RUNTIME_SCHEMA_USER	WLS_RUNTIME schema user for SOA domain	MPUSSOA_WLS_RUNTIME	
18	DB_SCHEMA_PASSWORD	Password for MDS schema user	welcome1	
19	DB_IP	i/p address of MDS db machine	10.180.84.113	
20	DB_PORT	Port of MDS db port	1521	
21	DB_SERVICE_NAME	Service Name of MDS user	P84113A	
22	HOST_SCHEMA_USER	OBP Host Database username	OBP2712	
23	HOST_SCHEMA_PASSWORD	OBP Host Database password	welcome1	
24	HOST_DB_IP	OBP Host Database i/p address	10.180.84.113	
25	HOST_DB_PORT	OBP Host Database port	1521	
26	HOST_DB_SERVICE_NAME	OBP Host Database service name	P84113A	
27	ONS_NODE	i/p address of ONS service	10.180.84.113	
28	ONS_PORT	Port of ONS	6250	

Sr. No	Name	Description	Example Value	Value
		service		
29	OPSS_SOA_SCHEMA_USER	SOA OPSS Schema Name	SOA27_OPSS	
30	OPSS_SOA_AUDIT_DBDS	SOA OPSS AUDIT Schema name	SOA27_IAU_APPEND	
31	OPSS_SOA_AUDIT_VIEWDS	SOA OPSS AUDIT VIEWDS Schema name	SOA27_IAU_VIEWER	
32	OPSS_SOA_SCHEMA_PASSWORD	Password of OPSS_SOA_SCHEMA_USER	welcome1	
33	OPSS_SOA_DB_IP	i/p address of SOA OPSS DB.	10.180.84.113	
34	OPSS_SOA_DB_PORT	Port of SOA OPSS DB.	1521	
35	OPSS_SOA_DB_SERVICE_NAME	Service name of SOA OPSS DB.	P84113A	
36	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.112	
37	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
38	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen address	7002	
39	SOA_SERVER_LISTEN_ADDRESS	Listen address of SOA server	10.180.84.112	
40	SOA_SERVER_LISTEN_PORT	Listen port of SOA server	8001	
41	SOA_SERVER_SSL_LISTEN_PORT	SSL Listen port of SOA server	8002	
42	HUMANTASK_SERVER_LISTEN_ADDRESS	Listen address of humantask	10.180.84.112	

Sr. No	Name	Description	Example Value	Value
		server		
43	HUMANTASK_ SERVER_LISTEN_ PORT	Listen port of humantask server	9001	
44	HUMANTASK_ SERVER_SSL_ LISTEN_PORT	SSL listen port of humantask server	9002	
45	BAM_SERVER_ LISTEN_ADDRESS	Listen address of BAM server	10.180.84.112	
46	BAM_SERVER_ LISTEN_PORT	Listen port of BAM server	9003	
47	BAM_SERVER_SSL_ LISTEN_PORT	SSL Listen port of BAM server	9004	
48	HOST_ADMIN_ SERVER_LISTEN_ ADDRESS	Listen address of HOST admin server	10.180.84.110	
49	HOST_ADMIN_ SERVER_LISTEN_ PORT	Listen port of HOST admin server	7001	
50	HOST_MANAGED_ SERVER_LISTEN_ ADDRESS	Listen address of host managed server	10.180.84.110	
51	HOST_MANAGED_ SERVER_LISTEN_ PORT	Listen port of host managed server	8001	
52	OBEPM_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obepm managed server	10.180.4.113	
53	OBEPM_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obepm managed server	8003	
54	OBEDM_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obedm managed	10.40.80.141	

Sr. No	Name	Description	Example Value	Value
		server		
55	OBEDM_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obedm managed server	8003	
56	OBEO_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obeo managed server	10.180.4.98	
57	OBEO_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obeo managed server	8001	
58	OBPM_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obpm managed server	10.180.4.98	
59	OBPM_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obpm managed server	8003	
60	OBCCM_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of occm managed server	10.180.4.113	
61	OBCCM_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of occm managed server	8005	
62	OBLS_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obls managed server	10.40.73.121	
63	OBLS_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obls managed server	8001	
64	OBDLOC_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obdloc managed server	10.40.73.121	

Sr. No	Name	Description	Example Value	Value
65	OBDLOC_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obdloc managed server	8003	
66	OBEPR_HOST_ MANAGED_SERVER_ LISTEN_ADDRESS	Listen address of obepr managed server	10.180.4.113	
67	OBEPR_HOST_ MANAGED_SERVER_ LISTEN_PORT	Listen port of obepr managed server	8001	
68	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
69	OID_IP	I/P address of the OID server.	10.180.84.113	
70	OID_PORT	Port of the OID process instance.	3060	
71	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn=orcladmin	
72	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
73	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
74	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	ou=obp,cn=Users,dc=in,dc=oracle,dc=com	
75	NODE_MGR_PORT	Refers to the port number to be used for	5556	

Sr. No	Name	Description	Example Value	Value
		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		
76	SOA_IP	i/p address of SOA server	10.180.84.112	
77	SOA_CLUSTER_NAME	Cluster name of SOA server	obpsoa_cluster1	
78	SOA_SERVER_NAME	Server name of SOA server	soa_server1	
79	HUMAN_TASK_ CLUSTER_NAME	Cluster name of Humantask server	obphumantask_cluster1	
80	HUMAN_TASK_ SERVER_NAME	Server name of Humantask server	obphumantask_server1	
81	SOA_TARGET	Target folder of SOA machine where files will be copied temporarily during installation	/scratch/install/target	
82	SOA_JAVA_HOME	Refers to the home directory of java installation of	/scratch/app/product/jdk1.8.0_281	

Sr. No	Name	Description	Example Value	Value
		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.		
83	OUI_JAVA_HOME	Refers to the home directory of java installation.	/scratch/app/product/jdk1.8.0_281	
84	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory/	
85	SOA_MW_HOME	Refers to the middleware home of the weblogic installation on the SOA server.	/scratch/app/product/fmw	
86	UI_IP	i/p address of UI server	10.180.84.111	
87	UI_UNIX_USER	Linux login user id for UI server	ofssobp	
88	UI_DOMAIN_HOME	Full path of UI domain	/scratch/app/ product/fmw/ user_projects/ domains /ui_domain	
89	INSTALL_AS	Linux login user id used to install the OBP	ofssobp	

Sr. No	Name	Description	Example Value	Value
		solution.		
90	SOA_ADMIN_JVM_ PARAMS	SOA domain admin JVM startup parameters	-Xms1024m -Xmx2048m	
91	SOA_ HUMANTASKSERVER_ 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:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -Dobp.http.maxRetryCount=1 -Dobp.http.socketBufferSize=8192 -Dobp.http.maxConnectionsPerHost=20 -Dobp.http.expireAndRetry=true -Dobp.http.maxConnectionsPerHost=150 -Dobp.http.connectionTimeout=90000 -Dobp.http.connectionRequestTimeout=90000 -Dobp.http.idleTimeoutPollInterval=10000 -Dobp.http.staleCheckEnabled=true -Dweblogic.servlet.DIDisabled=true"	
92	SOA_MANAGED_JVM_ PARAMS	SOA domain managed soa server's JVM startup parameters	"-XX:NewSize=2048m -XX:MaxNewSize=4096m -XX:+UseParNewGC -XX:+CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -Xms11g -Xmx11g"	
93	KEYSTORE_ PASSWORD	Password for generating	welcome1	
94	UI_MANAGED_ SERVER_LISTEN_ ADDRESS	i/p address of UI Managed server	10.180.84.111	
95	UI_MANAGED_ SERVER_SSL_ LISTEN_PORT	Listen port of UI Managed server	8002	
96	UI_ADMIN_SERVER_ LISTEN_ADDRESS	UI_ADMIN_ SERVER_ LISTEN_ ADDRESS	i/p address of UI Admin server	
97	UI_ADMIN_SERVER_ LISTEN_PORT	UI_ADMIN_ SERVER_ LISTEN_ PORT	Listen port of UI Admin server	
98	DEFAULT_BANK_ CODE	Default bank code will be set while	8	

Sr. No	Name	Description	Example Value	Value
		configuring SOA domain		
99	DEFAULT_ TRANSACTION_ BRANCH_CODE	Default branch code will be set while configuring SOA domain	89999	
100	DEFAULT_TARGET_ UNIT	Default target unit will be set while configuring SOA domain	OBP_BU	
101	CARD_USERNAME	Username of Card connector.	orakey	
102	CARD_PASSWORD	Password of Card connector	welcome1	
103	RULE_USERNAME	Username of Rule connector	orakey	
104	RULE_PASSWORD	Password of Rule connector	welcome1	
105	USER_TIMEZONE	Time zone entry	+5:30	
106	SOA_SSL_PASSWORD	Password for configuring SSL in SOA domain	welcome1	
107	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
108	BAM_INSTALLATION	During SOA installation value Must be ‘N’ During BAM installation value Must be Y.	N	
109	IPM_USERNAME	Username of IPM connector	ofssobp	

Sr. No	Name	Description	Example Value	Value
110	IPM_PASSWORD	Password of IPM connector	welcome1	
111	OFFLINE_CHANNEL_OUTBOUND_USERNAME	Username of offline connector	offlineuser	
112	OFFLINE_CHANNEL_OUTBOUND_PASSWORD	Password of offline connector	welcome1	
113	FTP_IPM_USERNAME	Username of FTP_IPM connector	ofssobp	
114	FTP_IPM_PASSWORD	Password of FTP_IPM connector	ofssobp123	
115	FTP_IPM_BATCH_USERNAME	Username of FTP_IPM_BATCH connector	ofssobp	
116	FTP_IPM_BATCH_PASSWORD	Password of FTP_IPM_BATCH connector	ofssobp123	
117	SOA_OUTBOUND_USERNAME	Username of SOA connector	weblogic	
118	SOA_OUTBOUND_PASSWORD	Password of SOA connector	weblogic1	
119	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
120	IPM_SERVER_PORT	port of IPM server	16000	
121	IPM_UNIX_USER	Linux login user id for IPM server	ofssobp	
122	IPM_MW_HOME	Oracle IPM middleware Home directory on IPM server	/scratch/app/product/fmw	
123	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/wccontent	

Sr. No	Name	Description	Example Value	Value
124	BIP_SERVER_IP	I/P of the BIP server to host OBP reports	10.180.84.115	
125	BIP_SERVER_PORT	Port of the BIP server that hosts OBP reports	9502	
126	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
127	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
128	OAAM_SERVER_IP	oaam sever ip address	oaam-ofss.com	
129	OAAM_SERVER_PORT	oaam server port	14000	
130	OIM_SERVER_IP	oim server ip	oim-ofss.com	
131	OIM_SERVER_PORT	oim server port	16000	
132	OFSAA_SERVER_IP	ofss server ip	ofsaa-ofss.com	
133	OFSAA_SERVER_ PORT	ofss server port	17000	
134	DOCUMAKER_ SERVER_IP	documaker server ip	documaker-ofss.com	
135	DOCUMAKER_ SERVER_PORT	documaker server port	15000	
136	BAM_SERVER_NAME	Bam server name	bam-ofss.com	
137	BAM_SERVER_PORT	Bam server port	9003	
138	ODI_SERVER_NAME	Odi server name	odi-ofss.com	
139	ODI_SERVER_PORT	Odi server port	8001	

Table 2–7 Values for updating installobp.properties - For UI***

Sr.No	Name	Description	Example Value	Value
1	SILENT_INSTALL	Flag for	Y	

Sr.No	Name	Description	Example Value	Value
		executing installer remotely		
2	SECURITY_ENABLED	Flag for security enable	Y	
3	IPM_INSTALLED	Flag for if IPM is installed	Y	
4	BIP_INSTALLED		Y	
5	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	
6	LOCAL_DISPLAY_ VALUE	Value of DISPLAY variable to be exported to generate installation wizard in local machine	0	
7	DOMAIN_NAME	Weblogic Domain name	Host_domain or ui_domain or base_ domain	
8	XD_COMPONENT_ NAME	XD Component value	obpui	This will be always obpui
9	LOCALIZATION_TYPE	Type of localization	US	Depends on localization type
10	DOMAIN_ DIRECTORY_ LOCATION	Location where DOMAIN_ NAME folder will be created	/scratch/app/product/fmw/user_ projects/domains	
11	WEBLOGIC_ USERNAME	Username for weblogic domain	weblogic	
12	WEBLOGIC_ PASSWORD	Password for weblogic domain	weblogic1	

Sr.No	Name	Description	Example Value	Value
13	LOCAL_ DATASOURCE	Username of LOCAL_ DATASOURCE	COLLUI_STB	
14	WLS_RUNTIME_ SCHEMA_USER	Username of WLS Runtime schema	COLLUI_WLS_RUNTIME	
15	OPSS_UI_SCHEMA_ USER	OPSS UI schema name	COLLUI_OPSS	
16	OPSS_UI_SCHEMA_ PASSWORD	OPSS UI schema password	Welcome1	
17	OPSS_UI_DB_IP	OPSS UI DB IP	10.180.84.113	
18	OPSS_UI_DB_PORT	OPSS UI DB PORT	1521	
19	OPSS_UI_DB_ SERVICE_NAME	OPSS UI DB SERIVICE NAME	P84113A	
20	MDS_SCHEMA_USER	MDS schema name	COLLUI _MDS	
21	MDS_SCHEMA_ PASSWORD	Password of MDS schema	welcome1	
22	MDS_DB_IP	MDS DB IP	10.180.84.113	
23	MDS_DB_PORT	MDS DB PORT	1521	
24	MDS_DB_SERVICE_ NAME	MDS DB SERVIVE NAME	P84113A	
25	OPSS_HOST_ SCHEMA_USER	HOST OPSS Schema name	COLLMW _OPSS	
26	OPSS_HOST_AUDIT_ DBDS	HOST OPSS AUDIT schema name	COLLMW_IAU_APPEND	
27	OPSS_HOST_AUDIT_ VIEWDS	HOST OPSS AUDIT VIEWDB Schema name	COLLMW_IAU_VIEWER	
28	OPSS_HOST_ SCHEMA_ PASSWORD	HOST OPSS password for above three OPSS schema	welcome1	
29	OPSS_HOST_DB_IP	Service name of UI OPSS DB	10.180.84.113	
30	OPSS_HOST_DB_ PORT	HOST OPSS DB PORT	1521	

Sr.No	Name	Description	Example Value	Value
31	OPSS_HOST_DB_SERVICE_NAME	HOST OPSS DB SERVICE NAME	P84113A	
32	HOST_SCHEMA_USER	OBP Host Database username	OBEDMUS211	
33	HOST_SCHEMA_PASSWORD	OBP Host Database password	welcome1	
34	HOST_DB_IP	OBP Host Database i/p address	10.180.84.113	
35	HOST_DB_PORT	OBP Host Database listen port	1521	
36	HOST_DB_SERVICE_NAME	OBP Host Database service name	P84113A	
37	ONS_NODE	i/p address of ONS service	10.180.84.113	
38	ONS_PORT	Listen port of ONS service	6200	
39	ADMIN_SERVER_LISTEN_ADDRESS	Admin server listen address	10.180.84.111	
40	ADMIN_SERVER_LISTEN_PORT	Admin server listen port	7001	
41	ADMIN_SERVER_SSL_LISTEN_PORT	Admin server SSL listen port	7002	
42	MANAGED_SERVER_LISTEN_ADDRESS	Managed server listen address	10.180.84.111	
43	MANAGED_SERVER_LISTEN_PORT	Managed server listen port	8001	
44	MANAGED_SERVER_SSL_LISTEN_PORT	Managed server SSL listen port	8002	
45	LDAP_PROVIDER	Refers to LDAP Provider .Value will be OID or OVD.	OID	
46	OID_IP	I/P address of the OID server	10.180.84.113	
47	OID_PORT	Port of the OID process instance.	3060	

Sr.No	Name	Description	Example Value	Value
48	OID_ADMIN_USER	Admin user id which can be used to login of the OID as administrator.	cn=orcladmin	
49	OID_ADMIN_PWD	Refers to the password of admin user of the OID	welcome1	
50	OID_GROUP_DSN	The DSN used for object class Groups in the OID ldap.	cn=Groups,dc=in,dc=oracle,dc=com	
51	OID_USER_DSN	The DSN used for object class Users in the OID ldap.	cn=Users,dc=in,dc=oracle,dc=com	
52	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	
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_CLUSTER_NAME	Name of UI Managed Cluster	obpui_cluster1	
55	UI_SERVER_NAME	Name of UI Managed Server	obpui_server1	
56	UI_TARGET	Refers to a location on the UI server where the installables	/scratch/install/target	

Sr.No	Name	Description	Example Value	Value
		can be transferred. The user id of the use used for installation of OBP should have read, write and execute privileges on this directory.		
57	UI_MW_HOME	Refers to the middleware home of the weblogic installation on the UI server.	/scratch/app/product/fmw	
58	UI_JAVA_HOME	Refers to the home directory of java installation. The version of java installed should be 1.8.0 or above. This is used to execute the OBP security policies policy seeding utility at the end of the installation.	/scratch/app/product/jdk1.8.0_231	
59	OUI_JAVA_HOME	Refers to the home directory of java installation. The version of java installed should be 1.8.0 . This is used for OBP patching.	/scratch/app/product/jdk1.8.0_231	
60	CENTRAL_ INVENTORY_LOC	Refers to the path of central inventory. This path is used for oui patching.	/scratch/app/oraInventory	
61	INSTALL_AS	Linux login user id used to install the OBP solution.	ofssobp	
62	IPM_UNIX_USER	Linux login user id of IPM server	ofssobp	

Sr.No	Name	Description	Example Value	Value
63	IPM_SERVER_IP	i/p address of IPM server	10.180.84.114	
64	IPM_SERVER_PORT	Listen port of IPM server	16000	
65	IPM_MW_HOME	Oracle Weblogic Home directory on IPM server	/scratch/app/product/fmw	
66	IPM_HOME	Oracle IPM Home directory on IPM server	/scratch/app/product/fmw/Oracle_ECM1	
67	BIP_SERVER_IP	I/P of the BIP server to host OBP reports	10.180.84.115	
68	BIP_SERVER_PORT	Port of the BIP server that hosts OBP reports	9502	
69	BIP_UNIX_USER	Linux login user id for BIP server	ofssobp	
70	BIP_HOME	Oracle BIP Home directory on BIP server	/scratch/app/product/fmw/bi	
71	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	
72	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	
73	OIM_SERVER_IP	Oracle Identity Manager i/p address	oim-ofss.com	
74	OIM_SERVER_PORT	Oracle Identity	16000	

Sr.No	Name	Description	Example Value	Value
		Manager Listen Port		
75	OFSAA_SERVER_IP	OFSAA Server i/p address	ofsaa-ofss.com	
76	OFSAA_SERVER_ PORT	OFSAA Server listen port	17000	
77	UI_ADMIN_JVM_ PARAMS	UI domain admin JVM startup parameters	-Xms2048m -Xmx4096m	
78	UI_MANAGED_JVM_ PARAMS	UI domain managed JVM startup parameters	-Djbo.ampoo l.doampooling=false -Xms6g -Xmx6g -XX:NewSize=512m -XX:MaxNewSize =2048m -XX:+UseParNewGC -XX:+CMSParallel RemarkEnabled -XX:+UseConcMark SweepGC -XX:CMSInitiating Occupancy Fraction=75 -Djbo.load.com ponents.lazily=true	
79	HOST_ADMIN_ SERVER_LISTEN_ ADDRESS	Listen address of HOST admin server	10.180.84.110	
80	HOST_ADMIN_ SERVER_LISTEN_ PORT	Listen port of HOST admin server	7001	
81	HOST_MANAGED_ SERVER_LISTEN_ ADDRESS	Listen address of host managed server	10.180.84.110	
82	HOST_MANAGED_ SERVER_LISTEN_ PORT	Listen port of host managed server	8001	
83	SOA_MANAGED_ SERVER_LISTEN_ ADDRESS	Listen address of SOA server	10.180.84.112	
84	SOA_MANAGED_ SERVER_LISTEN_ PORT	Listen port of SOA server	8001	
85	SOA_ADMIN_ SERVER_LISTEN_ ADDRESS	Listen address of SOA Admin server	10.180.84.112	
86	SOA_ADMIN_ SERVER_LISTEN_	Listen port of SOA Admin	7001	

Sr.No	Name	Description	Example Value	Value
	PORT	server		
87	KEYSTORE_ PASSWORD	Password for generating certificate	welcome1	
88	UI_SSL_PASSWORD	Password for configuring SSL in UI domain	welcome1	
89	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	
90	UCM_IP	UCM_IP the IP address of the UCM WebLogic managed server.	ofss.ucm.com	
91	UCM_PORT	Port of UCM.	4444	
92	OFFLINE_CHANNEL_ OUTBOUND_ USERNAME	Offline username created in connector	offlineuser	

Sr.No	Name	Description	Example Value	Value
93	OFFLINE_CHANNEL_OUTBOUND_PASSWORD	Password for the Offlineuser user in connector	welcome1	
94	CARD_USERNAME	Username of Card connector.	orakey	
95	CARD_PASSWORD	Password of Card connector.	welcome1	
96	RULE_USERNAME	Username of Rule connector	orakey	
97	RULE_PASSWORD	Password of Rule connector	welcome1	
98	USER_TIMEZONE	Time zone entry	+5:30	
99	REMOTE_EXECUTION	Flag for executing installer remotely	Y	
100	IPM_USERNAME	Username of IPM connector	weblogic	
101	IPM_PASSWORD	Password of IPM connector	weblogic1	
102	FTP_IPM_USERNAME	Username of FTP_IPM connector	ofssobp	
103	FTP_IPM_PASSWORD	Password of FTP_IPM connector	ofssobp123	
104	FTP_IPM_BATCH_USERNAME	Username of FTP_IPM_BATCH	ofssobp	
105	FTP_IPM_BATCH_PASSWORD	Password of FTP_IPM_BATCH	ofssobp123	
106	HOST_UNIX_USER	Linux login user id for HOST server	ofssobp	
107	HOST_MW_HOME	Refers to the middleware home of the weblogic installation on the Host server.	/scratch/app/product/fmw	
108	SOA_MW_HOME	Refers to the middleware	/scratch/app/product/fmw	

Sr.No	Name	Description	Example Value	Value
		home of the weblogic installation on the SOA server.		
109	SOA_DOMAIN_NAME	Domain name of SOA	base_domain	

2.4.3 Database and WebLogic Domain Configuration

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

Table 2–8 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 OBEO Oracle DB server	10.180.90.30	
6	Port of the OBEO Oracle DB instance	1521	
7	OBEO DB Service Name	OBPDB	
8	OBEO 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 OBEO 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 OBEO UI domain for:	Default Values	

Sr. No.	Name	Description and Example	Value
	Admin server HTTP port for managed server HTTPS port for managed server	Admin Server Port: 7001 Managed Server http port: 15308 Managed Server https port: 15309	
13	Password for the key generated to establish trust between the OBEO UI and Host.	Decide on the password to be used and note it. This is required for the post installation tasks of UI domain.	
14	Password for keystore generated to establish trust.	Decide on the password to be used and note it. This is required for the post installation tasks UI domain.	
Additional Host Install Checklist			
15	Admin user id and password for the OBEO 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 OBEO 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 OBEO UI and Host.	This is same as password in row 11. This is required for the post installation tasks of host domain.	
18	Password for keystore generated to establish trust.	This is same as password in row 12. This is required for the post installation tasks of host domain.	

2.5 OID Schema Setup – Custom OBEO Schema

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

2.5.1 Prerequisite – OID setup

I4.1. It is assumed that OID 12.2.1.4.0 is installed with ODSM and configured.

2.5.2 Verify the OID installation

This section describes the procedure to verify the OID installation.

2.5.2.1 Start and Verify the OID processes

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

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

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

./startComponent.sh oid1

2.5.2.2 OPSS/OID Performance Tuning

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

Parameters

Change the parameter values as provided below.

Table 2–9 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 2–10 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;

Sr. No.	DB Property Name	Suggested Value for Tuning	Alter Command
2	SGA Target	3G	ALTER SYSTEM SET sga_target = 3221225472 SCOPE = spfile;
3	Audit Trail	None	ALTER SYSTEM SET audit_sys_ operations=FALSE SCOPE =SPFILE; ALTER SYSTEM SET audit_trail = NONE SCOPE = spfile;
4	Open Cursor	500	ALTER SYSTEM SET open_cursors = 500 SCOPE = spfile;
5	PGA_Aggregate_Target	1.5GB	ALTER SYSTEM SET pga_aggregate_ target = 1610612736 SCOPE = spfile;
6	NLS Sort	Binary	ALTER SYSTEM SET nls_sort = BINARY SCOPE = spfile;
7	Filesystemio_Options	SETALL	ALTER SYSTEM SET filesystemio_ options = SETALL SCOPE = spfile;
8	Fast_start_mttr_target	3600	ALTER SYSTEM SET fast_start_mttr_ target = 3600 SCOPE = spfile;
9	db_securefile	ALWAYS	ALTER SYSTEM SET db_securefile = ALWAYS SCOPE = spfile;
10	Session_cached_ cursors	500	ALTER SYSTEM SET session_ cached_cursors = 500 SCOPE = spfile;
11	plsql_code_type	NATIVE	ALTER SYSTEM SET plsql_code_ type = NATIVE SCOPE = spfile;
12	_b_tree_bitmap_plans	false	ALTER SYSTEM SET "_b_tree_ bitmap_plans" = FALSE scope=spfile;
13	Memory_target	0	ALTER SYSTEM SET memory_ target=0 SCOPE = SPFILE;

b. Redo log file.

Allocated Disk Space for Redo Log Files

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

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

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

c. Undo tablespace.

Increase Disk Space Allocated for UNDO Tablespace

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

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

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

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

   b. Add following properties:

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

```
<propertySet name="props.db.1">
<property name="authorization_cache_enabled"
value="true"/>
<property name="connection.pool.min.size" value="20"/>
<property name="connection.pool.max.size" value="40"/>
<property name="connection.pool.provider.type"
value="IDM"/>
<property name="connection.pool.timeout" value="300000"/>
<property name="connection.pool.provider.type"
value="5"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.t
ype" value="STATIC"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
trategy" value="NONE"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.s
ize" value="100"/>
<property
name="oracle.security.jps.policystore.policy.lazy.load.e
nable" value="true"/>
<property
name="oracle.security.jps.policystore.policy.cache.strat
egy" value="NONE"/>
```

```
<property
name="oracle.security.jps.policystore.policy.cache.size"
value="1000000"/>
<property
name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
<property
name="oracle.security.jps.policystore.refresh.purge.time
out" value="43200000"/>
<property
name="oracle.security.jps.ldap.policystore.refresh.inter
val" value="6000000"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.w
armup.enable" value="true"/>
</propertySet>
```

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

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

```
<property
name="oracle.security.jps.policystore.policy.cache.size"
value="1000000"/>
<property
name="oracle.security.jps.policystore.refresh.enable"
value="true"/>
<property
name="oracle.security.jps.policystore.refresh.purge.time
out" value="43200000"/>
<property
name="oracle.security.jps.ldap.policystore.refresh.inter
val" value="6000000"/>
<property
name="oracle.security.jps.policystore.rolemember.cache.w
armup.enable" value="true"/>
</serviceInstance>
```

3. adf-config.xml (optional)

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

4. setDomainEnv.sh

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

   Table 2–11 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

Property	Description
Djps.auth.debug=false	Turn off debugging. This is turned on to debug access denied errors.
Djps.subject.cache.key=5	JPS uses a Subject Resolver to convert a platform subject to JpsSubject which contains user/enterprise-role information, as well as ApplicationRole information. This information is represented as principals in the subject. Value = 5: Instead of using the whole subject as the key, this settings uses a subset of the principal set inside the subject as the key (actually use principals of WLSUSerImpl type). This setting will accelerate the cache retrieval operation if the subject has a large principal set.
Djps.subject.cache.ttl=600000	Cache's Time To Live (TTL) for case '5' (above). This system property controls how long the cache is valid. When the time expired, the cached value is dumped. The setting can be controlled by the flag of -Djps.subject.cache.ttl=xxxx, where 'xxx' is the duration in milliseconds. Consider setting the duration of this TTL setting to the same value as the value used for the group and user cache TTL in WLS LDAP authenticator.

Example:

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

export JAVA_PROPERTIES
```

2.5.2.3 Import OBEO 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 OBEO.

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

Note

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

1. Extract the 'obpus-host.zip' or 'obpau-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 2–12 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
```

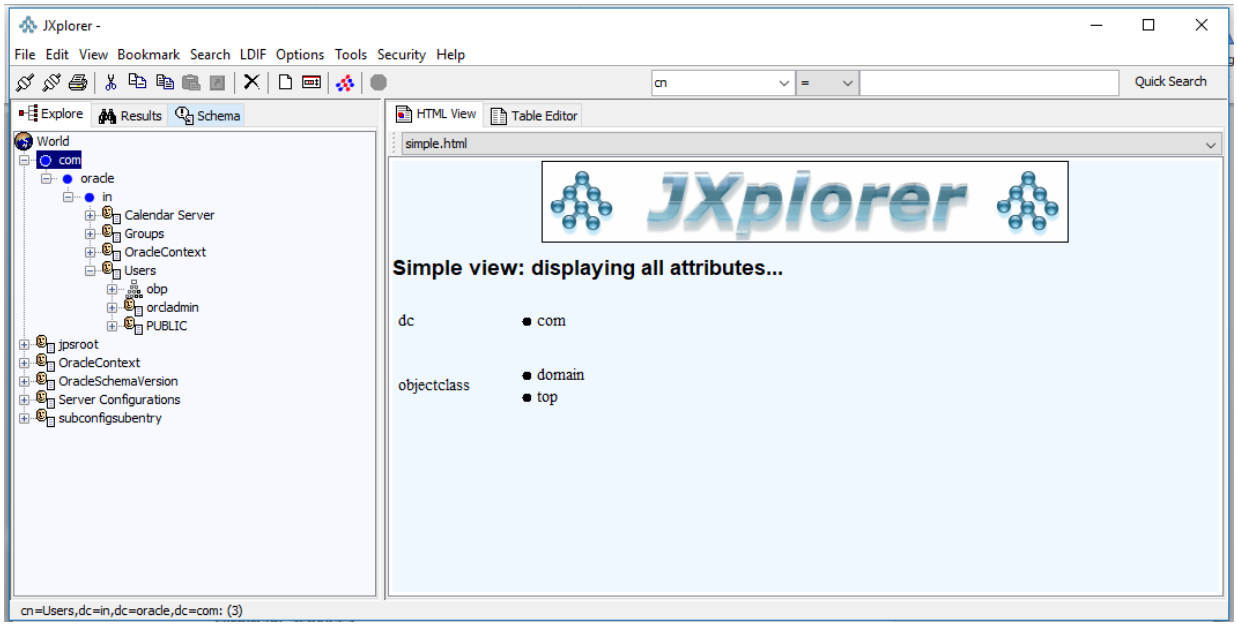
ldapadd Administrators.ldif

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

2.5.2.4 Verify the import using ODSM or JXplorer

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

Figure 2–2 JXplorer



3 OBEO Localization SOA Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Enterprise Originations Localization SOA Media Pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

3.1 Installation and Configuration Procedure

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

3.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBEO 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' or'obpau-ui-soa.zip' to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Three files will be extracted:

- A zip file 'obpinstall-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 2.4 Installation Checklist of this guide and note the values applicable for each point in the last column for 'Value' so that the same is handy during the actual installation.

3.1.2 Pre-Installation Steps

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

Step 1 Updating installobpsoa.properties

Navigate to the directory where the files obpinstall-ui-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 7.1 Pre-Installation Steps and Section 7.2 OBEO Database Setup – RCU Installation.

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

Step 3 OS Level Tuning

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

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

For more information, see the following document:

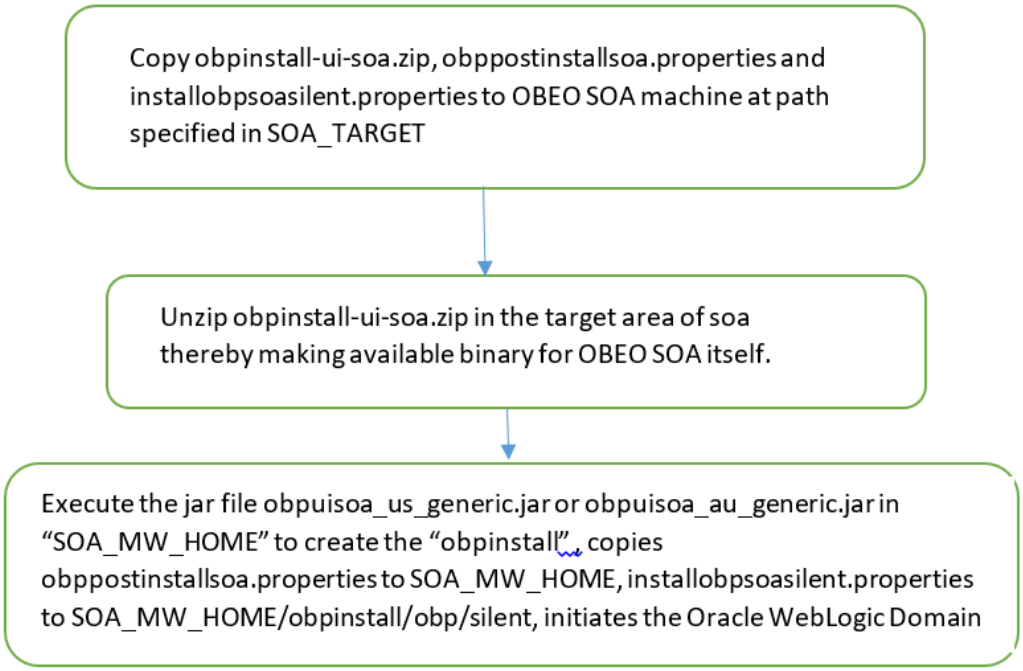
http://www.oracle.com/technetwork/database/availability/maa-fmwsharedstoragebestpractices-402094.pdf

3.1.3 Installation Steps

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

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

Figure 3–1 Steps in installobpsoa.sh script



A sample output is given here.

./installobpsoa.sh

Figure 3–2 Verification of Properties

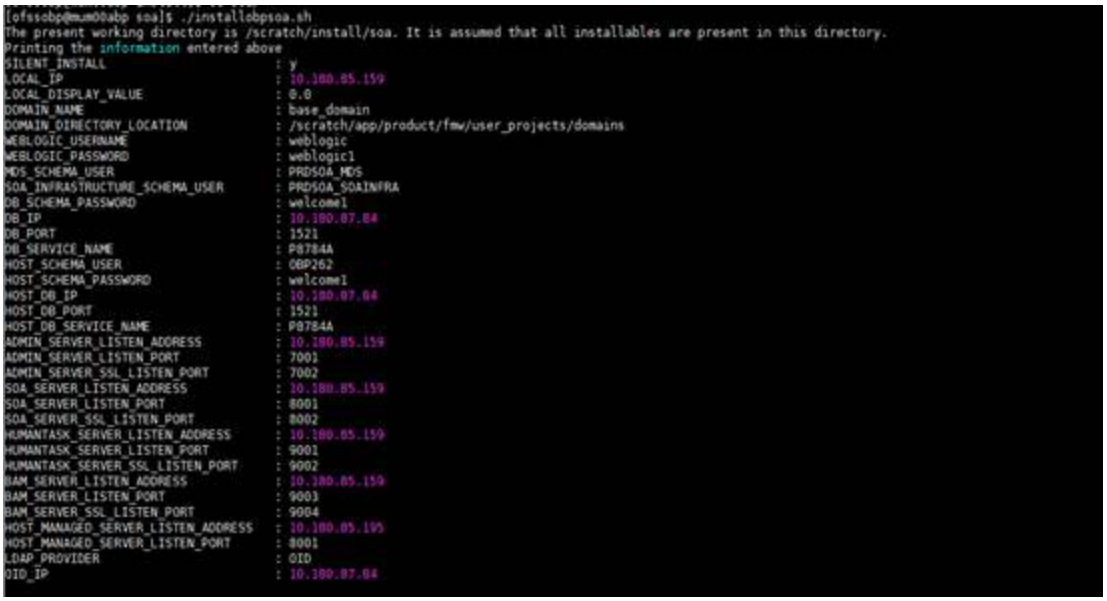


Figure 3–3 Verification of Properties

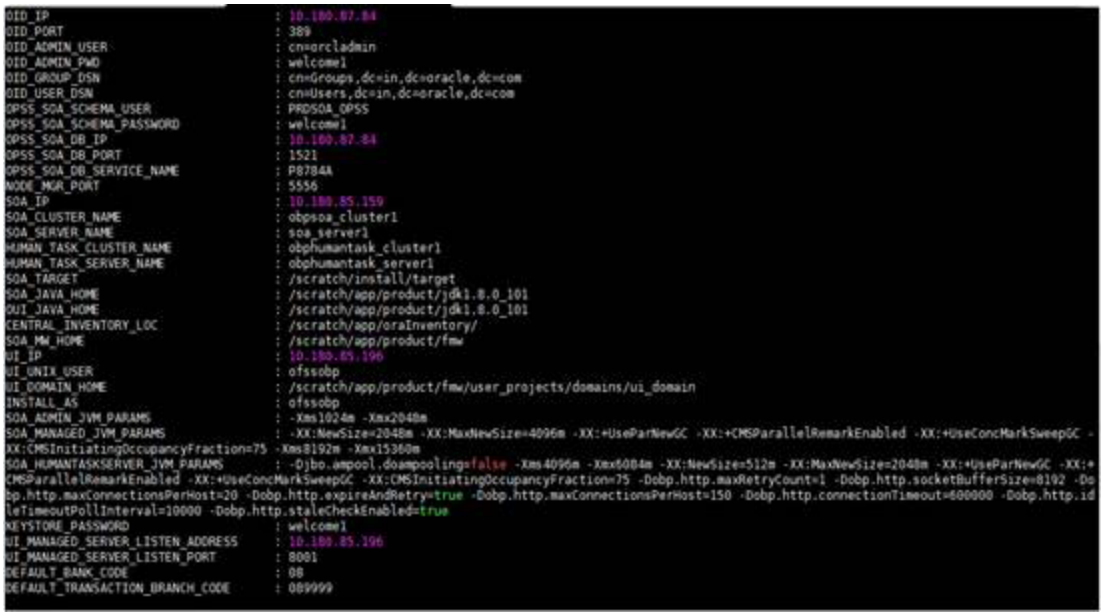
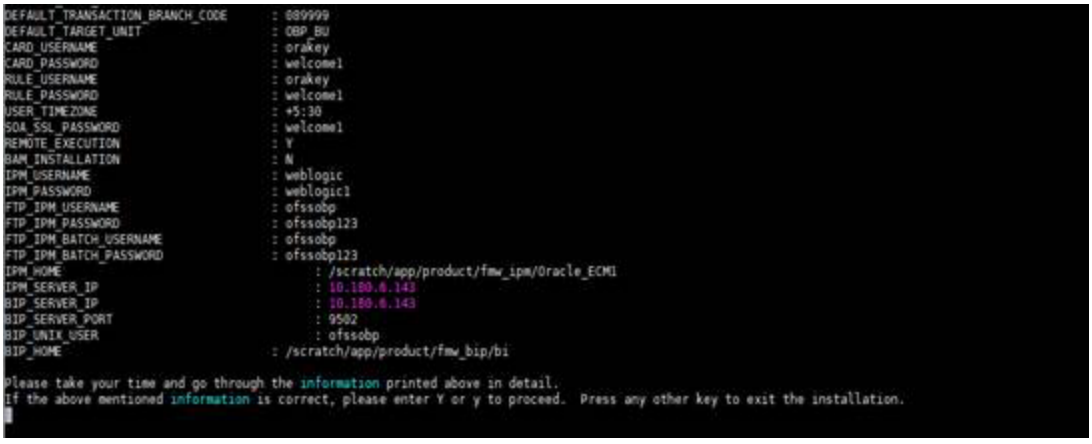


Figure 3–4 Confirmation to Proceed Domain Installation (cont.)



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

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

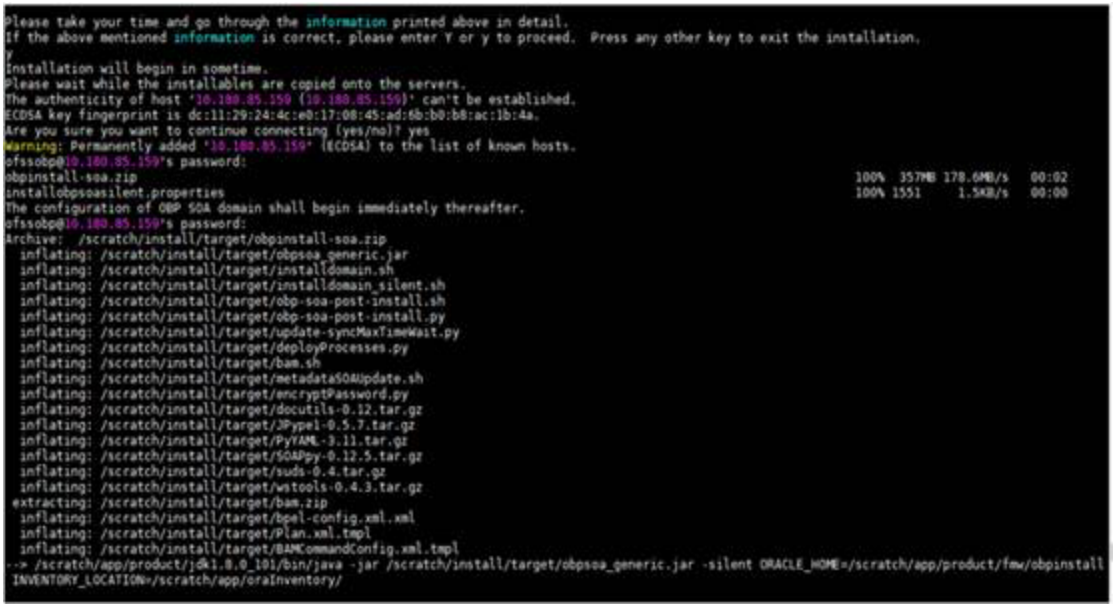


Figure 3–6 Copying and Extraction of obpinstall-ui-soa.zip

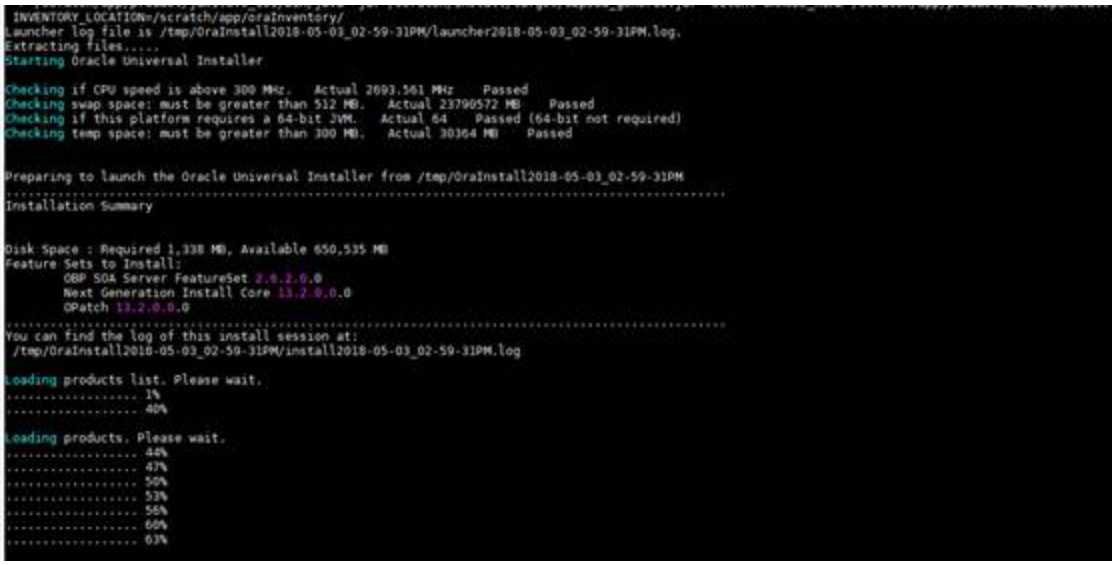


Figure 3–7 Copying and Extraction of obpinstall-ui-soa.zip

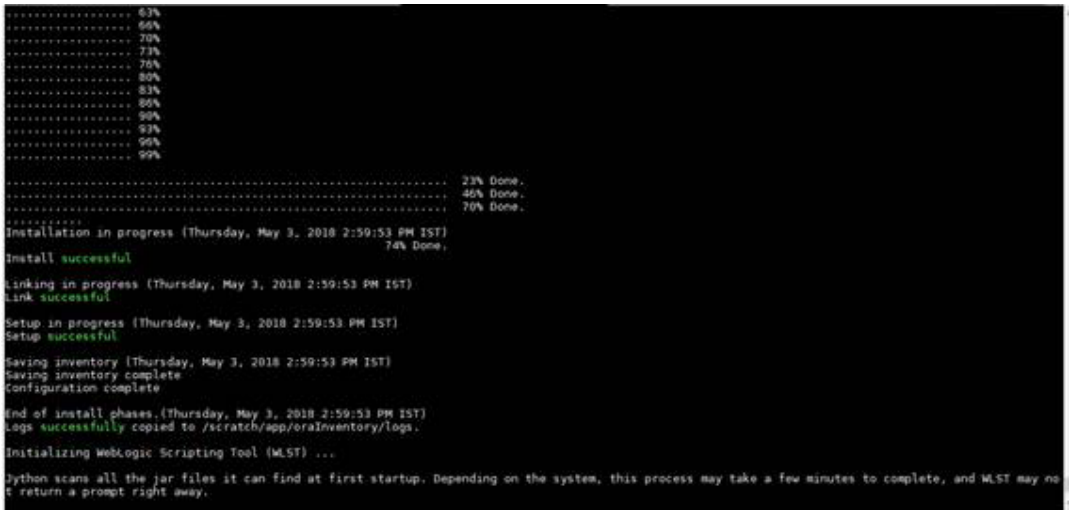


Figure 3–8 Domain Creation Confirmation

3.2 Post Installation Configuration

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

Checklist for Post Installation Procedure

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

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

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

Post Installation Configuration

1. Start the OBEO 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

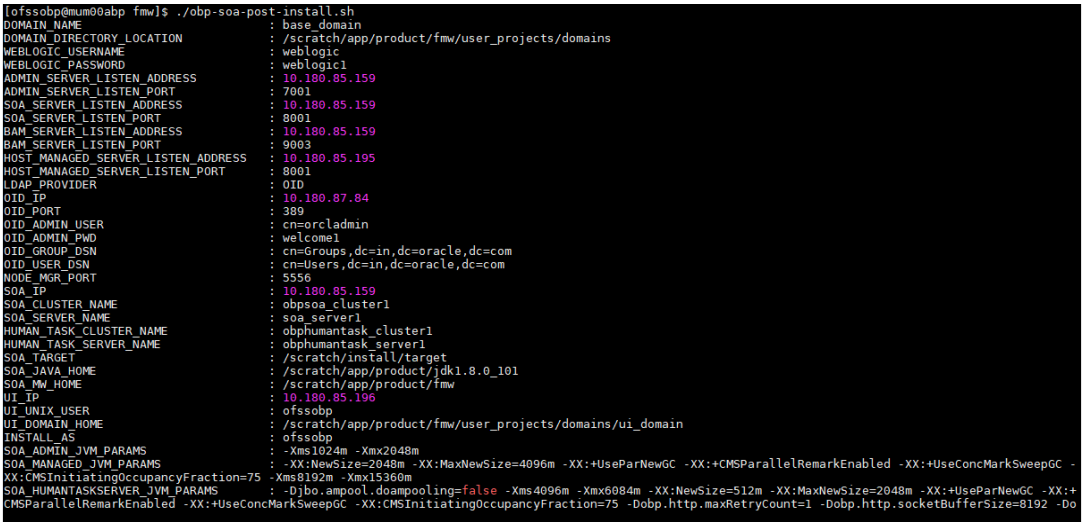


Figure 3–10 Starting Post Installation (contd)

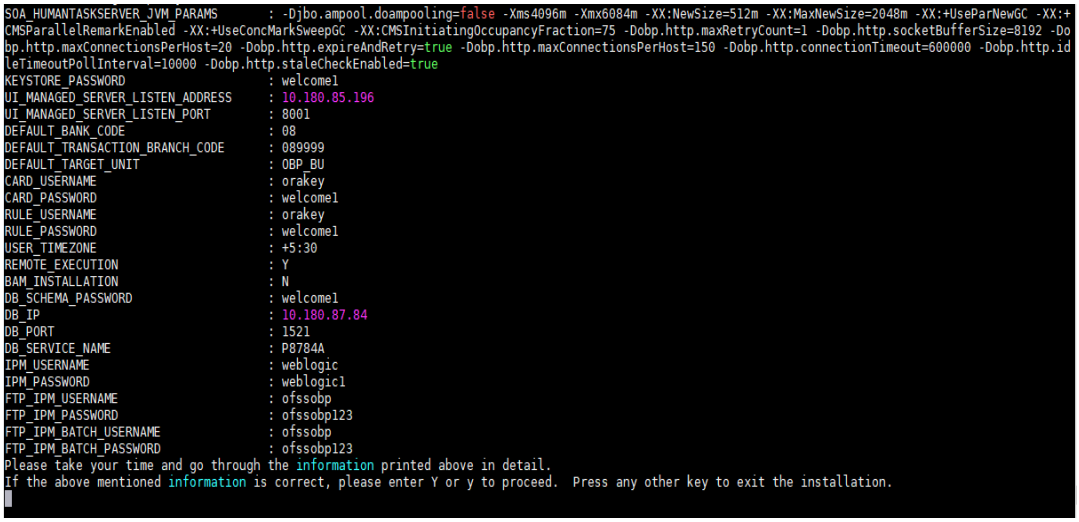


Figure 3–11 Starting Post Installation (contd)

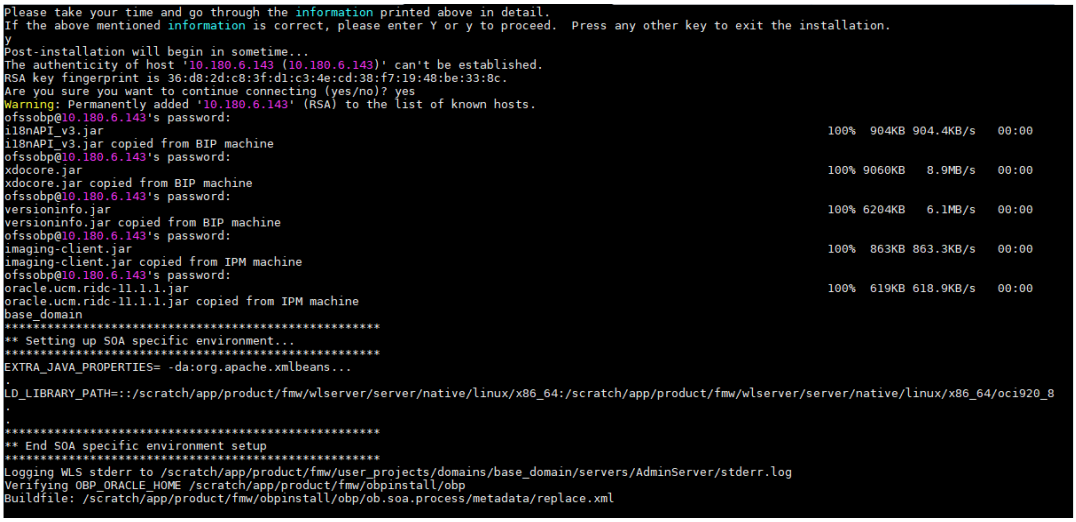
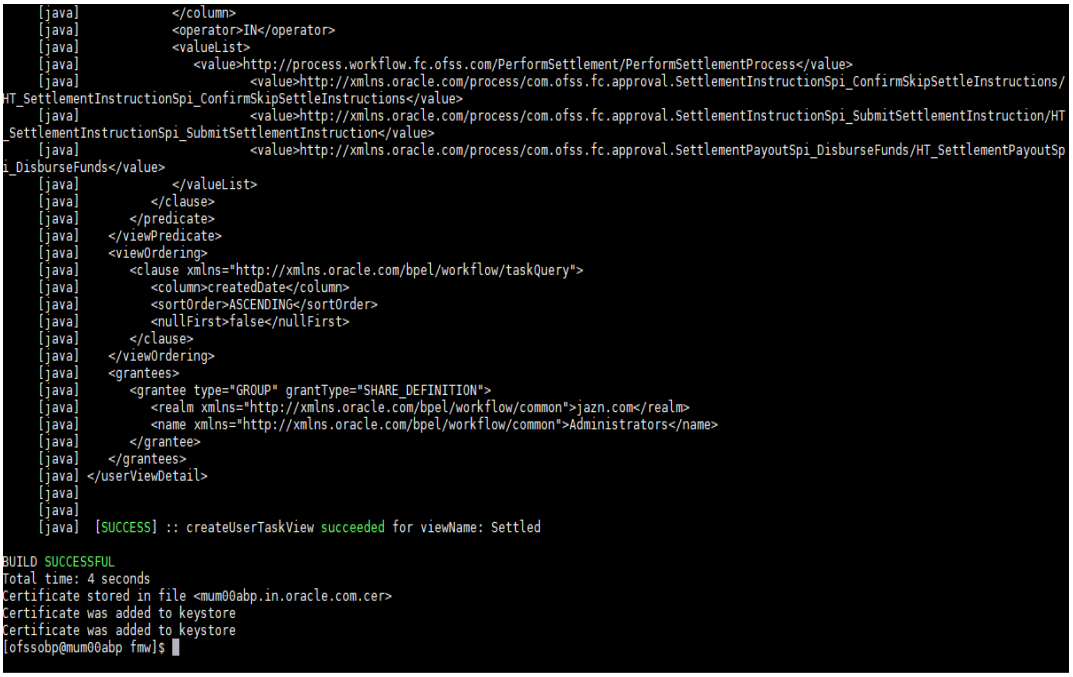


Figure 3–12 Starting Post Installation (contd)

Figure 3–13 SOA Post Installation Completion



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

   deploy-composite-SOA-WLST.log

   post-obp-SOA-WLST.log

   post-soa-GrantAndPolicySet-log.log

   post-soa-taskflow-grants.log

update-syncMaxTimeWait.log

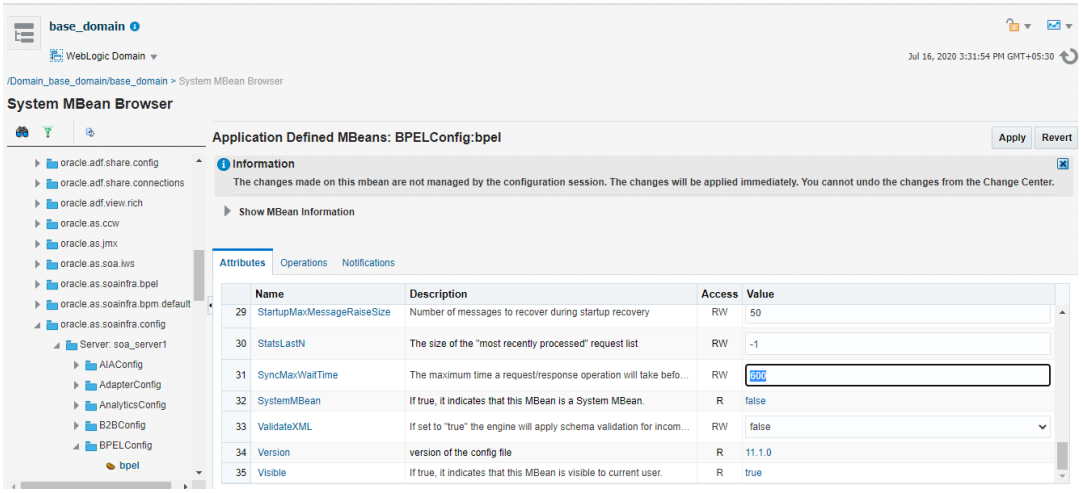
obp-soa-install-log.txt

7. SyncMaxWaitTime value from 45 to 600

    a. Login to SOA EM and click on

    base_domain -> System Mbean Browser -->Application Defined Mbeans -> -> oracle.as.soainfra.config --> Server: soa_server1 --> BPELConfig--> bpel

Figure 3–14 Go to BPEL Config

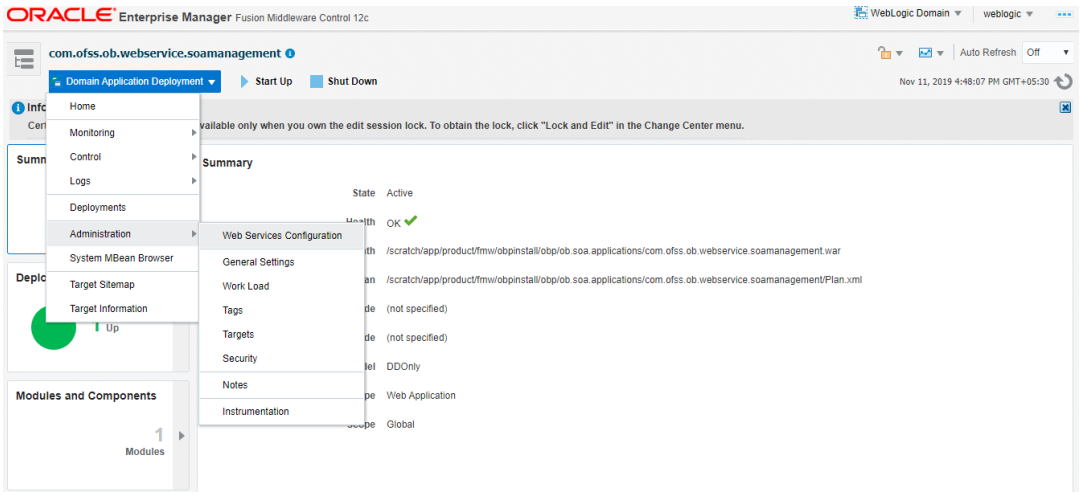


8. Restart SOA admin and SOA managed server and obphumantask server.
9. After completion of restart, attach the oracle/wss_saml_or_username_token_service_policy in com.ofss.ob.webservice.soamanagement.war. To attach the policy:

    a. Log in to SOA EM.

    b. Click Application Deployments > com.ofss.ob.webservice.soamanagement > Domain Application Deployment > Administration > Web Services Configuration.

Figure 3–15 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 3–16 Attach Policy

4 OBEO Localization Host Media Pack Installation

This chapter details every step involved in the installation of Oracle Banking Enterprise Originations Localization Host Media Pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

4.1 Installation and Configuration Procedure

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

4.1.1 Preparatory Steps

This section lists the preparatory steps required for the OBEO 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 to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Below files will be extracted:

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

Step 3 Printing Checklists

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

4.1.2 Pre-Installation Steps

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

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

The following table lists the XD components.

Table 4–1 XD Components

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

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

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

XD Component Name	MW_HOME	Domain Name	Server Name or Cluster Name
batchhost	/scratch/app/product/fmw	host_ domain	obphost_ server1/obphost_ cluster1
obepmhost	/scratch/app/product/fmw_pm	obepm_ domain	obepm_ server1/obepm_ cluster1
obeohost	/scratch/app/product/fmw_or	obeo_ domain	obeo_server1/obeo_ cluster1
obpmhost	/scratch/app/product/fmw_party	obparty_ domain	obparty_ server1/obparty_ cluster1
obshhost	/scratch/app/product/fmw_sh	obsh_ domain	obshared_ server1/obshared_ cluster1
obeprhost	/scratch/app/product/fmw_pr	obpr_ domain	obpr_server1/obpr_ cluster1
obccmhost	/scratch/app/product/fmw_occm	occm_ domain	occm_server1/occm_ cluster1

Memory Parameters

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

Batchhost Installation Steps

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

Step 1 Updating installobphost.properties

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

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

- OID_FARM_AND_POLICY_SEEDING_FLAG
- BIP_REPORTS_UPLOADING_FLAG

Step 2 Checklist for a new setup

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

- Please make sure required RCU schemas have been created. For more information, see Section 7.1 Pre-Installation Steps and Section 7.2 OBEO Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against HOST_TARGET property.
- In case of re-installation ensure that the directory paths against DOMAIN_DIRECTORY_LOCATION, HOST_TARGET and HOST_MW_HOME specified in installobphost.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- No processes should be running on the port in HOST machine given in installobphost.properties.
- Values in installobphost.properties must be correct. At run time no option is given to change them.
- No other schema should exist in db with the same prefix as HOST_DB_SCHEMA_PREFIX specified in installobphost.properties. OBP_HOST_DB_USER should be given on the basis of HOST_DB_SCHEMA_PREFIX.

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

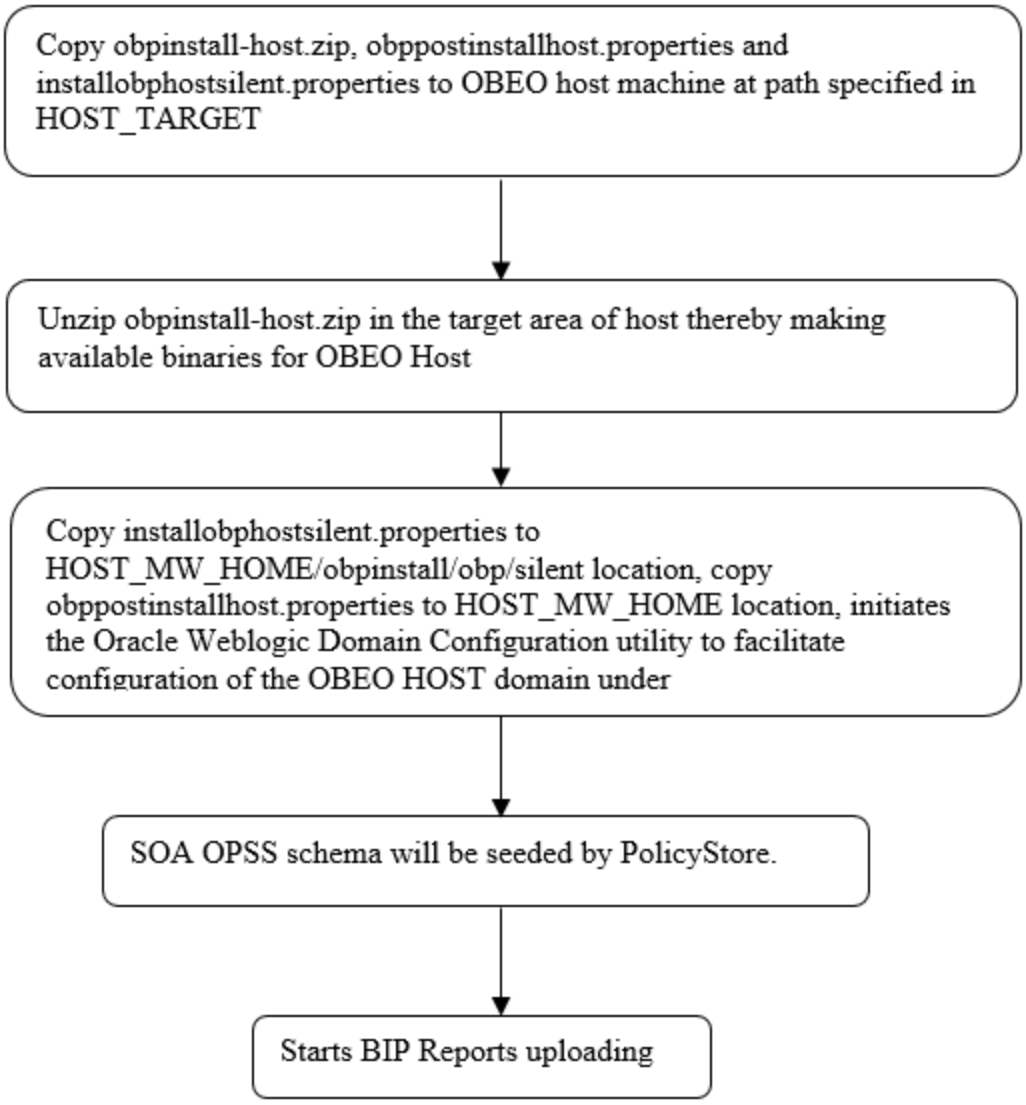
- OBP_HOST_DB_USER and BIP_DATASOURCE_NAME must be same in installobphost.properties.
- The following schemas are manually created prior to installation and are available for updation in the checklist:
  - OBP_HOST_DB_USER (by RCU)
- MDS_HOST_DB_USER as updated in installobphost.properties and MDS_SCHEMA_USER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

4.1.3 Installation Steps

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

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

Figure 4–1 Steps in installobphost.sh script



A sample output is given here.

Figure 4–2 Verification of Properties

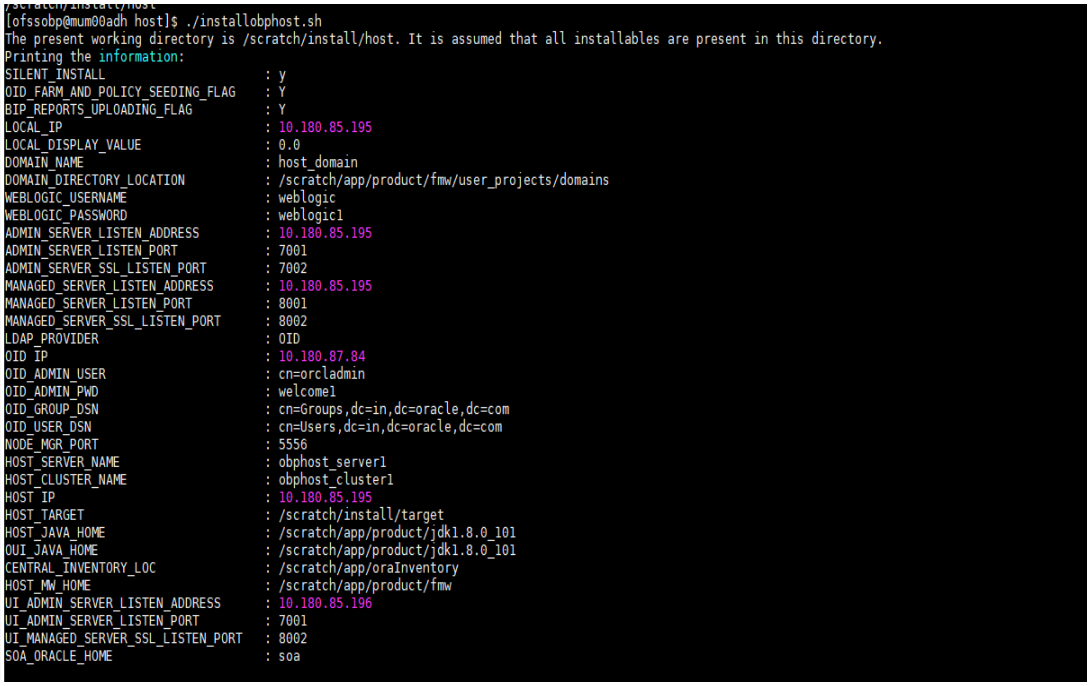


Figure 4–3 Verification of Properties (contd)

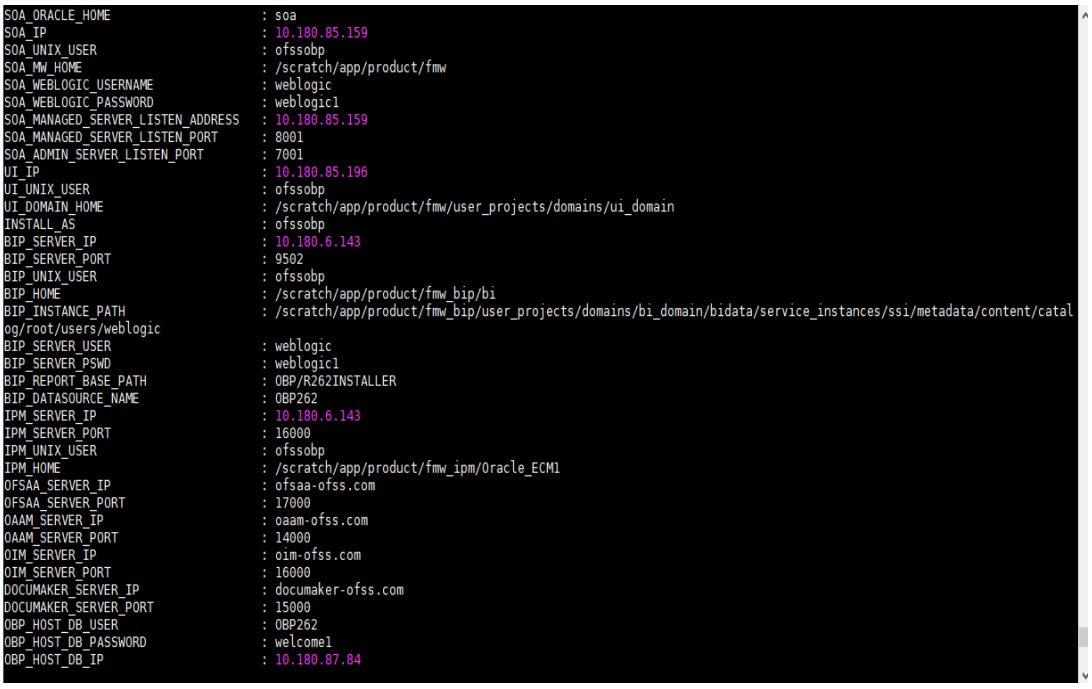


Figure 4–4 Verification of Properties (contd)

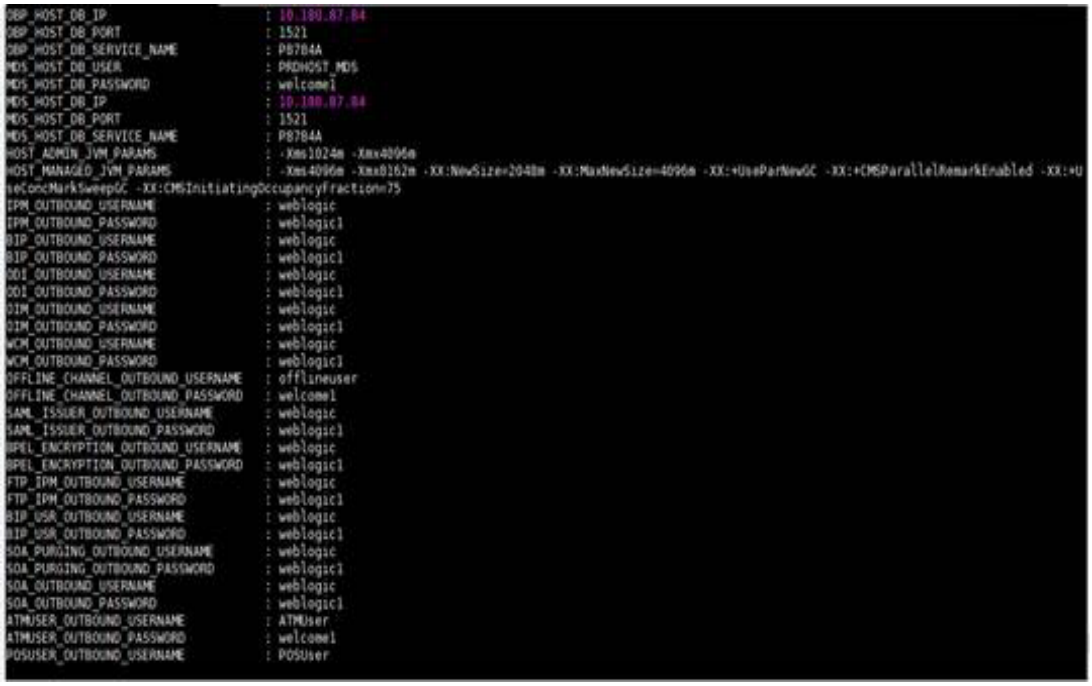
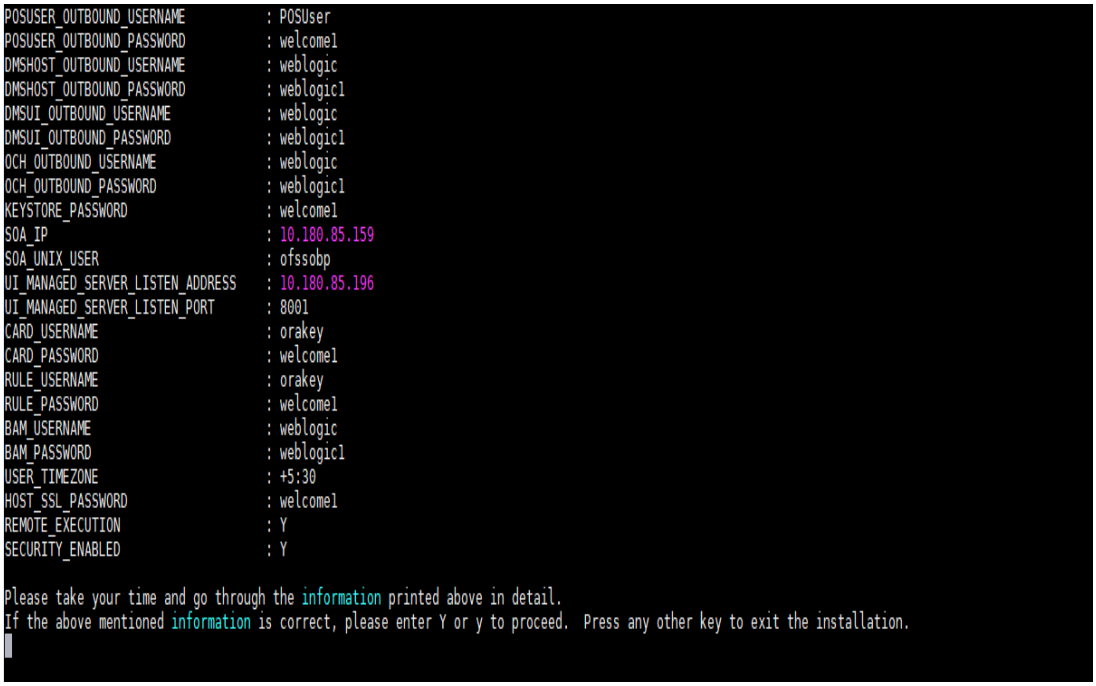


Figure 4–5 Verification of Properties (contd)



3. Verify the value of each property carefully before proceeding.

4. If all values are correct, then enter 'Y' or 'y' and press Enter to initiate the installation. The installation utility performs the installation and domain is created silently.

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

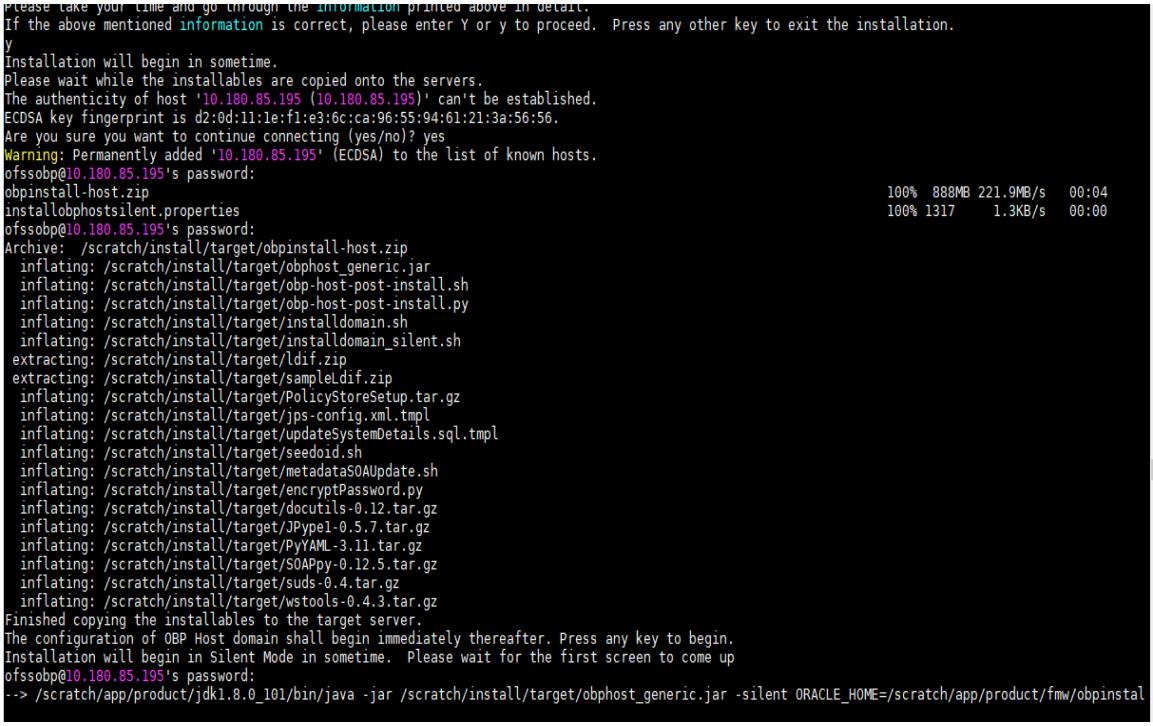


Figure 4–7 Confirmation and Copying of Installables to Target Machine (contd)

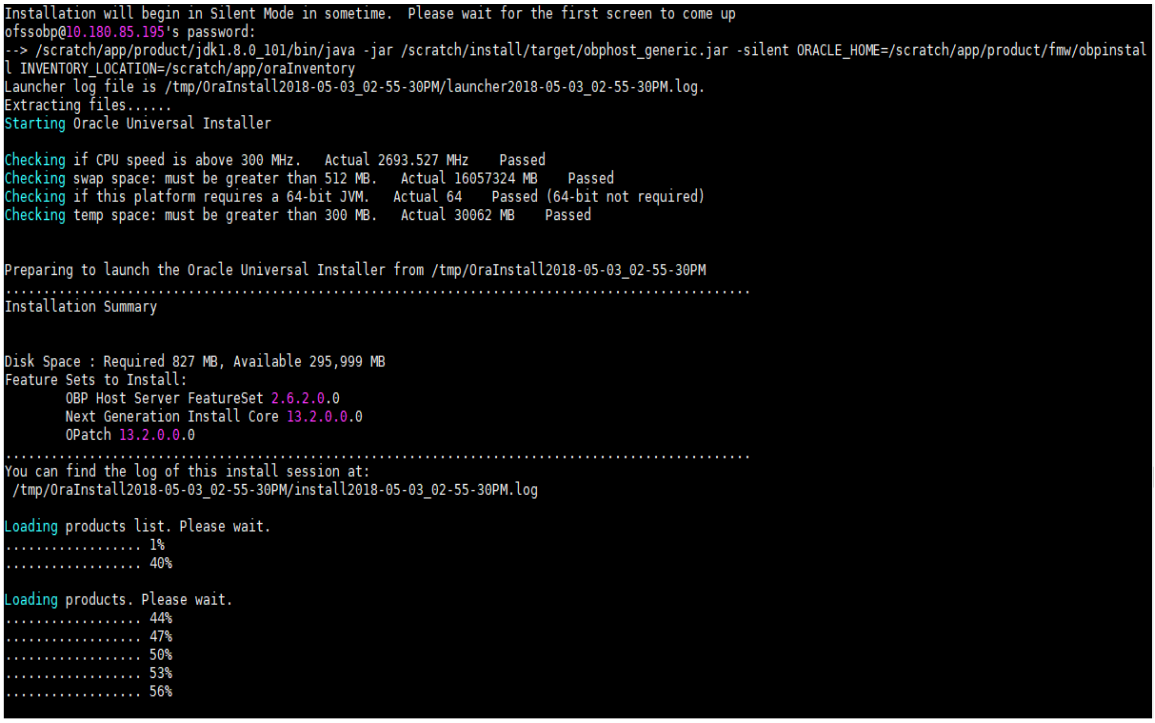
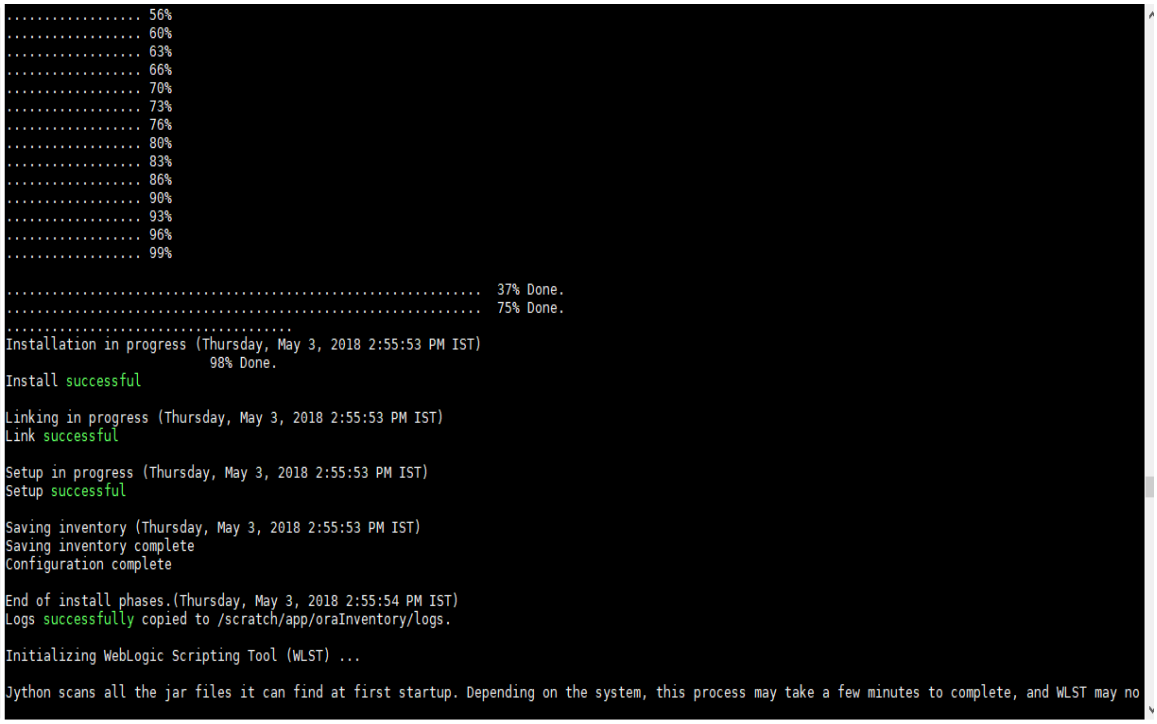
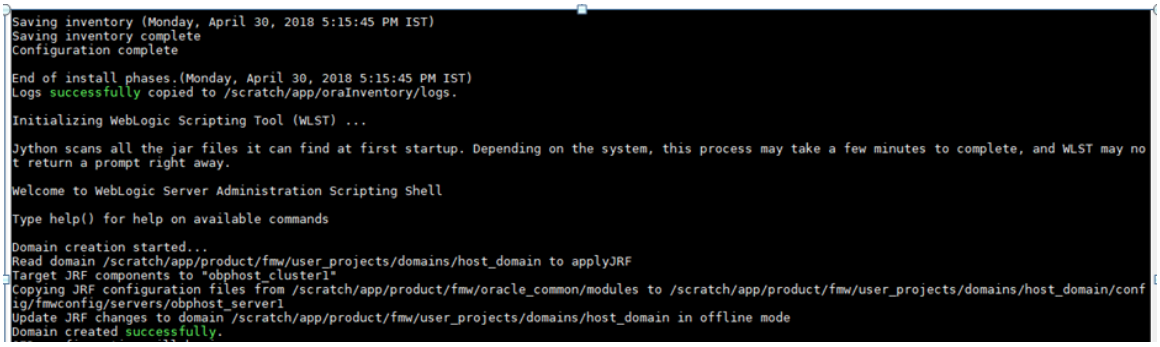


Figure 4–8 Confirmation and Copying of Installables to Target Machine (contd)



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

Figure 4–9 Domain Installation Confirmation



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

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

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

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

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

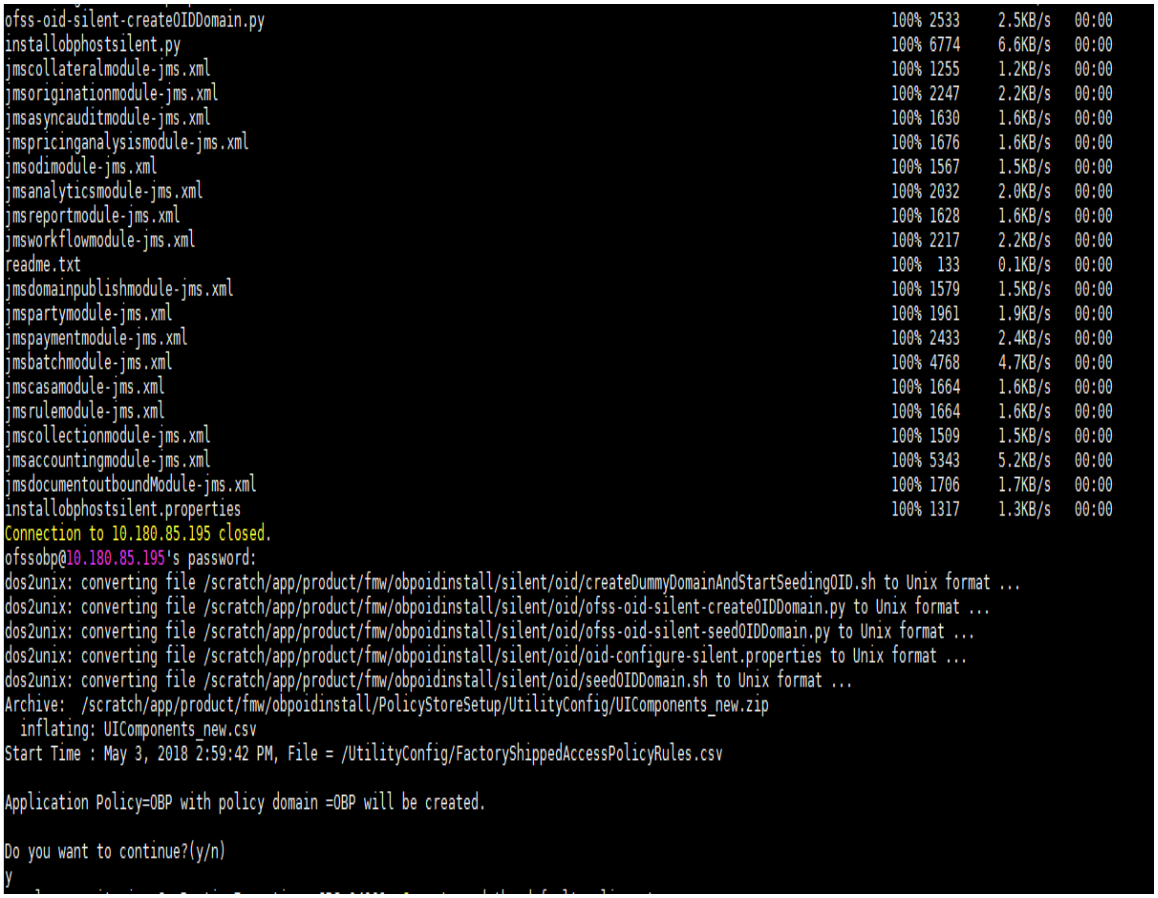


Figure 4–13 Policy Seeding

Figure 4–14 Policy Seeding (contd)

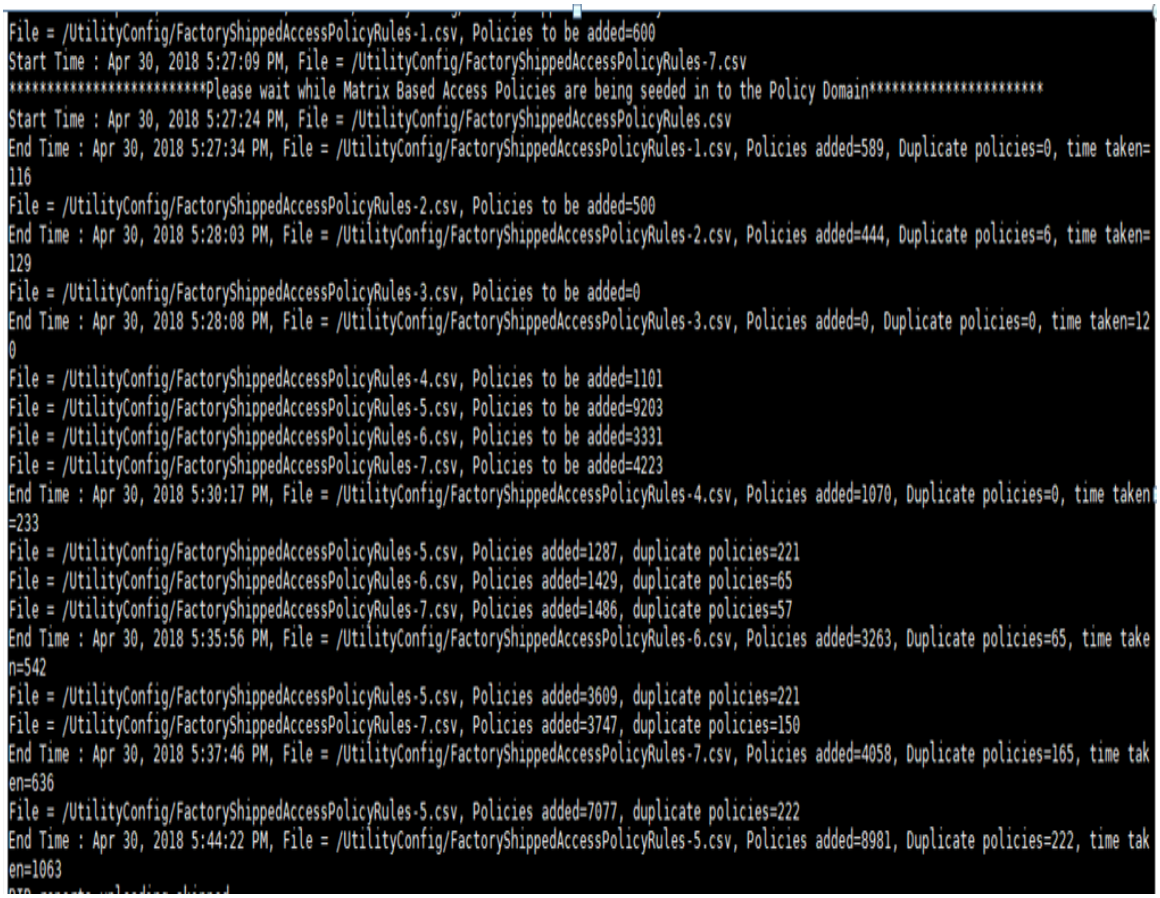


Figure 4–15 BIP Reports Upload

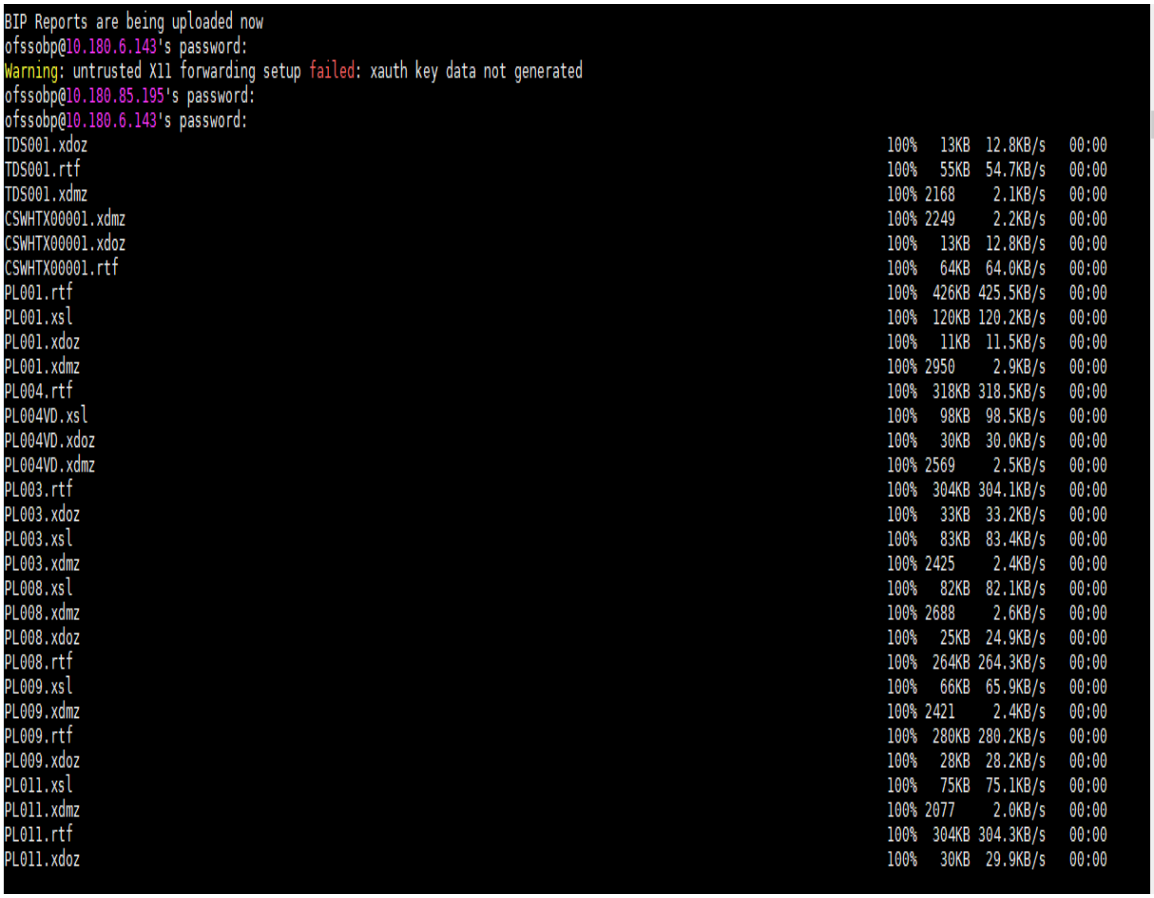
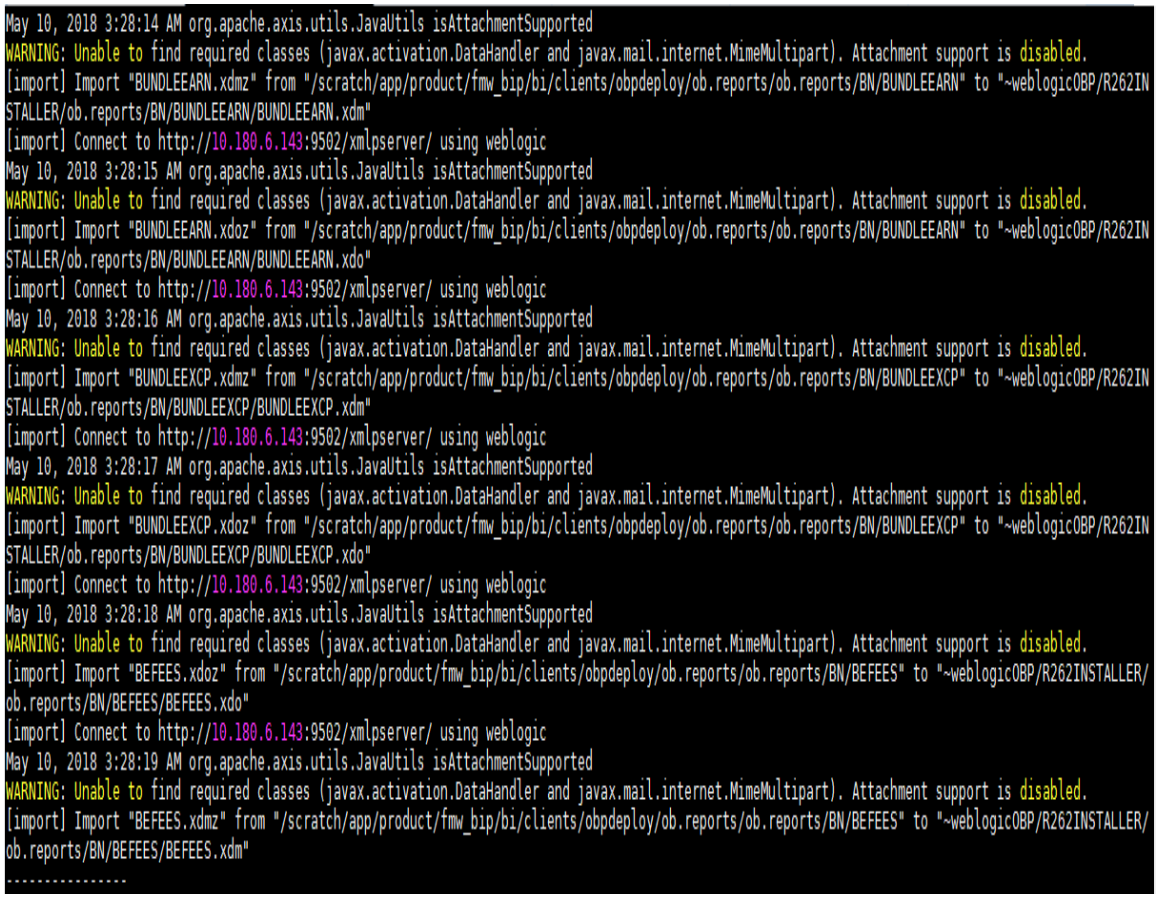


Figure 4–16 BIP Reports Upload (contd)

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

Figure 4–17 BIP Reports Upload (contd)



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

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

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

4.1.4 Front End Processing Interface (FEPI) Installation Steps

Following are the basic steps for FEPI installation procedure:

Step 1 Installation

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

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

Table 4–3 Properties

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

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

Step 2 ATM and POS Trace logs

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

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

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

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

Step 4 Multiple Instances

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

Table 4–4 Examples of files

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

4.2 Post Installation Configuration

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

Checklist for Post Installation Procedure

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

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

  For more information , see Section 7.3.3 HOST DB Schema Seeding and Section 7.3.4 System Configuration DB Update Script Execution.
- The node manager port should be free. You can verify this using the following command, where 5556 is the Node Manager Port.

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

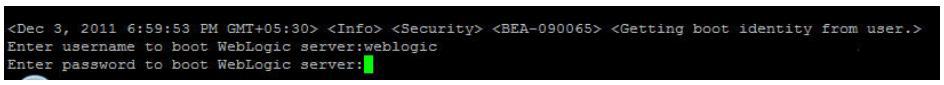
Post Installation Configuration

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

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

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

   Figure 4–18 Host Domain Admin Server Credentials

3. Once the server status changes to RUNNING, proceed to execute the post installation script for Host domain located under middleware. This script performs a multitude of configurations such as:
    - Making changes in OBEO config properties to point to the appropriate integration server (Example: Setting the BIP server URL)
    - Setting the security realm properties of WebLogic domain and reassociating the same to the OID
    - Trust configuration setup using the trust keys copied from the SOA domain

    Note

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

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

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

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

    Note

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

Figure 4–19 Host Domain Post Installation Script Execution

```
[ofssobp@mum00adh fmw]$ ./obp-host-post-install.sh
DOMAIN_NAME                     : host_domain
DOMAIN_DIRECTORY_LOCATION       : /scratch/app/product/fmw/user_projects/domains
WEBLOGIC_USERNAME               : weblogic
WEBLOGIC_PASSWORD               : weblogic1
ADMIN_SERVER_LISTEN_ADDRESS     : 10.180.85.195
ADMIN_SERVER_LISTEN_PORT        : 7001
LDAP_PROVIDER                   : OID
OID_IP                          : 10.180.87.84
OID_PORT                        : 389
OID_ADMIN_USER                  : cn=orcladmin
OID_ADMIN_PWD                   : welcome1
OID_GROUP_DSN                   : cn=Groups,dc=in,dc=oracle,dc=com
OID_USER_DSN                    : cn=Users,dc=in,dc=oracle,dc=com
NODE_MGR_PORT                   : 5556
HOST_IP                         : 10.180.85.195
HOST_TARGET                     : /scratch/install/target
HOST_JAVA_HOME                  : /scratch/app/product/jdk1.8.0_101
HOST_MW_HOME                    : /scratch/app/product/fmw
UI_ADMIN_SERVER_LISTEN_ADDRESS  : 10.180.85.196
UI_ADMIN_SERVER_LISTEN_PORT     : 7001
SOA_HOST_IP                     :
SOA_ORACLE_HOME                 : soa
SOA_UNIX_USER                   : ofssobp
SOA_MW_HOME                     : /scratch/app/product/fmw
SOA_MANAGED_SERVER_LISTEN_ADDRESS  : 10.180.85.159
SOA_MANAGED_SERVER_LISTEN_PORT  : 8001
SOA_WEBLOGIC_USERNAME           : weblogic
SOA_WEBLOGIC_PASSWORD           : weblogic1
UI_IP                           : 10.180.85.196
UI_UNIX_USER                    : ofssobp
UI_DOMAIN_HOME                  : /scratch/app/product/fmw/user_projects/domains/ui_domain
INSTALL_AS                      : ofssobp
BIP_UNIX_USER                   : ofssobp
BIP_HOME                        : /scratch/app/product/fmw_bip/bi
BIP_SERVER_IP                   : 10.180.6.143
BIP_SERVER_PORT                 : 9502
```

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

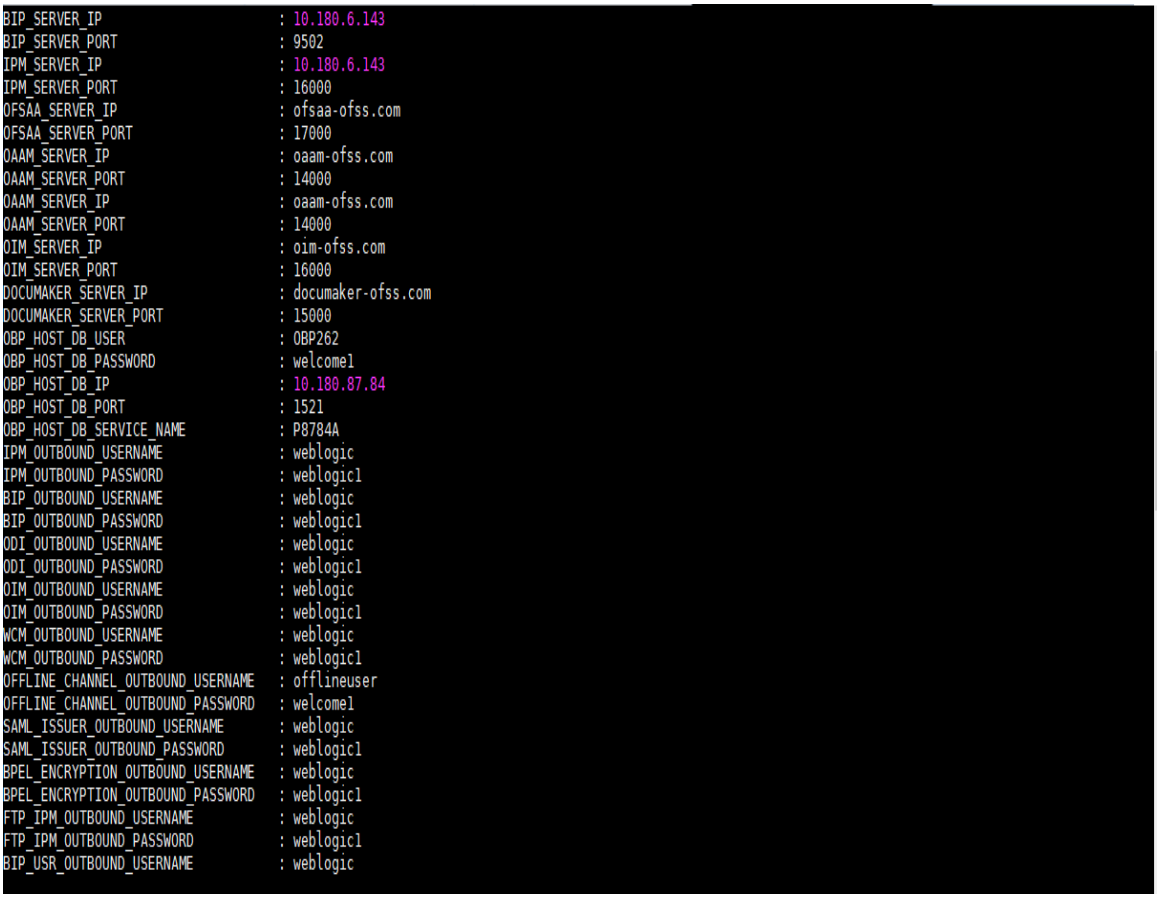


Figure 4–21 Host Domain Post Installation Script Execution (contd)

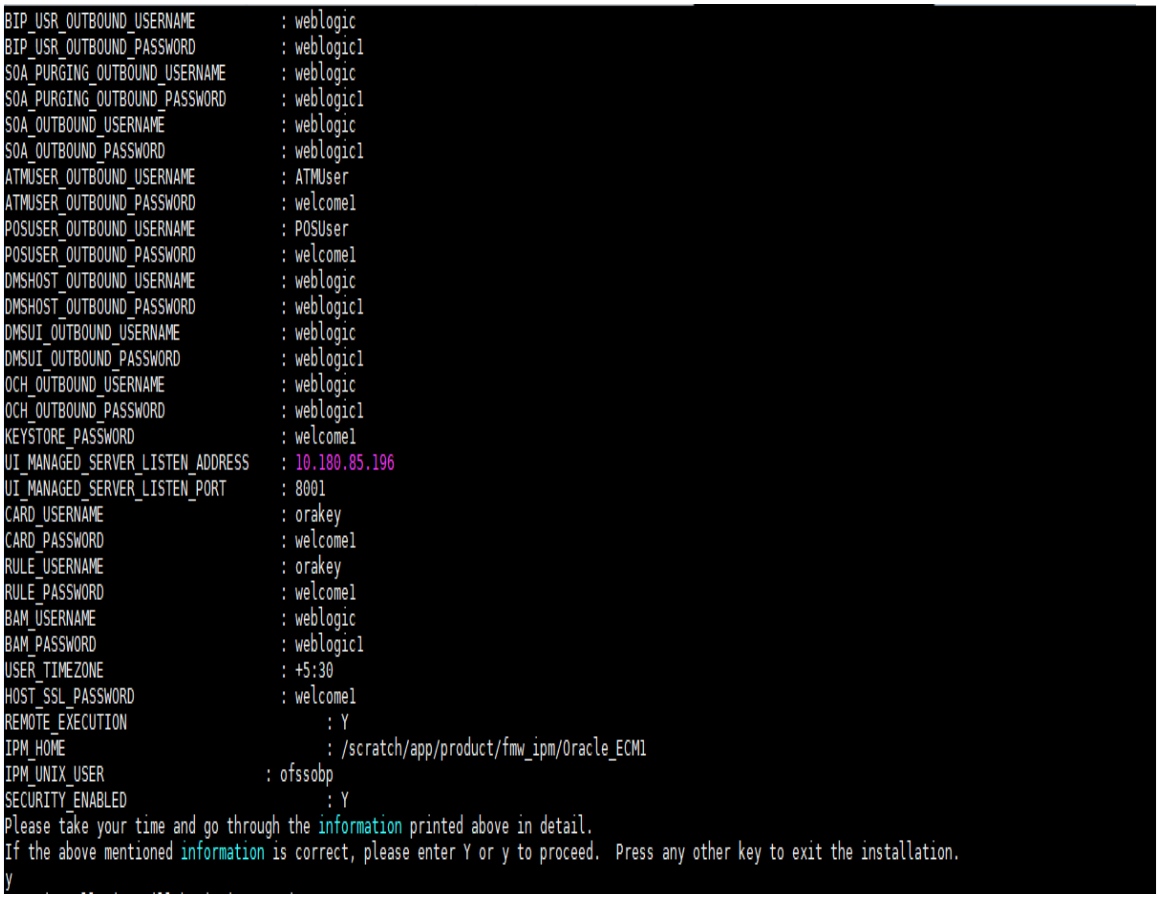


Figure 4–22 Host Domain Post Installation Script Execution (contd)

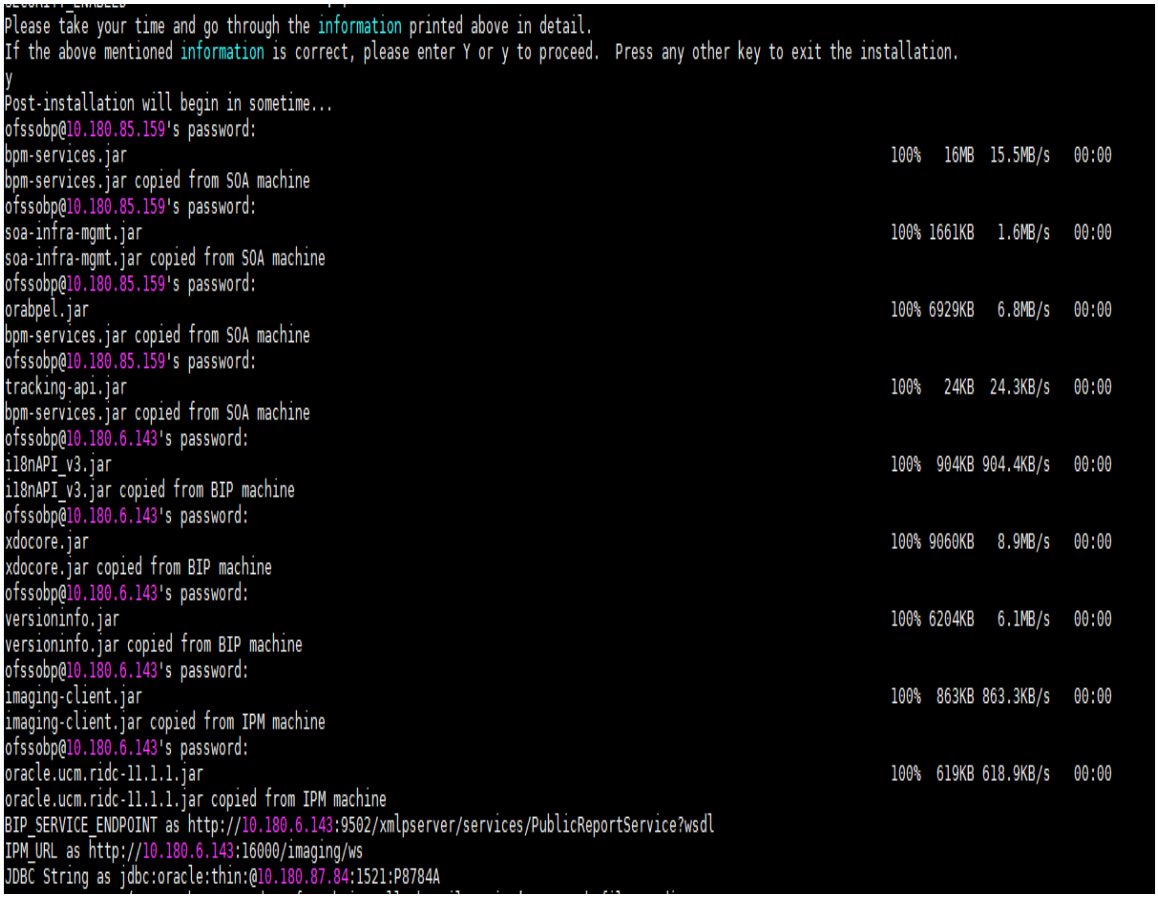
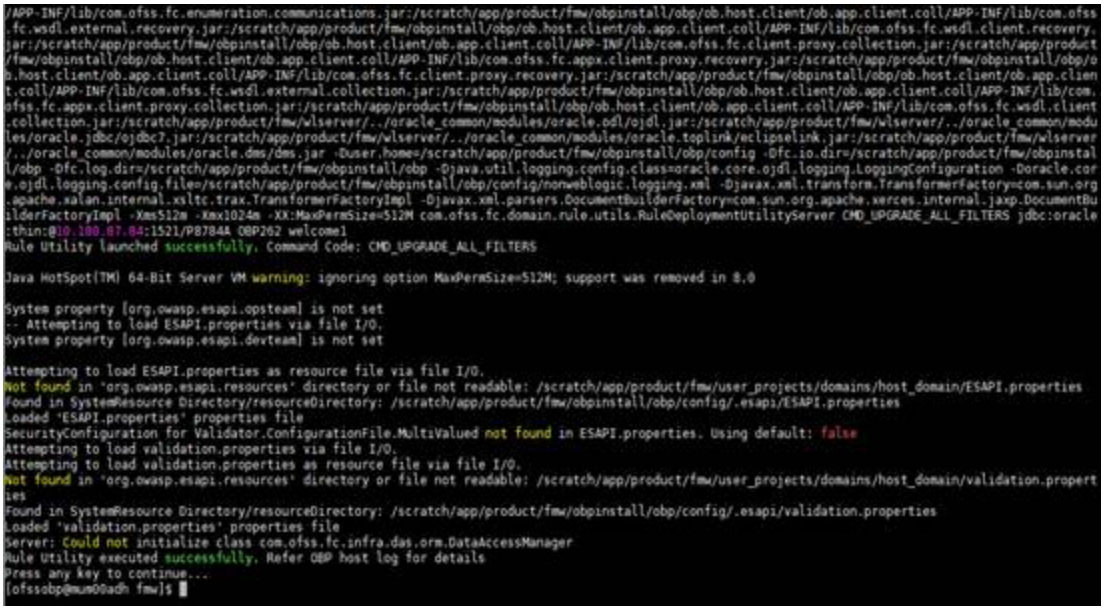


Figure 4–23 Host Domain Post Installation Script Execution Summary



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

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

   within the following xml tag:

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

   add:

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

9. Within the following xml tag:

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

add:

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

10. Then start the admin and managed servers after verifying details as mentioned in Section 4.3 REST (SWAGGER) Deployment Check to check the domain configuration status as described in verification part in Section 12.2 Host Domain Verification.

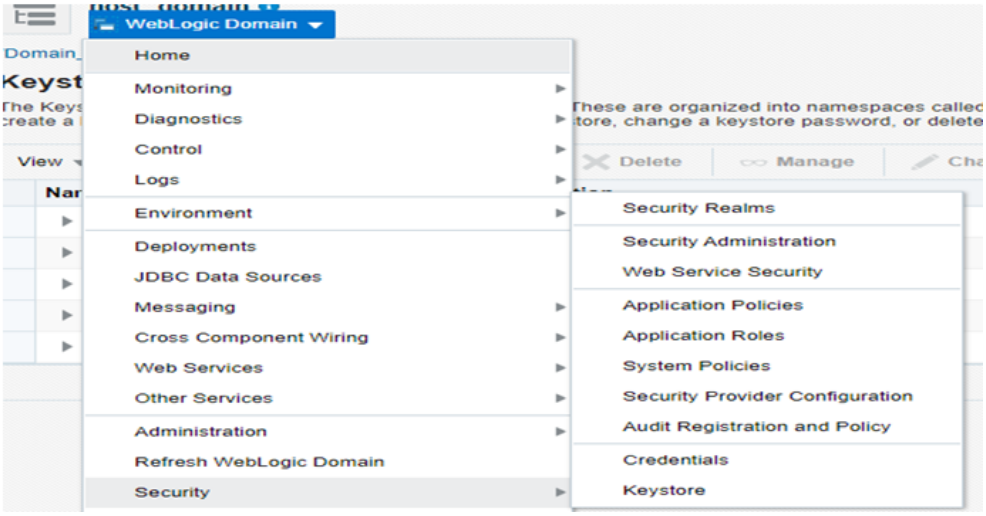
Similar to the above batchhost post installation, perform post installation for other XD components.

4.3 REST (SWAGGER) Deployment Check

This section lists the steps to check REST API deployment. REST API deployment has already been done in Section 4.2 Post Installation Configuration. Verify the following points that are part of batchhost installation:

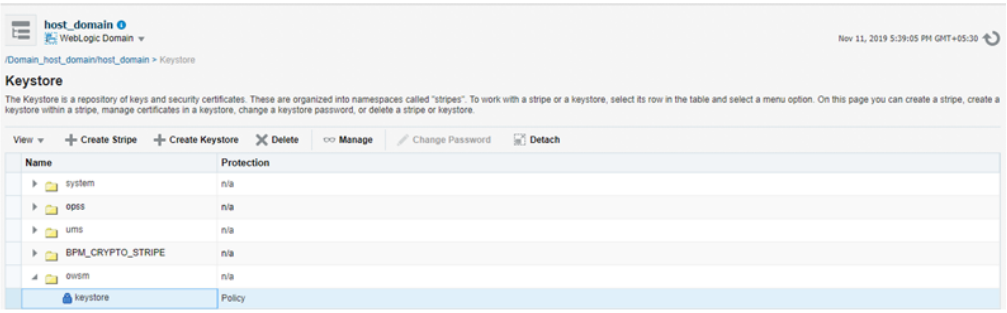
1. OWSM keystore creation on HOST EM: It is a part of host post installation. Verify if OWSM is present on HOST EM console. If not, then create it.
    a. Log in to HOST EM and click weblogin domain > security > keystore.

Figure 4–24 Navigate to Keystore



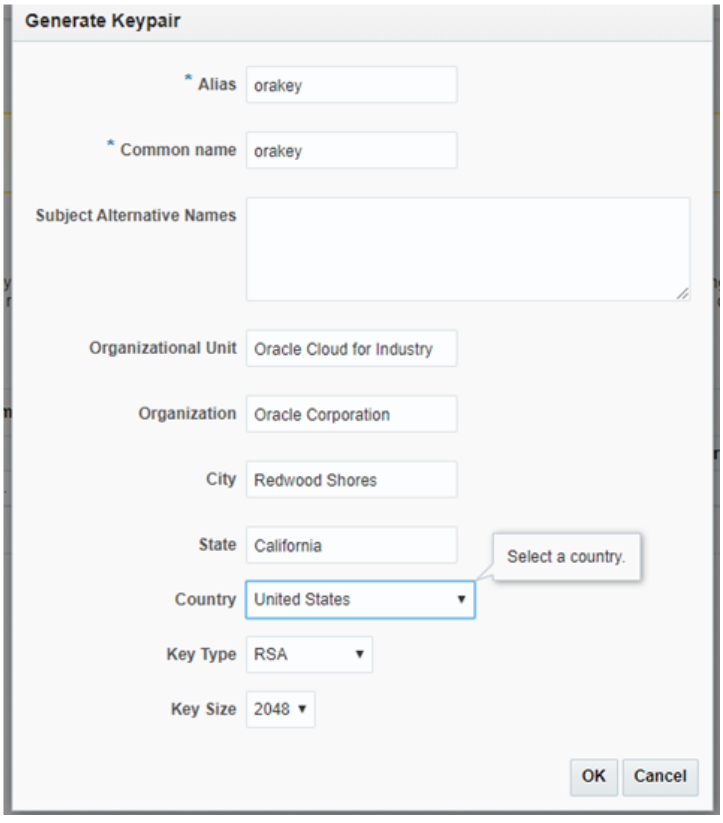
    b. Create Stripe 'OWSM'.
    c. Create KeyStore 'keystore' under OWSM.

Figure 4–25 Create Keystore



d. Click Manage and generate Keypair using the following values:
Alias: orakey
Common name: orakey
Organizational Unit: Oracle Cloud for Industry
Organization: Oracle Corporation
City: Redwood Shores
State: California
Country: United States

Figure 4–26 Generate Keypair



2. jax-rs library deployment on host console.

3. Host IP with port will be present in json/yaml files under $MW_HOME/obpinstall/obp/OBPAPI/yaml.
4. OBPAPI folder present under $MW_HOME/obpinstall/obp and it gets deployed as a war on host.

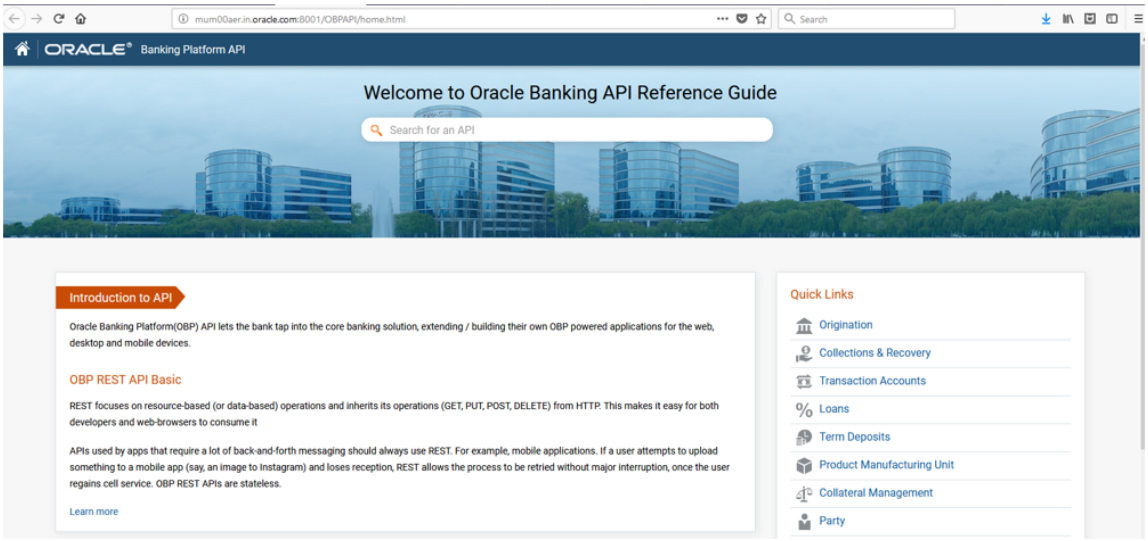
Figure 4–27 OBPAPI deploy on obphost_cluster1

ob.app.host.tp.cz(2.7.0.0.0,2.7.0.0.0)	Active		Library	obphost_server1	Global		100
OBPAPI	Active	OK	Web Application	obphost_cluster1	Global		100
odl.clickhistory(1.0,12.2.1)	Active		Library	AdminServer, obphost_cluster1	Global		100
odl.clickhistory.webapp(1.0,12.2.1)	Active		Library	AdminServer, obphost_cluster1	Global		100

5. After completion of the above steps, restart the HOST managed server to reflect the changes.

   http://$HOSTIP:$HOSTPORT/OBPAPI/home.html

Figure 4–28 REST API



Note:

- RestServices ear should be deployed on different weblogic domain for consumption by external clients.
- Current deployment will cater to OJET UI.

5 OBEO Localization Presentation Media Pack Installation

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

5.1 Installation and Configuration Procedure

This section details the installation procedure for the Oracle Banking Enterprise Originations Localization Presentation Media Pack.

5.1.1 Preparatory Steps

This section lists the preparatory steps required for the Oracle Banking Enterprise Originations 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' or 'obpau-ui-soa.zip' to a local Linux VM or Linux machine from where the installation will be carried out. Extract the zip file. Three files will be extracted:

- A zip file 'obpinstall-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 2.4 Installation Checklist of this guide and note the values applicable for each point in the last column for 'Value' so that the same is handy during the actual installation.

5.1.2 Pre-Installation Steps

This section lists the pre-installation steps required for the Oracle Banking Enterprise Originations 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:

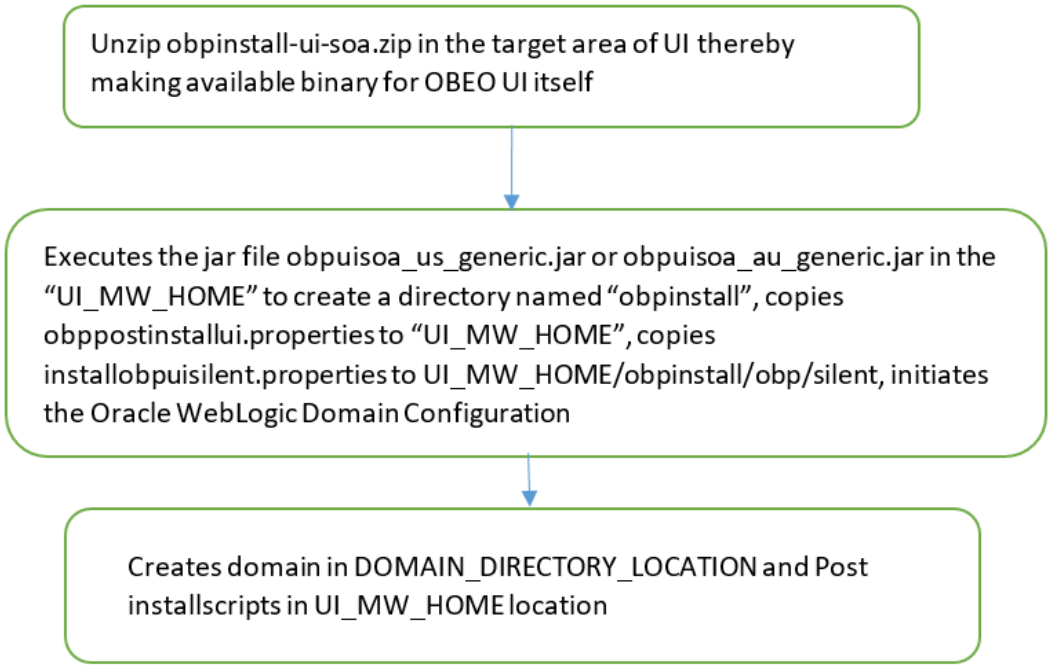
- Make sure required RCU schemas have been created. For more information, see Section 7.1 Pre-Installation Steps and Section 7.2 OBEO Database Setup – RCU Installation.
- Node manager must not be running on the target machine.
- Create a dummy folder named as Target and mention its path against UI_TARGET property.
- In case of a re-installation ensure that the directory paths against DOMAIN_DIRECTORY_ LOCATION, HOST_TARGET and HOST_MW_HOME specified in installobpui.properties are cleaned up for traces of any previous installations, as the remote shell copy may not be overwriting in case of any residual file left by the previous run.
- No processes should be running on the port in HOST machine given in installobpui.properties.
- MDS_SCHEMA_USER schema given in the installobpui.properties exists. This should point to the same schema as MDS_HOST_DB_USER of installobphost.properties.
- Values given in installobpui.properties must be correct. At run time, no option will be given to change the values.

5.1.3 Installation Steps

This section lists the installation steps required for the Oracle Banking Enterprise Originations 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

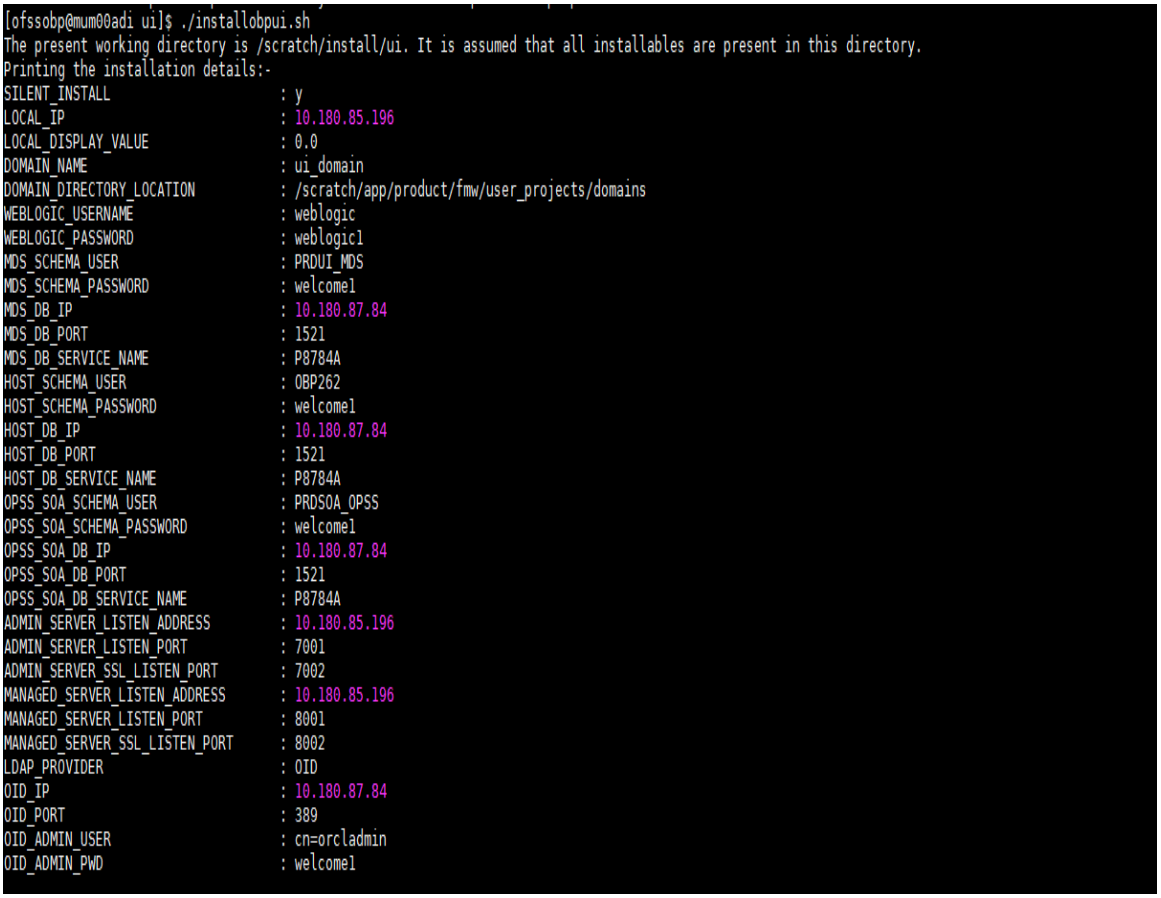


Figure 5–3 Confirmation to Proceed Domain Installation (contd)

```
OID_ADMIN_PWD                    : welcome1
OID_GROUP_DSN                    : cn=Groups,dc=in,dc=oracle,dc=com
OID_USER_DSN                     : cn=Users,dc=in,dc=oracle,dc=com
NODE_MGR_PORT                    : 5556
UI_IP                            : 10.180.85.196
UI_CLUSTER_NAME                  : obpui_cluster1
UI_SERVER_NAME                   : obpui_server1
UI_TARGET                        : /scratch/install/target
UI_MW_HOME                       : /scratch/app/product/fmw
UI_JAVA_HOME                     : /scratch/app/product/jdk1.8.0_101
OUI_JAVA_HOME                    : /scratch/app/product/jdk1.8.0_101
CENTRAL_INVENTORY_LOC            : /scratch/app/oraInventory
INSTALL_AS                       : ofssobp
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
OIM_SERVER_IP                    : oim-ofss.com
OIM_SERVER_PORT                  : 16000
UI_ADMIN_JVM_PARAMS              : -Xms2048m -Xmx4096m
UI_MANAGED_JVM_PARAMS            : -Djbo.ampool.doampooling=false -Xms4096m -Xmx6084m -XX:NewSize=512m -XX:MaxNewSize=2048m -XX:+UseParNewGC -XX:+C
MSParallelRemarkEnabled -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -Djbo.load.components.lazily=true
HOST_ADMIN_SERVER_LISTEN_ADDRESS : 10.180.85.195
HOST_ADMIN_SERVER_LISTEN_PORT    : 7001
HOST_MANAGED_SERVER_LISTEN_ADDRESS : 10.180.85.195
HOST_MANAGED_SERVER_LISTEN_PORT  : 8001
SOA_MANAGED_SERVER_LISTEN_ADDRESS : 10.180.85.159
SOA_MANAGED_SERVER_LISTEN_PORT   : 8001
SOA_ADMIN_SERVER_LISTEN_ADDRESS  : 10.180.85.159
SOA_ADMIN_SERVER_LISTEN_PORT     : 7001
KEYSTORE_PASSWORD                : welcome1
UI_SSL_PASSWORD                  : welcome1
UCM_READ_FROM_URL                : true
UCM_IP                           : ofss.ucm.com
UCM_PORT                         : 4444
OFFLINE_CHANNEL_OUTBOUND_USERNAME : offlineuser
```

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

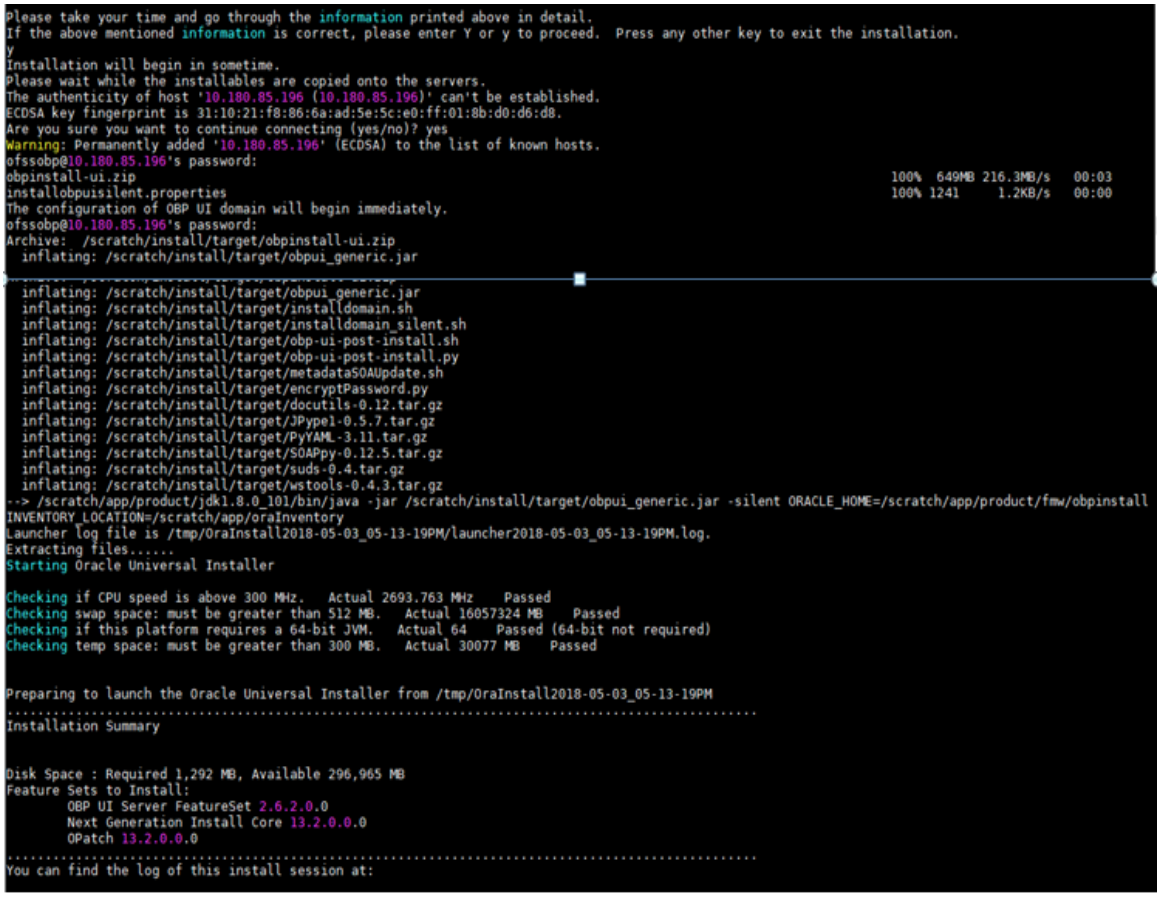


Figure 5–6 Copying and Extraction of obpinstall-ui-soa.zip (contd)

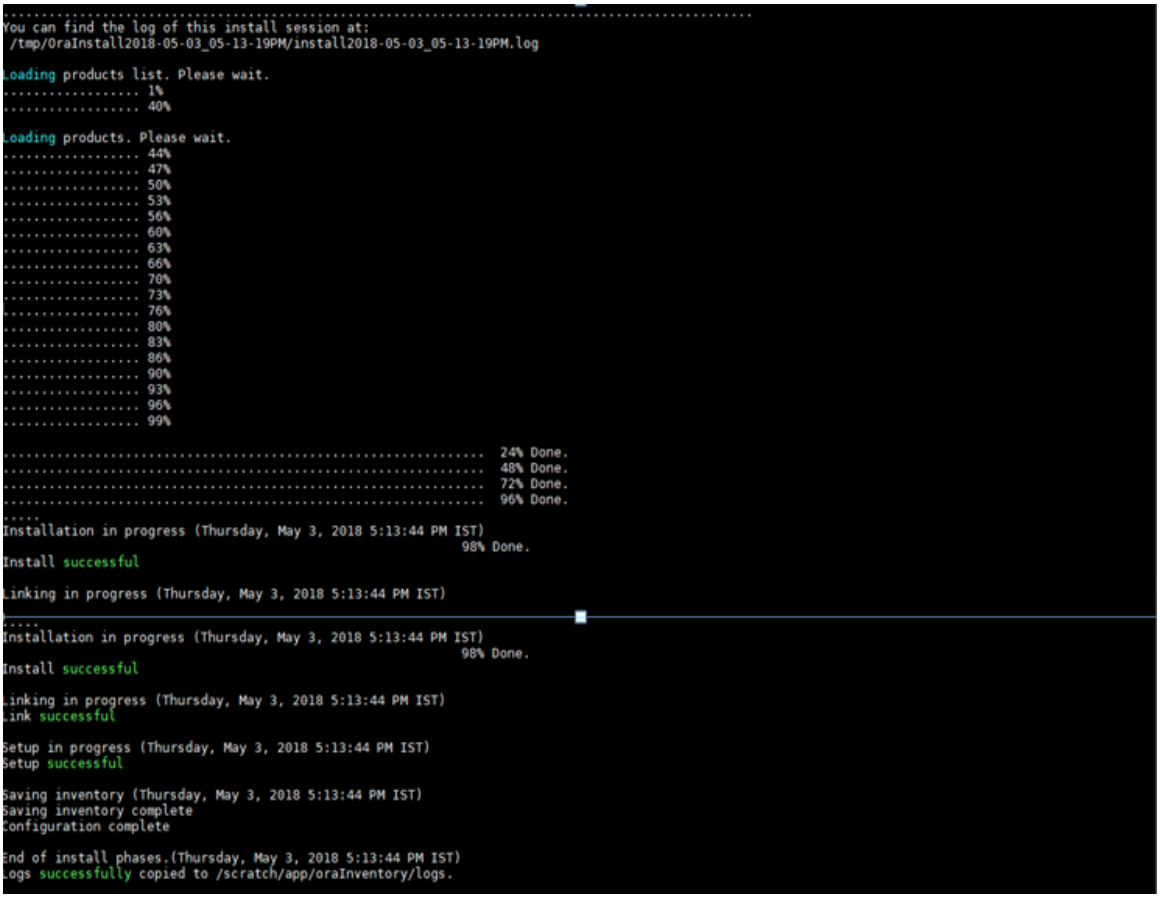
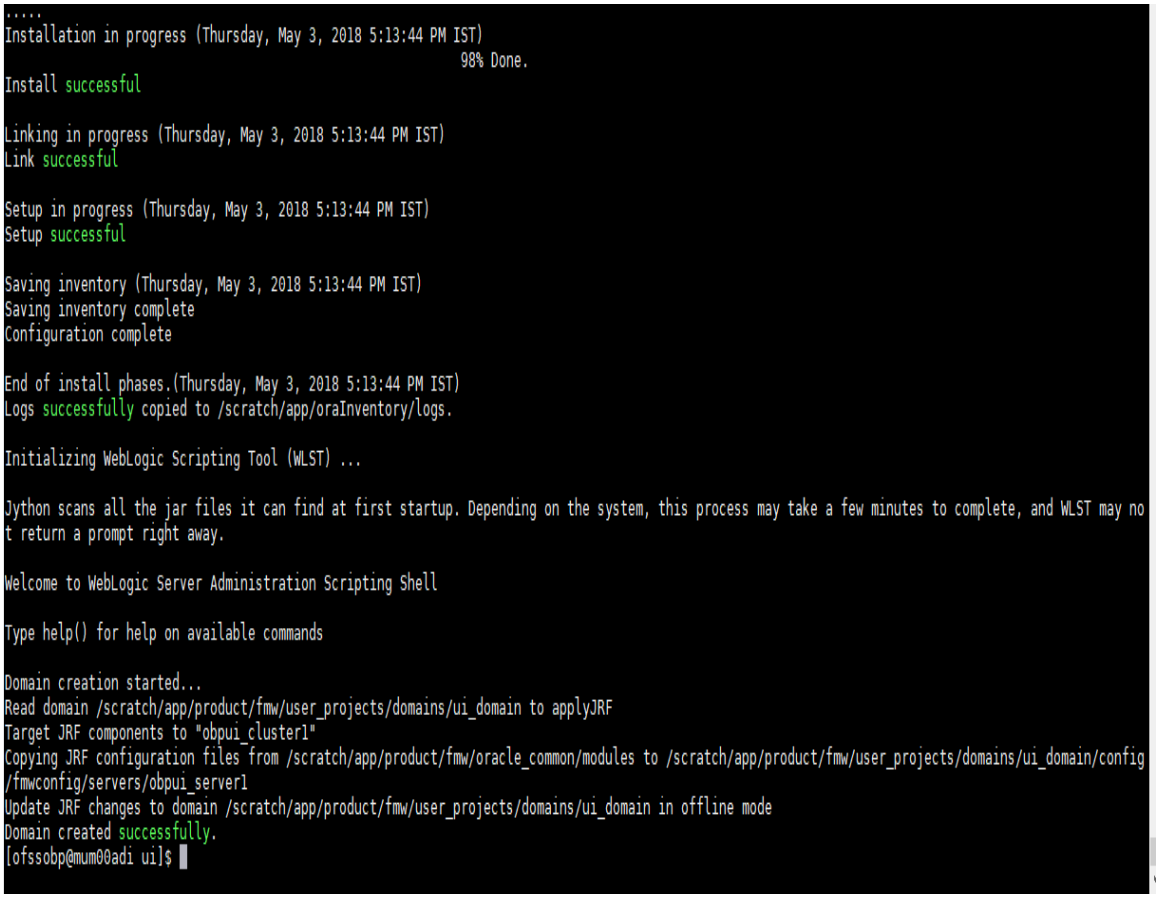


Figure 5–7 Domain Creation Confirmation



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 Oracle Banking Enterprise Originations 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

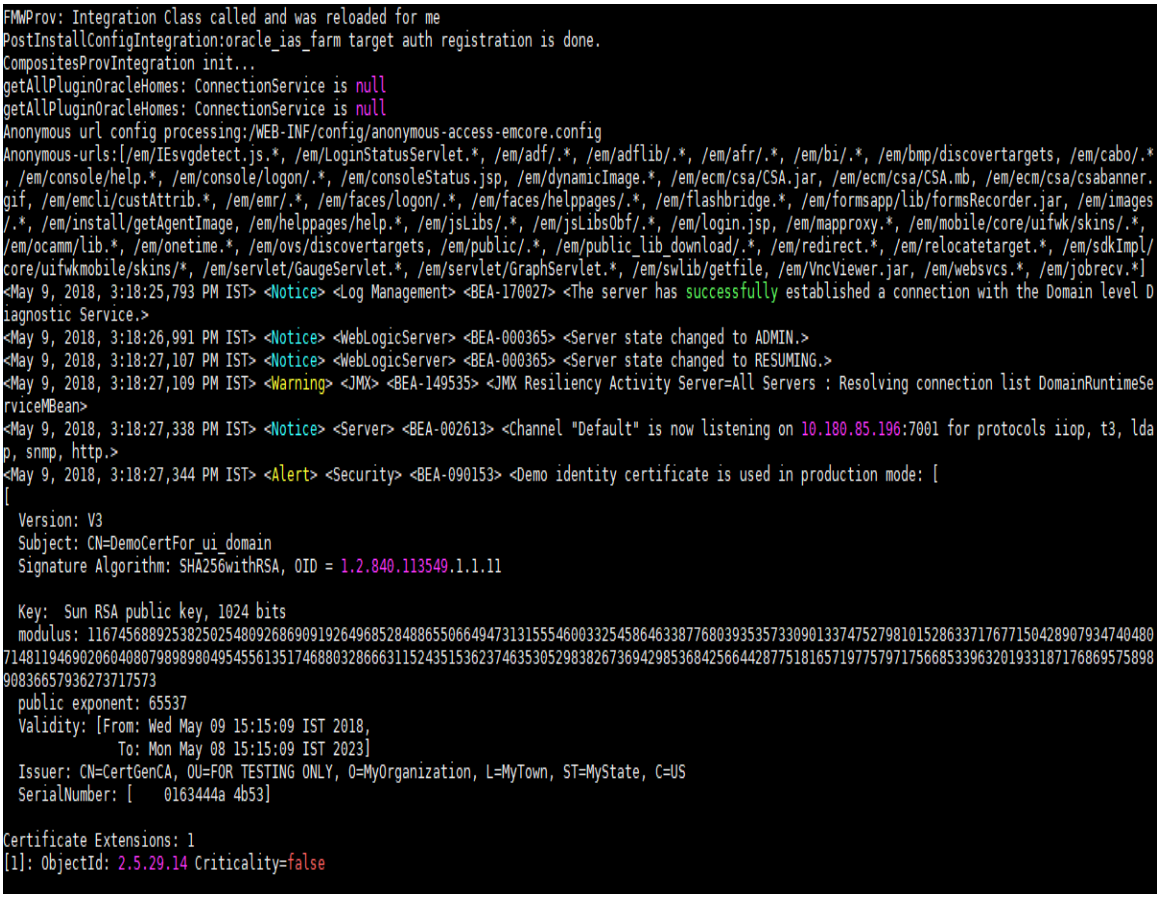


Figure 5–10 UI Admin Server Running (contd)

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

```
[ofssobp@mum00adi fmw]$ ./obp-ui-post-install.sh
DOMAIN_NAME                         : ui_domain
DOMAIN_DIRECTORY_LOCATION           : /scratch/app/product/fmw/user_projects/domains
ADMIN_SERVER_LISTEN_ADDRESS         : 10.180.85.196
ADMIN_SERVER_LISTEN_PORT            : 7001
MANAGED_SERVER_LISTEN_ADDRESS       : 10.180.85.196
MANAGED_SERVER_SSL_LISTEN_PORT      : 8002
MANAGED_SERVER_LISTEN_PORT          : 8001
WEBLOGIC_USERNAME                   : weblogic
WEBLOGIC_PASSWORD                   : weblogic1
UI_IP                               : 10.180.85.196
UI_TARGET                           : /scratch/install/target
UI_MW_HOME                          : /scratch/app/product/fmw
KEYSTORE_PASSWORD                   : welcome1
UI_SSL_PASSWORD                     : welcome1
INSTALL_AS                          : ofssobp
HOST_ADMIN_SERVER_LISTEN_ADDRESS    : 10.180.85.195
HOST_ADMIN_SERVER_LISTEN_PORT       : 7001
HOST_MANAGED_SERVER_LISTEN_ADDRESS  : 10.180.85.195
HOST_MANAGED_SERVER_LISTEN_PORT     : 8001
SOA_MANAGED_SERVER_LISTEN_ADDRESS   : 10.180.85.159
SOA_MANAGED_SERVER_LISTEN_PORT      : 8001
LDAP_PROVIDER                       : OID
OID_IP                              : 10.180.87.84
OID_PORT                            : 389
OID_ADMIN_USER                      : cn=orcladmin
OID_ADMIN_PWD                       : welcome1
OID_GROUP_DSN                       : cn=Groups,dc=in,dc=oracle,dc=com
OID_USER_DSN                        : cn=Users,dc=in,dc=oracle,dc=com
NODE_MGR_PORT                       : 5556
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
OIM_SERVER_IP                       : oim-ofss.com
OIM_SERVER_PORT                     : 16000
```

Figure 5–12 Starting Post Installation (contd)

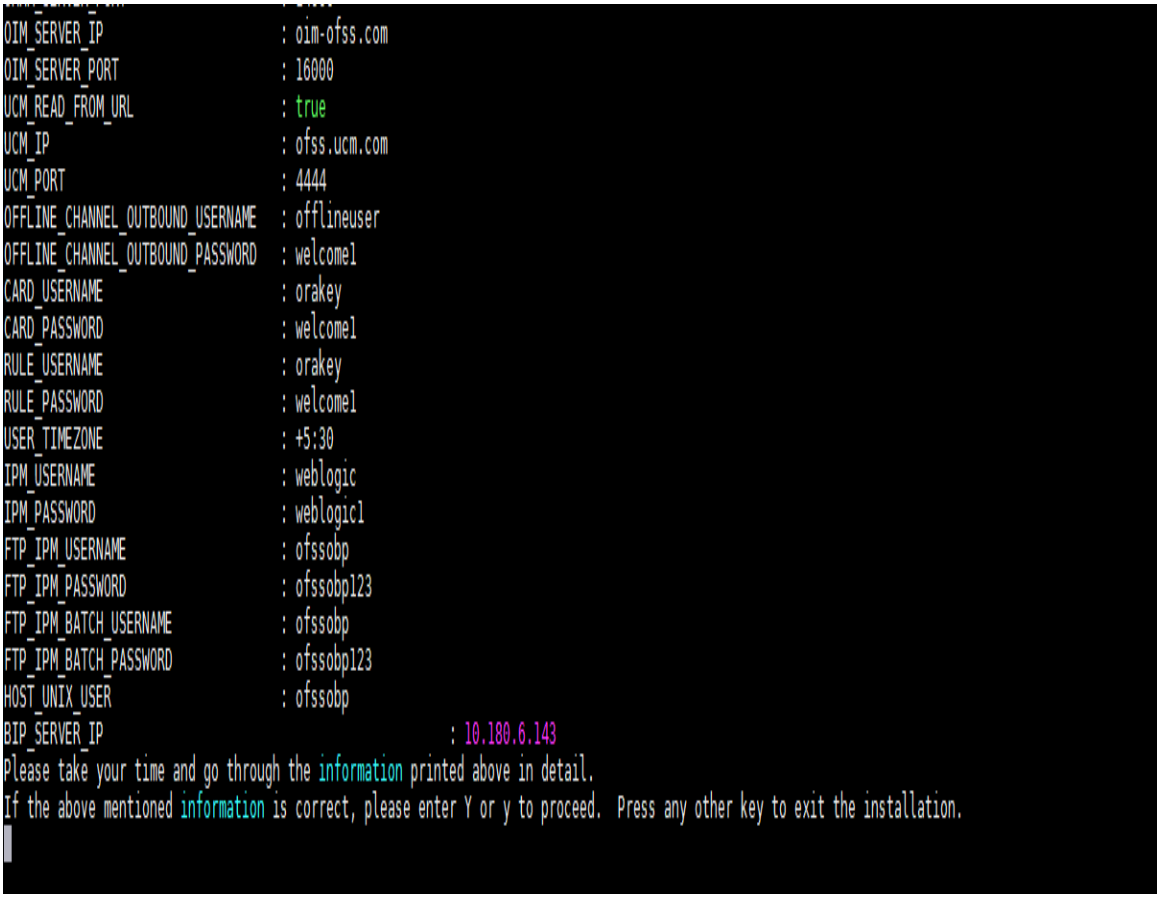


Figure 5–13 Continuation of Post-Installation

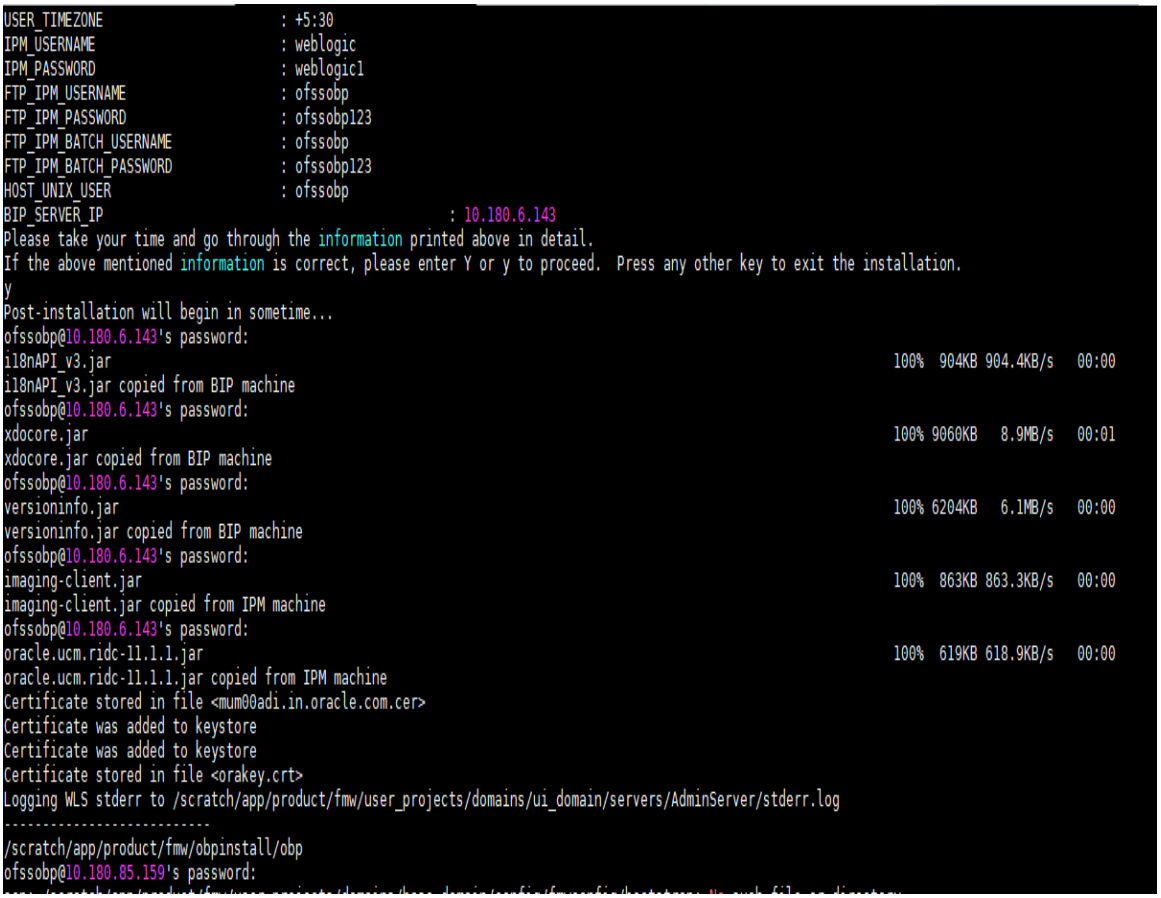
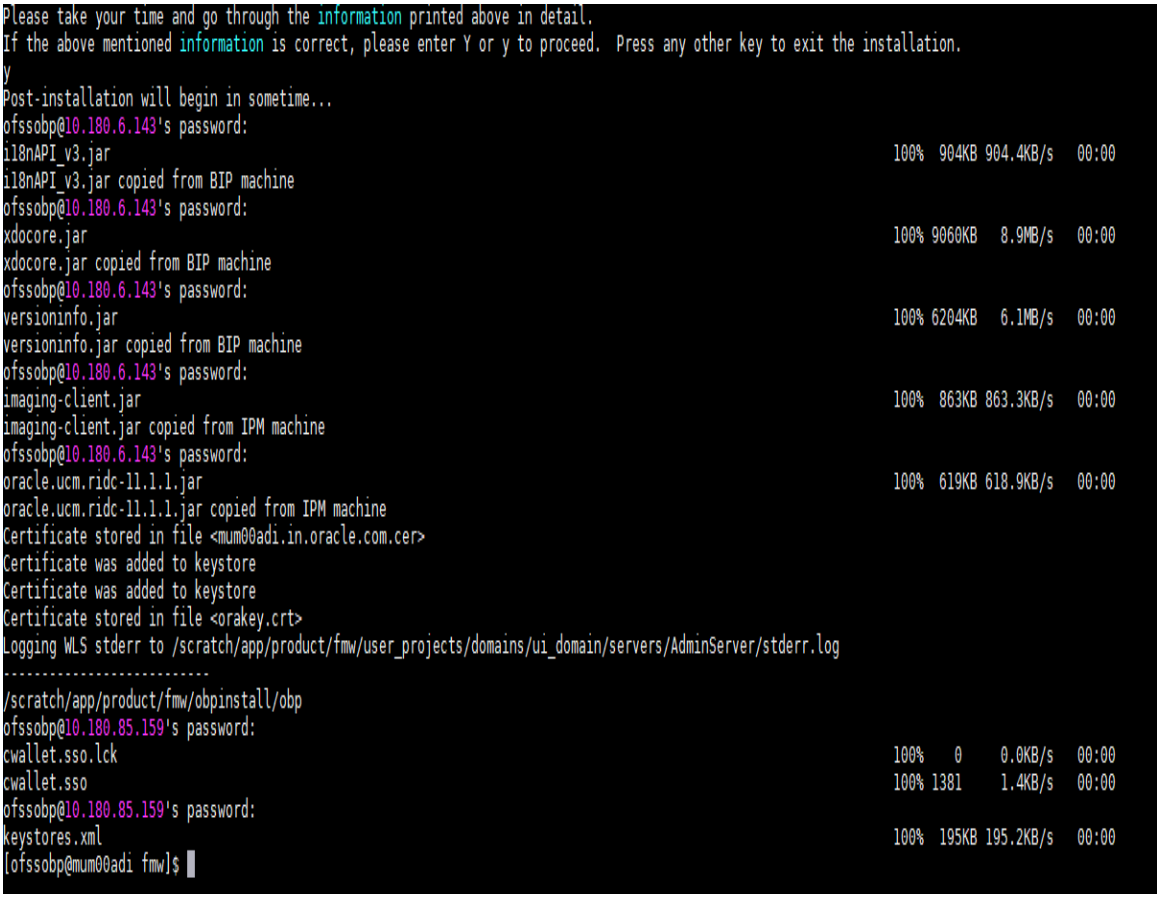


Figure 5–14 Continuation of Post-Installation (contd)



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 BAM Installation using OBEO Localization SOA Media Pack

This chapter details every step involved in the installation of Oracle Business Activity Monitoring (BAM) using OBEO Localization SOA Media pack. The subsequent section refers to the variable names specified in Section 2.4 Installation Checklist.

It is mandatory not to carry out BAM installation in the same machine where SOA installation was done.

6.1 Installation and Configuration Procedure

This section details the installation procedure for BAM using OBEO Localization SOA Media Pack.

6.1.1 Preparatory Steps

This section lists the preparatory steps required for BAM using OBEO Localization SOA Media Pack.

Step 1 Procuring Installables

Download the appropriate SOA media pack from the following location:

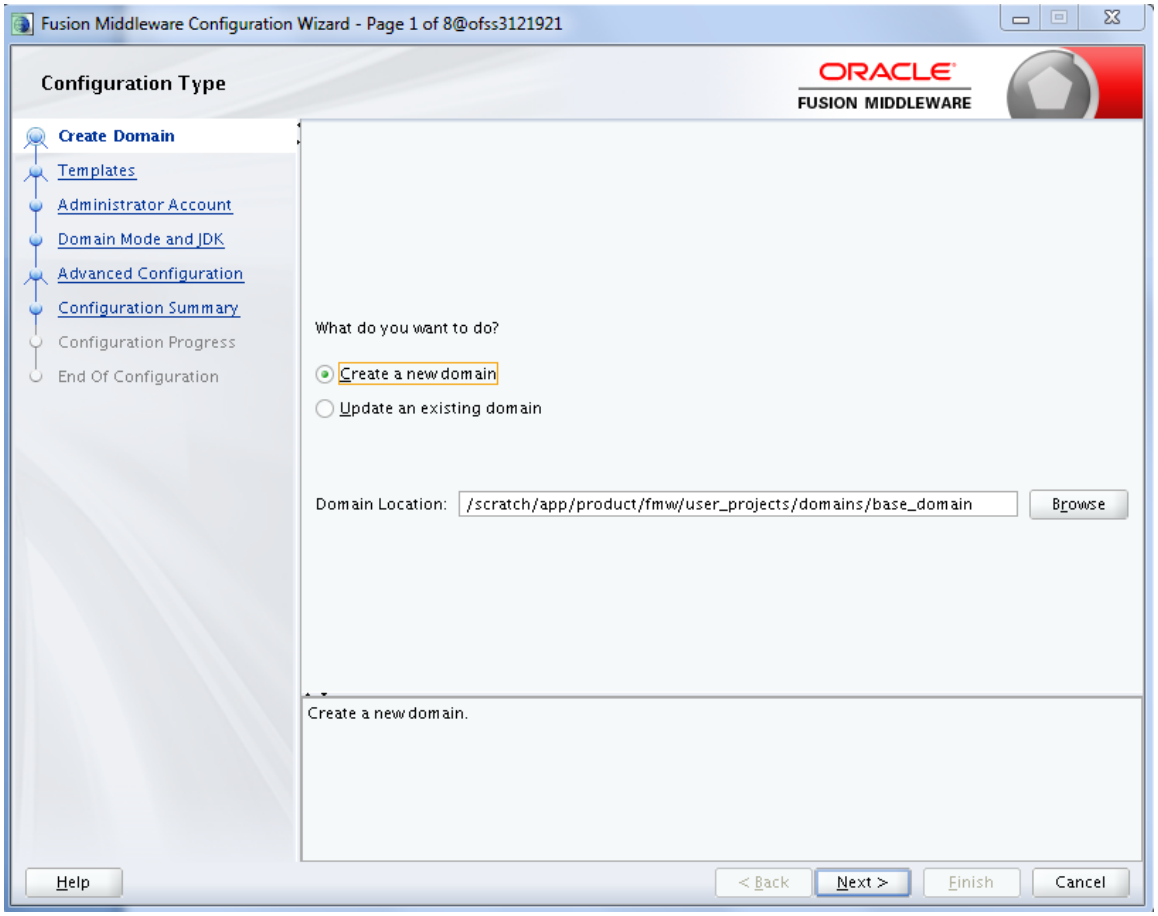
http://edelivery.oracle.com/

6.1.2 BAM Domain Creation Steps

This section lists the steps for creating BAM domain. Make sure BAM RCU schemas and SOA suite are installed before domain creation.

1. Go to <MIDDLEWARE_HOME>/oracle_common/common/bin directory.
2. Execute config.sh. A configuration wizard window appears.
3. In the **Configuration Type** page, select the **Create a new domain** option.

Figure 6–1 Configuration Type page



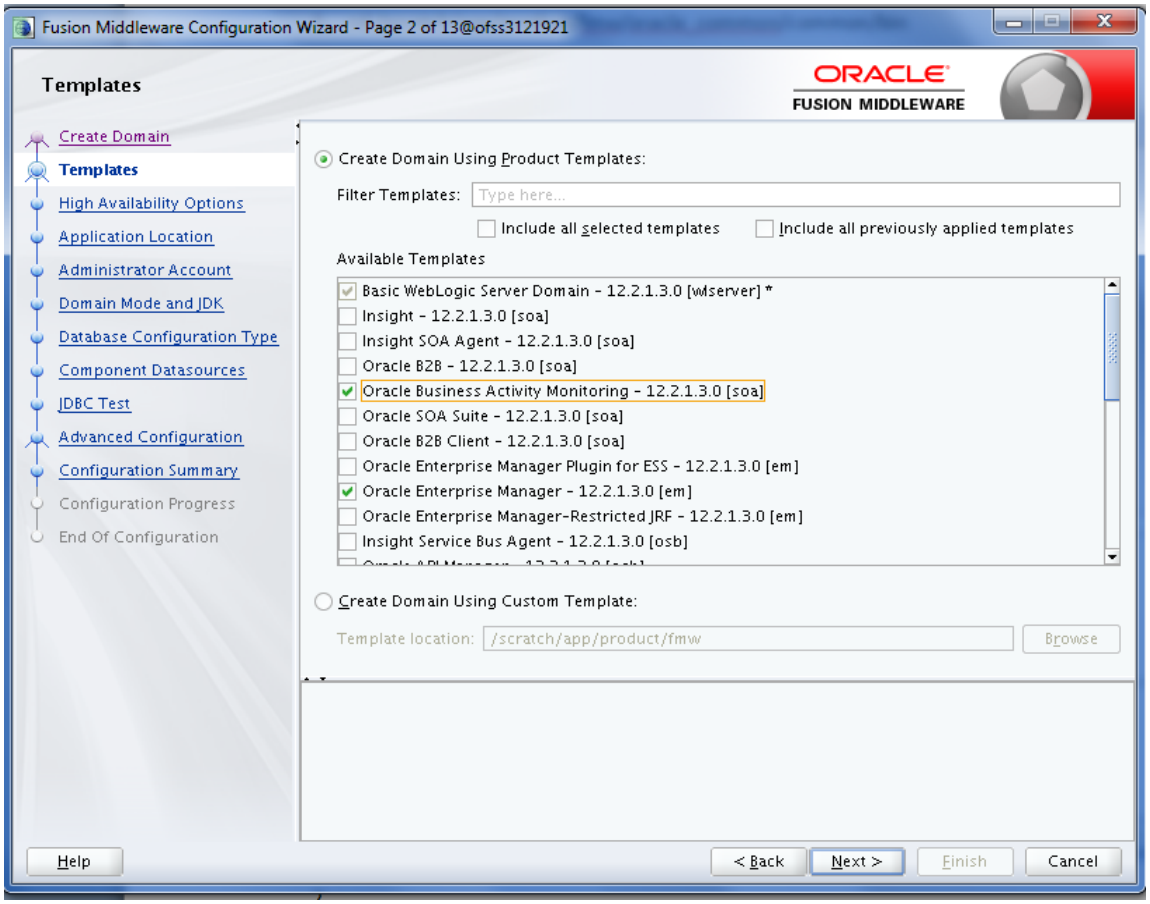
4. Provide the following domain path and click **Next.**

   cd /scratch/app/product/fmw/oracle_common/common/bin

   ./config.sh

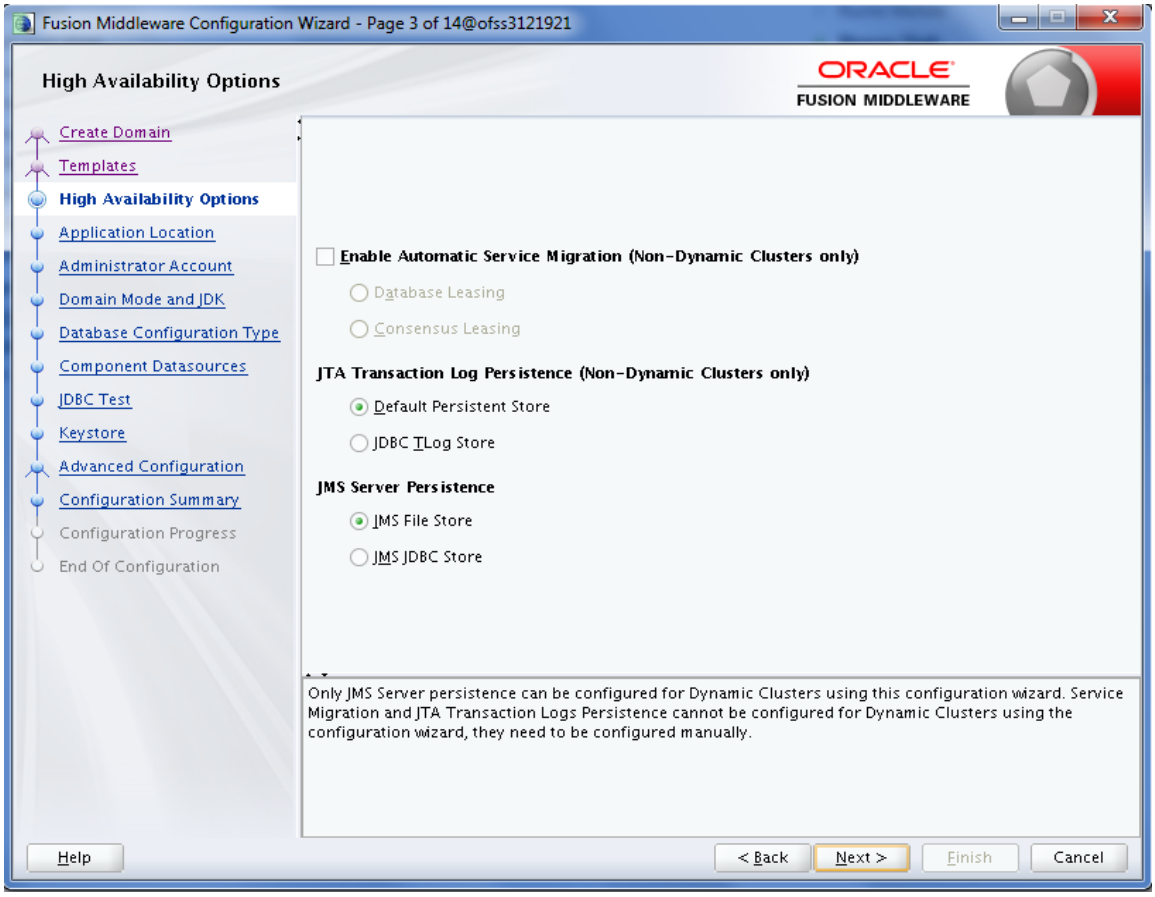
5. In the **Templates** page, select the **Oracle Business Activity Monitoring** check box, in the **Available Templates** section and click **Next**.

Figure 6–2 Templates page



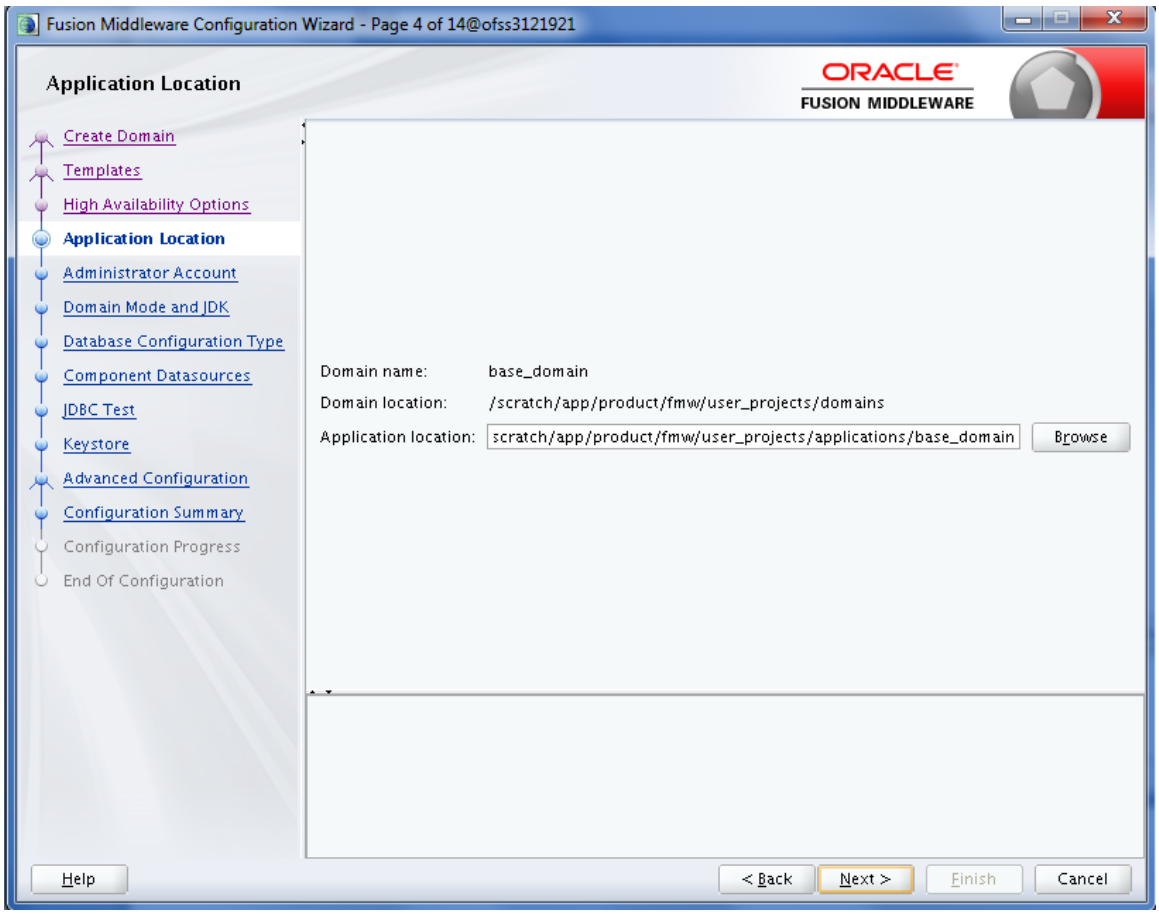
6. In the **High Availability Options** page, select the required options and then click **Next.**

Figure 6–3 High Availability Options page



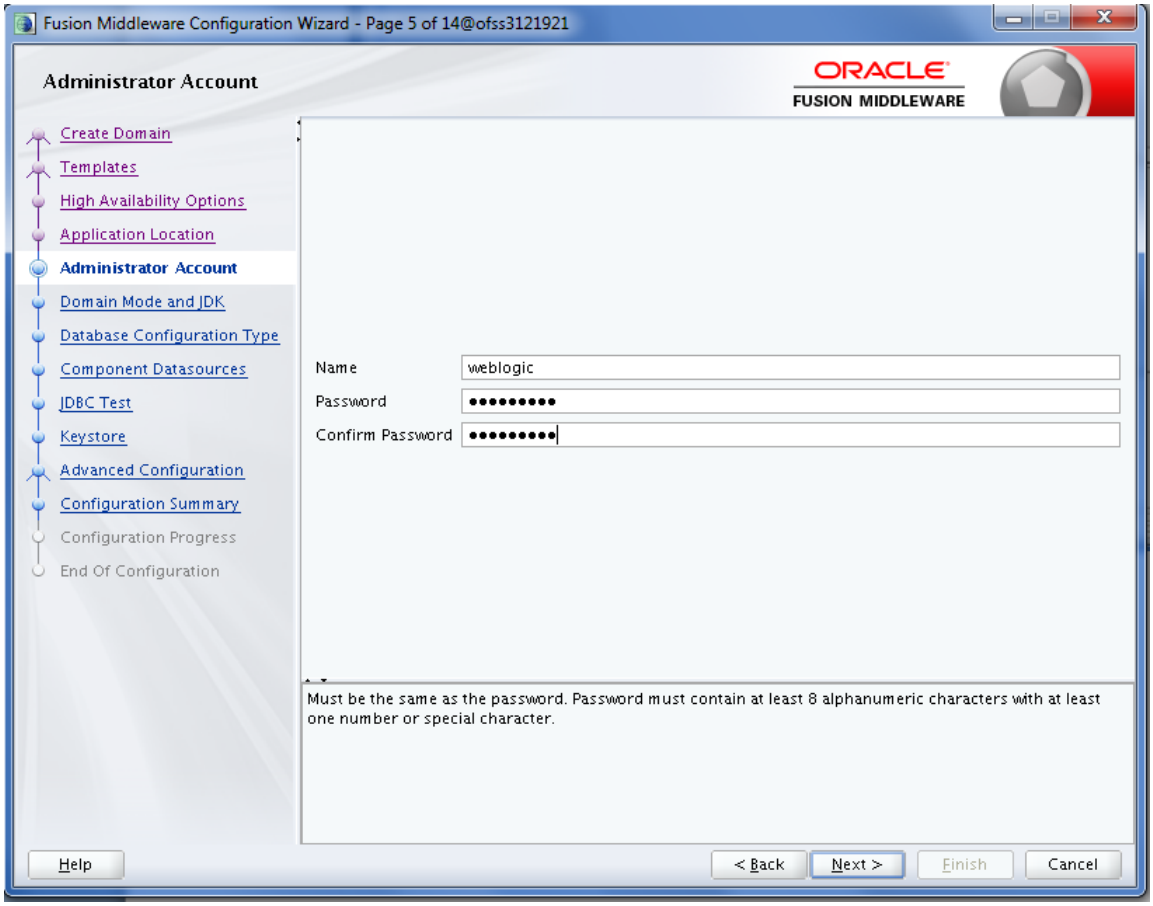
7. In the **Application Location** page, enter the location and then click **Next.**

Figure 6–4 Application Location page



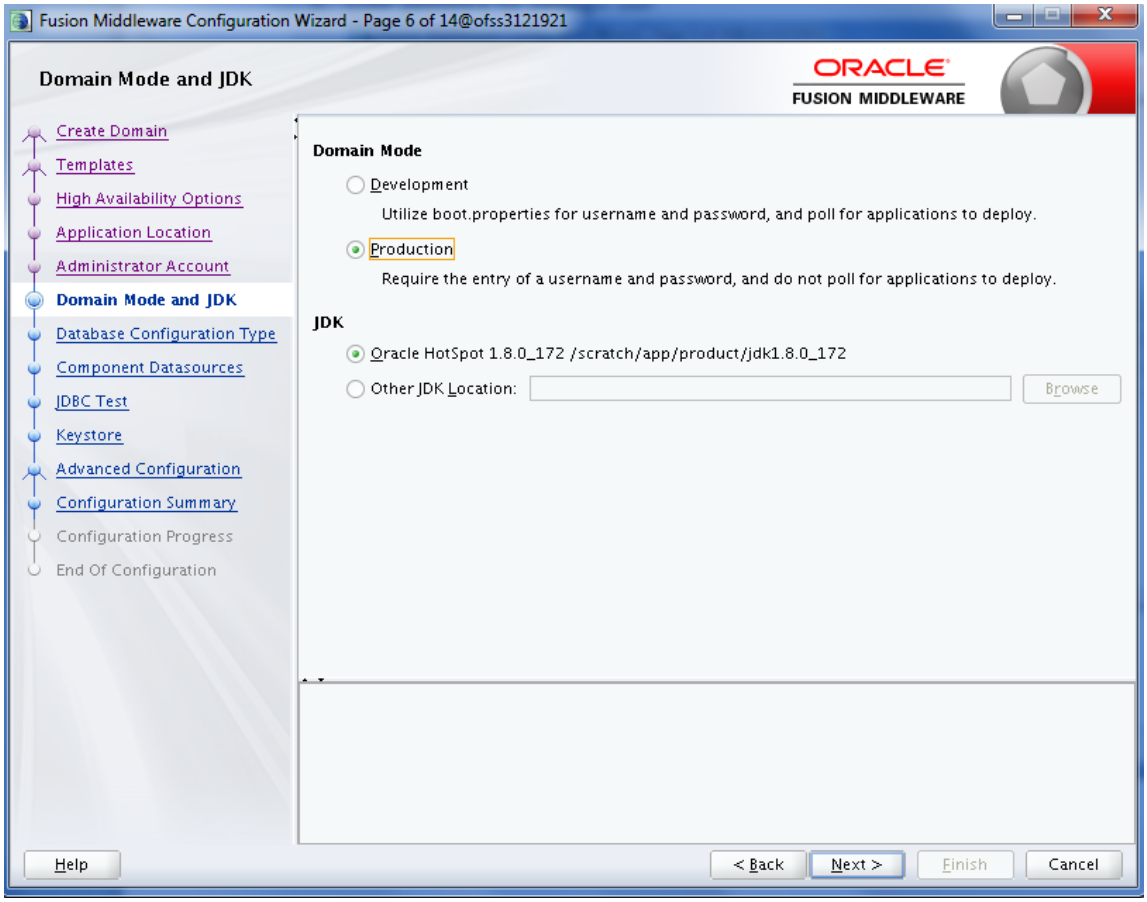
8. In the **Administrator Account** page, enter the password for the weblogic user and then click **Next**.

Figure 6–5 Administrator Account page



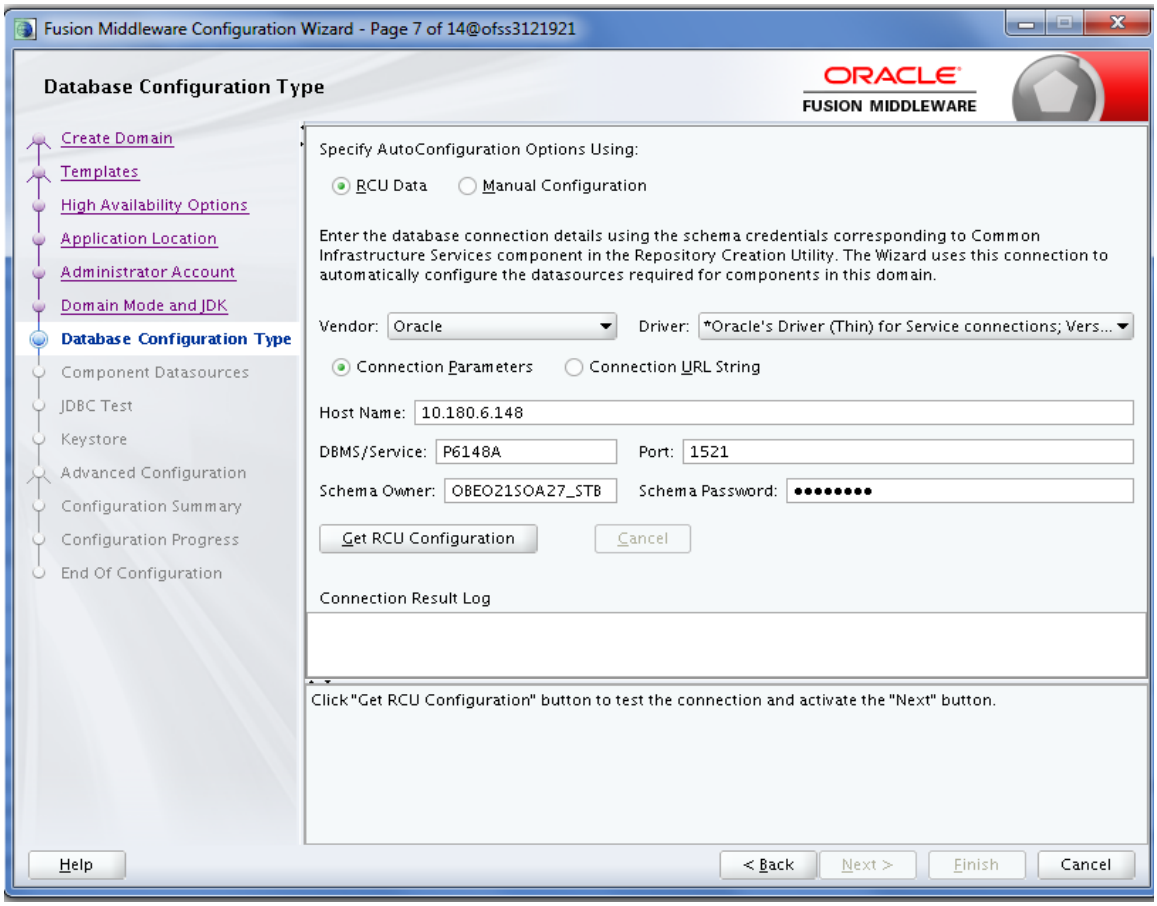
9. In the **Domain Mode and JDK** page, select the **Production** mode and then click **Next**.

Figure 6–6 Domain Mode and JDK page



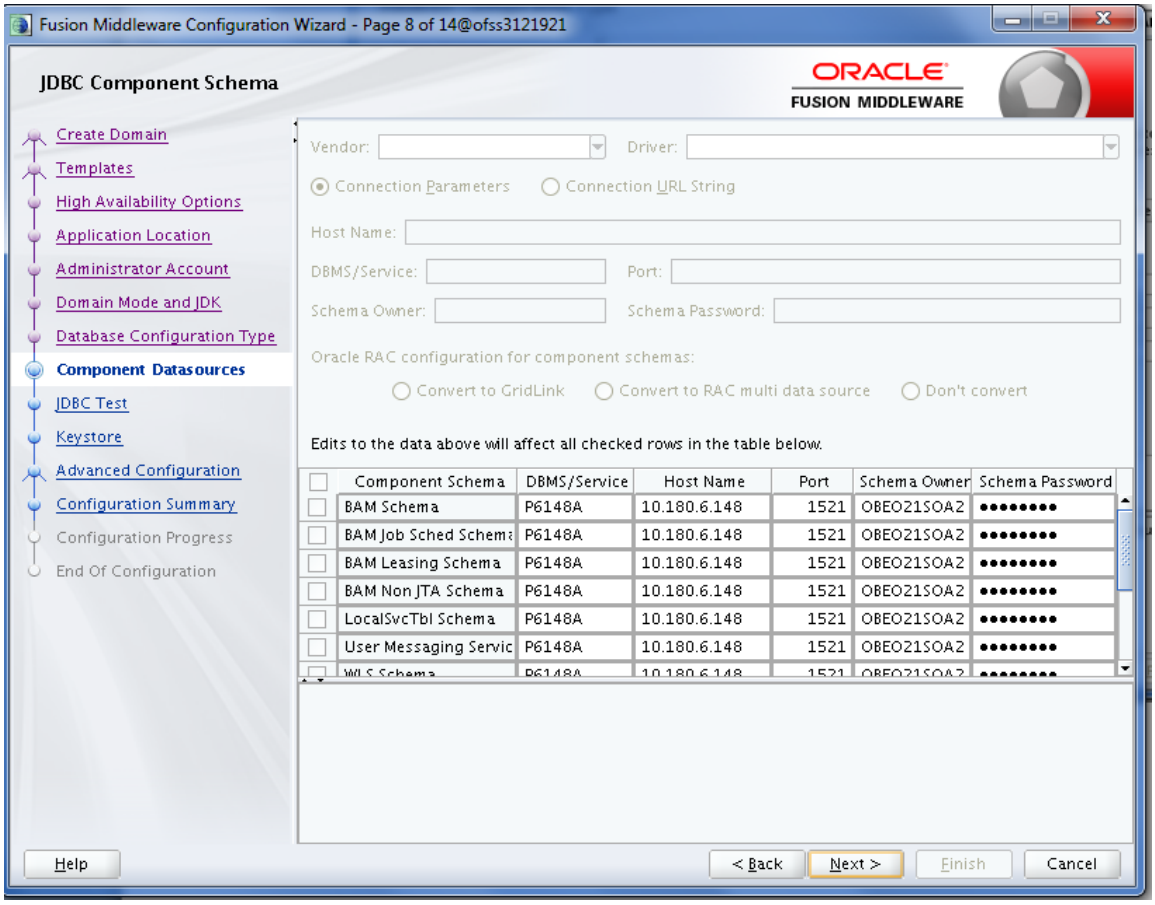
10. In the **Database Configuration Type** page, enter the RCU details and click **Next**.

Figure 6–7 Database Configuration Type page



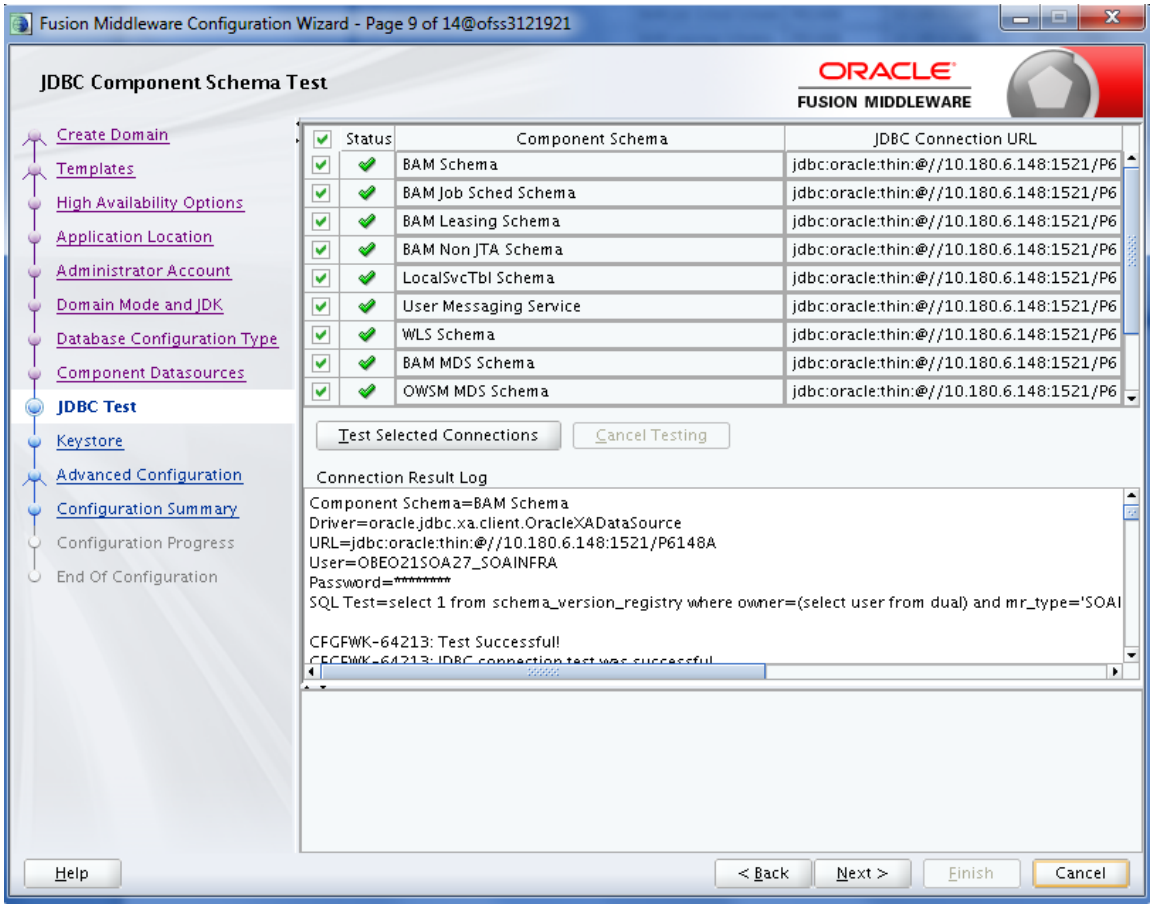
11. In the **Component Datasources** page, click **Next**.

Figure 6–8 Component Datasources page



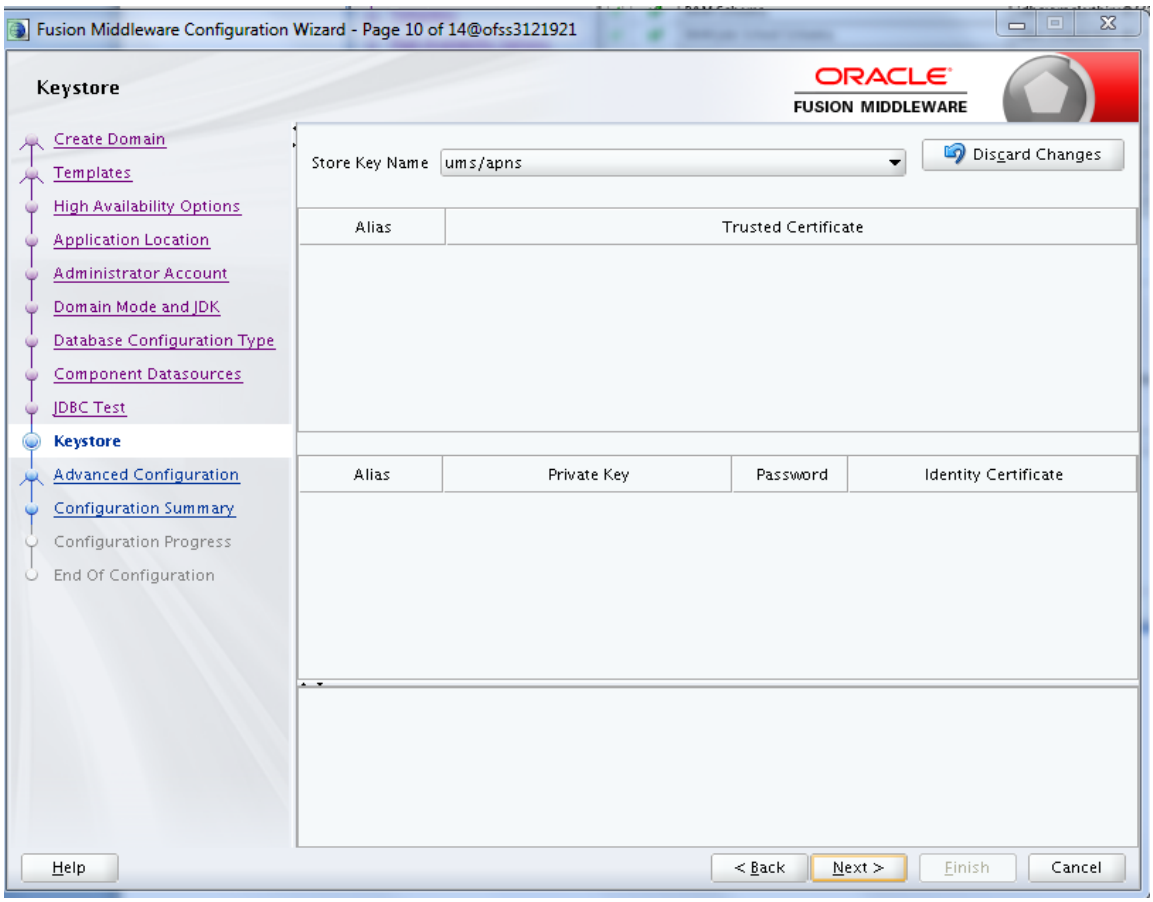
12. In the **JDBC Test** page, click **Test Selected Connections** and then click **Next**.

Figure 6–9 JDBC Test page



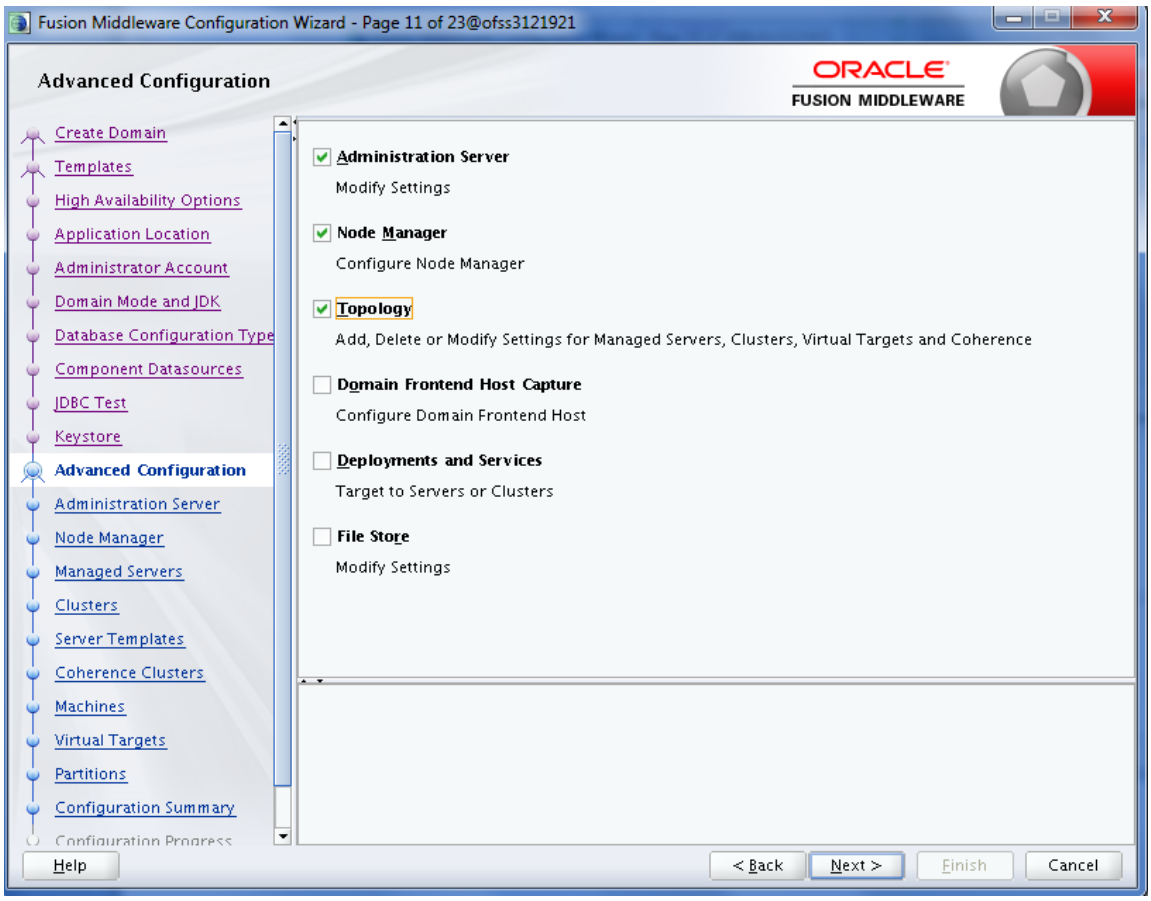
13. In the **Keystore** page, click **Next**.

Figure 6–10 Keystore page



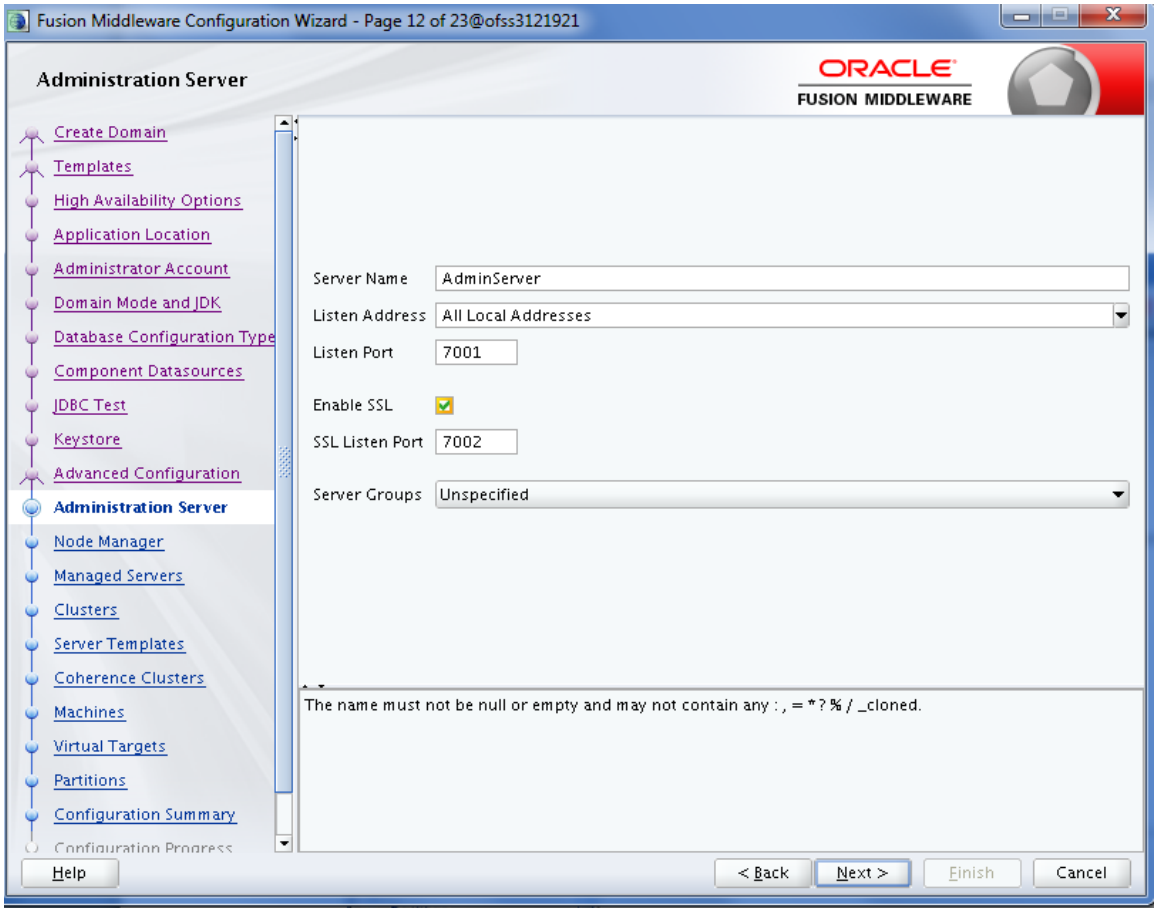
14. In the **Advanced Configuration** page, select the **Administration Server**, **Mode Manager** and **Topology** check boxes and then click **Next**.

Figure 6–11 Advanced Configuration page



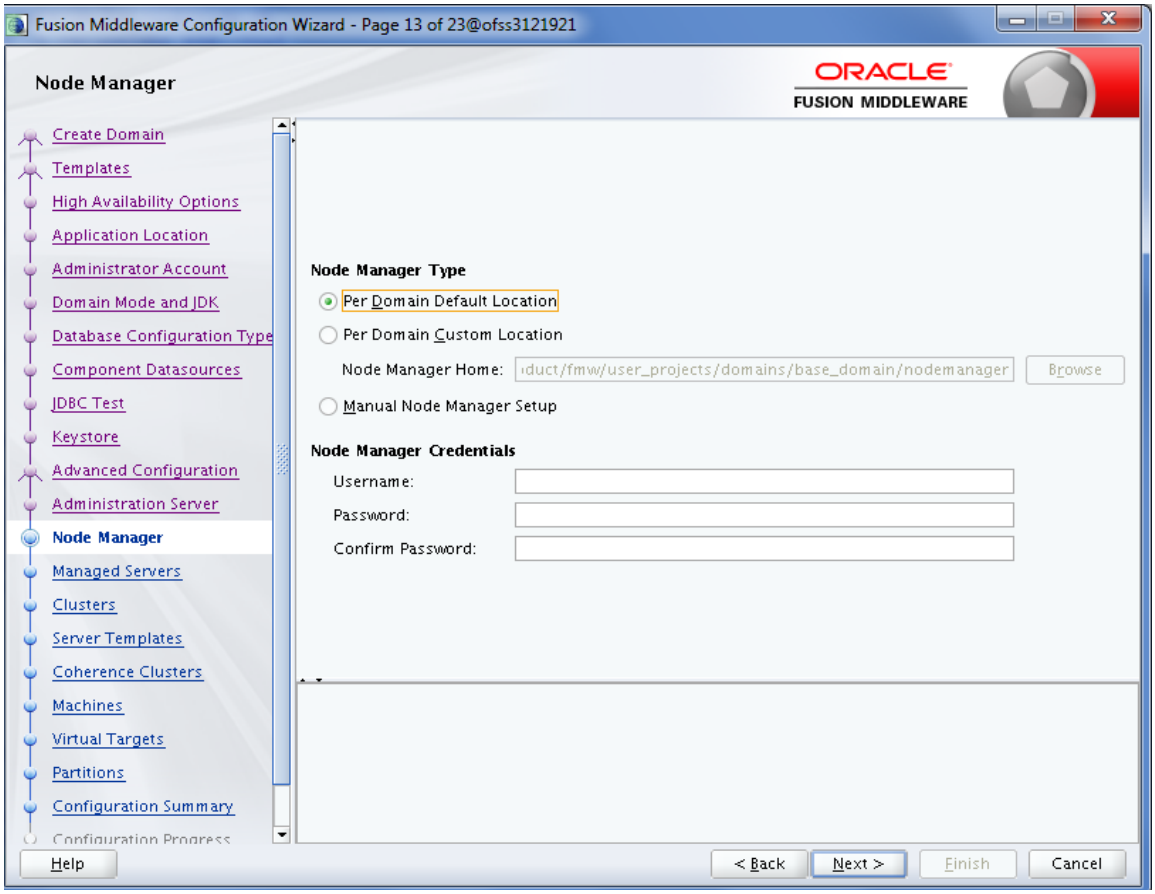
15. In the **Administration Server** page, select the listen address and select the **Enable SSL** check box. Click **Next.**

Figure 6–12 Administration Server page



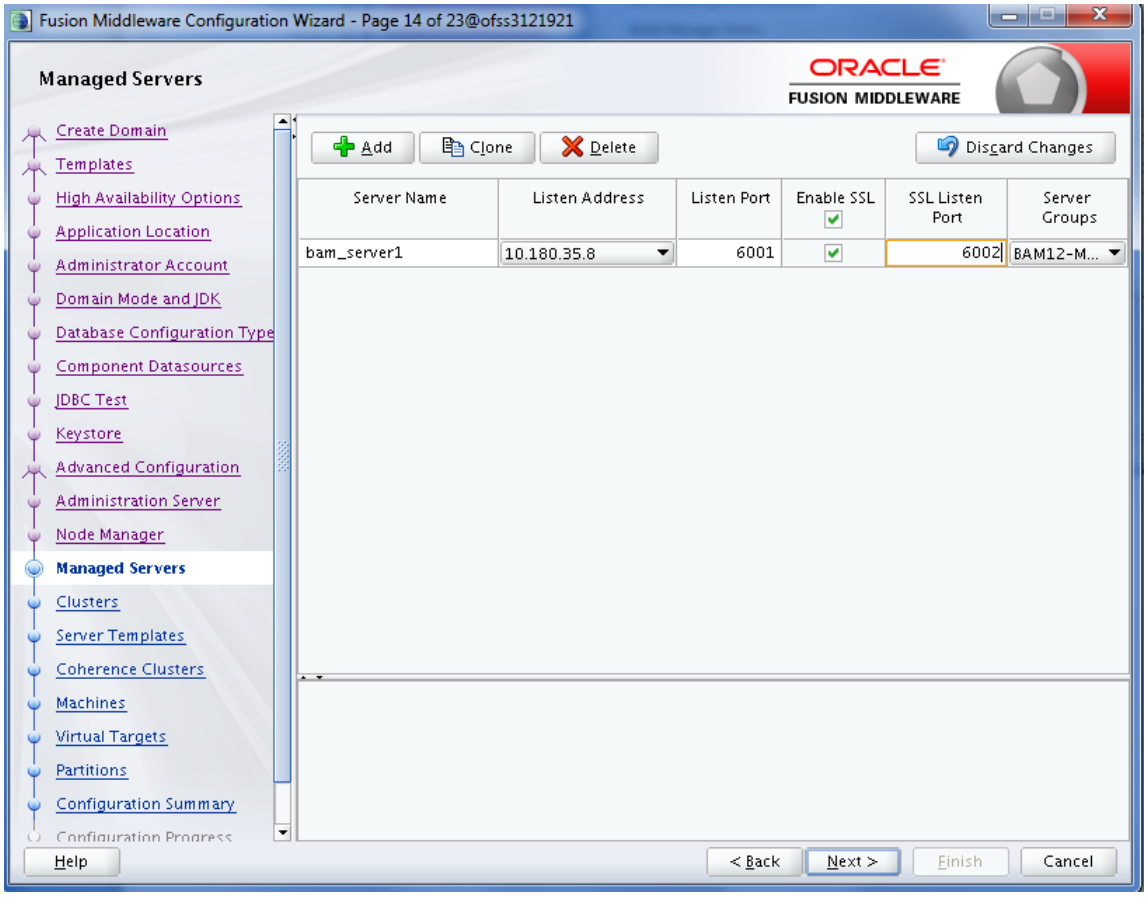
16. In the **Node Manager** page, provide user name and password for node manager, and then click **Next.**

Figure 6–13 Node Manager page



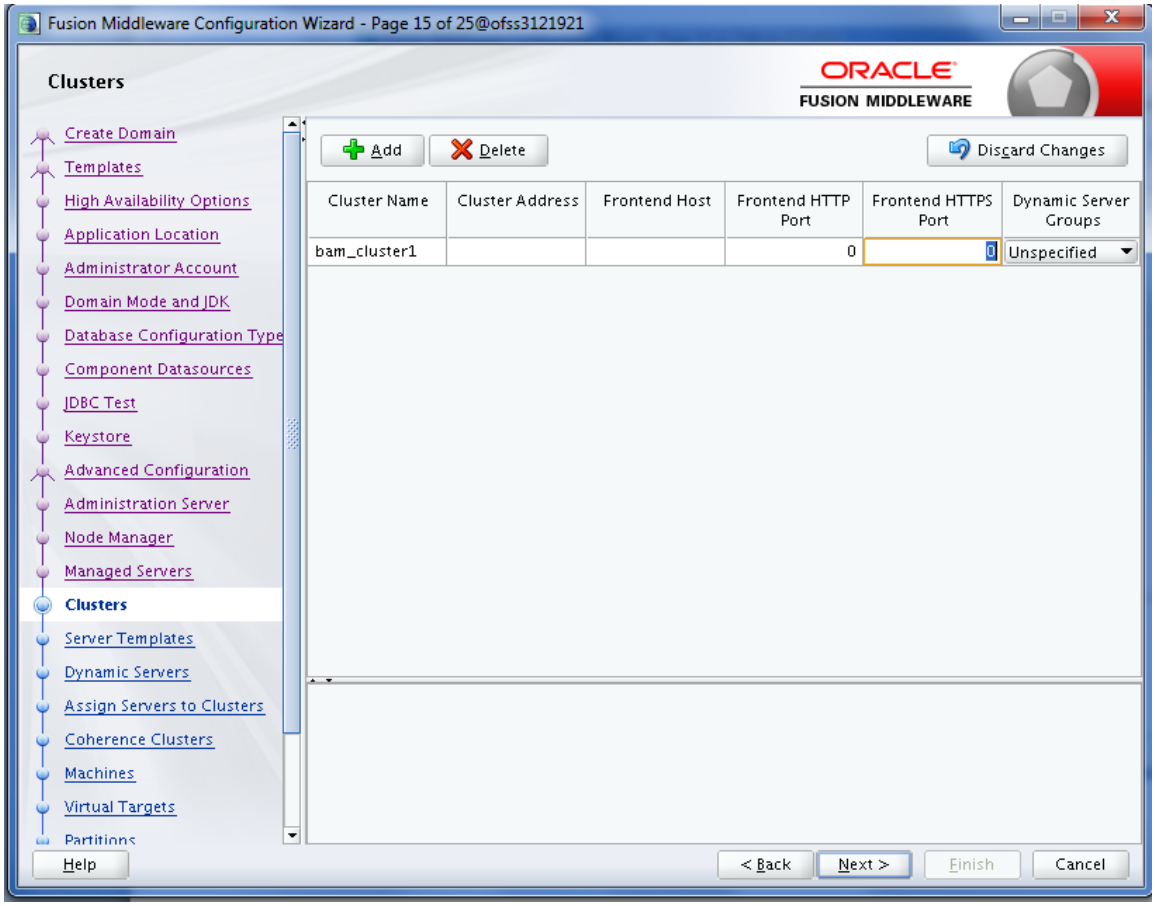
17. In the **Managed Servers** page, add BAM server (bam_server1).

Figure 6–14 Managed Servers page



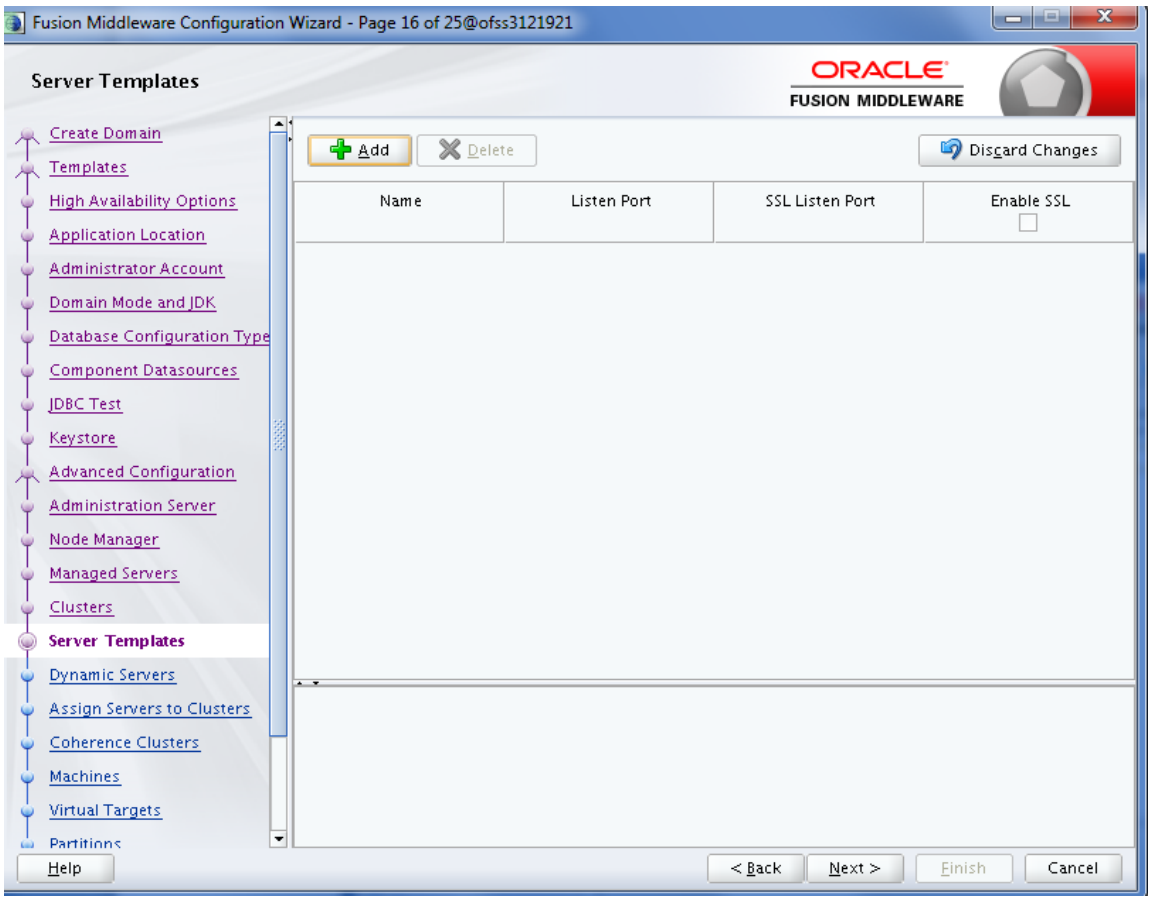
18. Click **Next.**
19. In the **Clusters** page, add BAM cluster and then click **Next.**

Figure 6–15 Clusters page



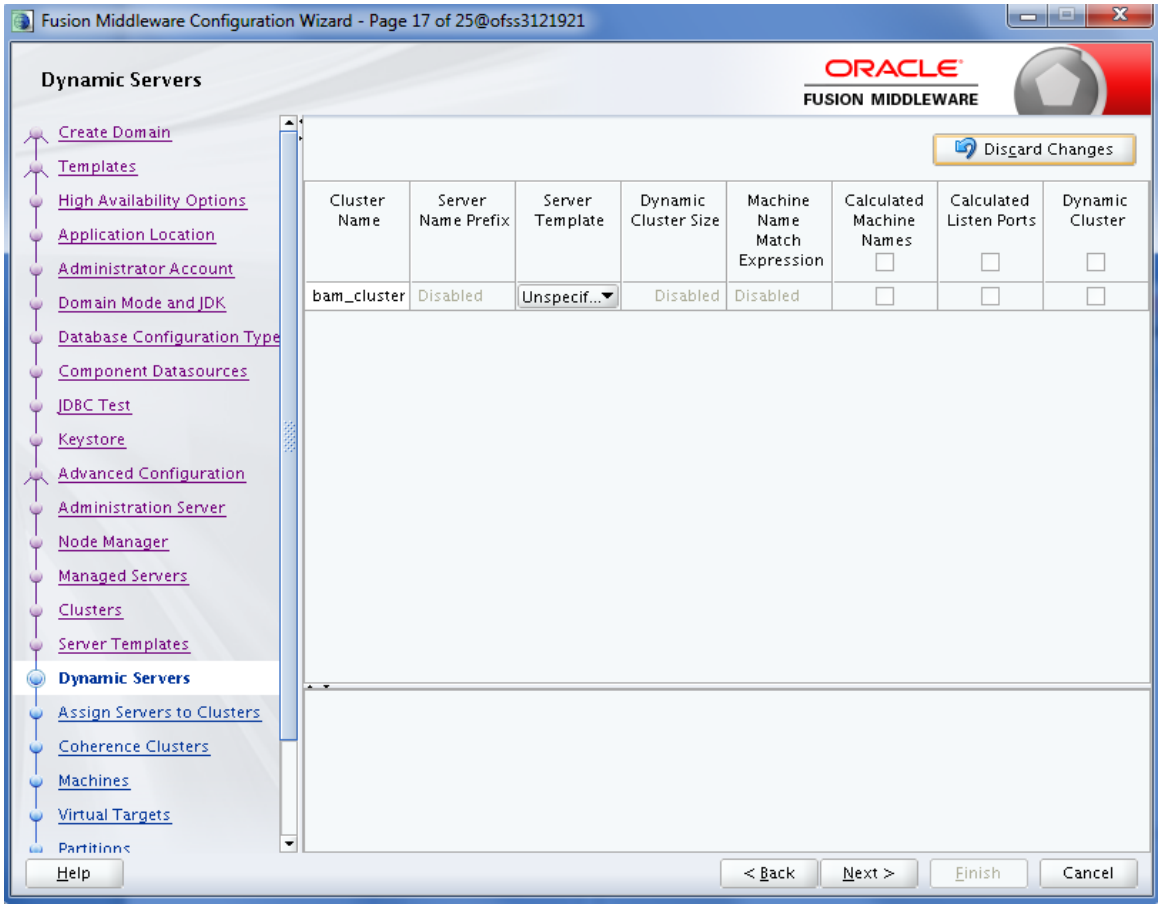
20. In the **Server Templates** page, click **Next**.

Figure 6–16 Server Templates page



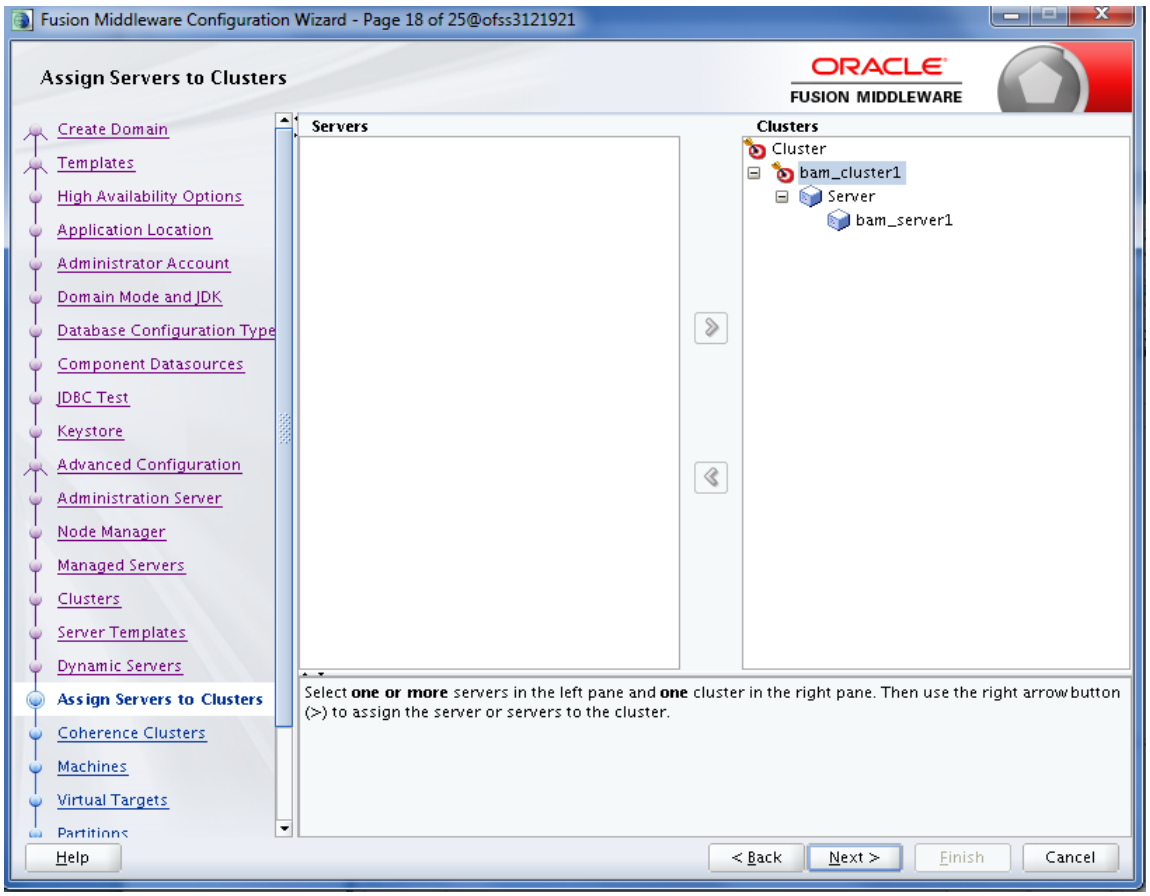
21. In the **Dynamic Servers** page, click **Next**.

Figure 6–17 Dynamic Servers page



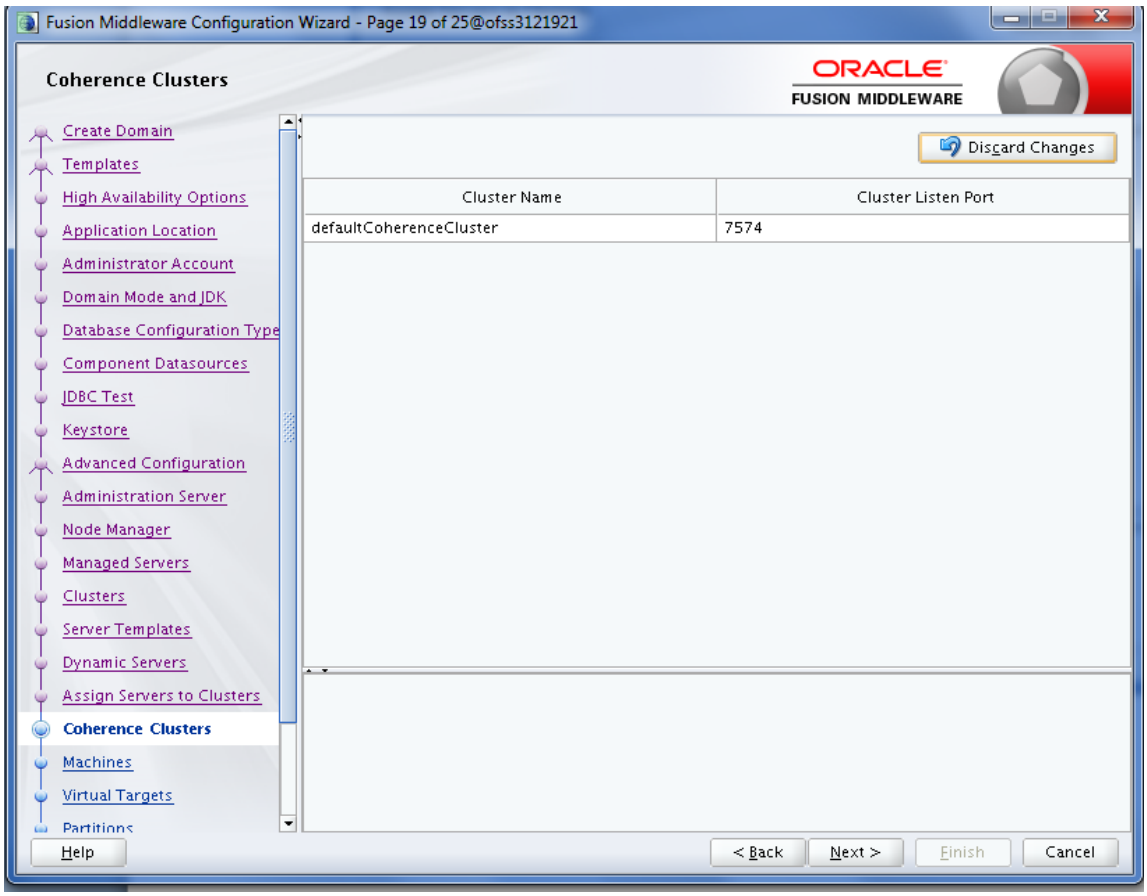
22. In the **Assign Servers to Clusters** page, add BAM server to BAM cluster and click **Next.**

Figure 6–18 Assign Servers to Clusters page



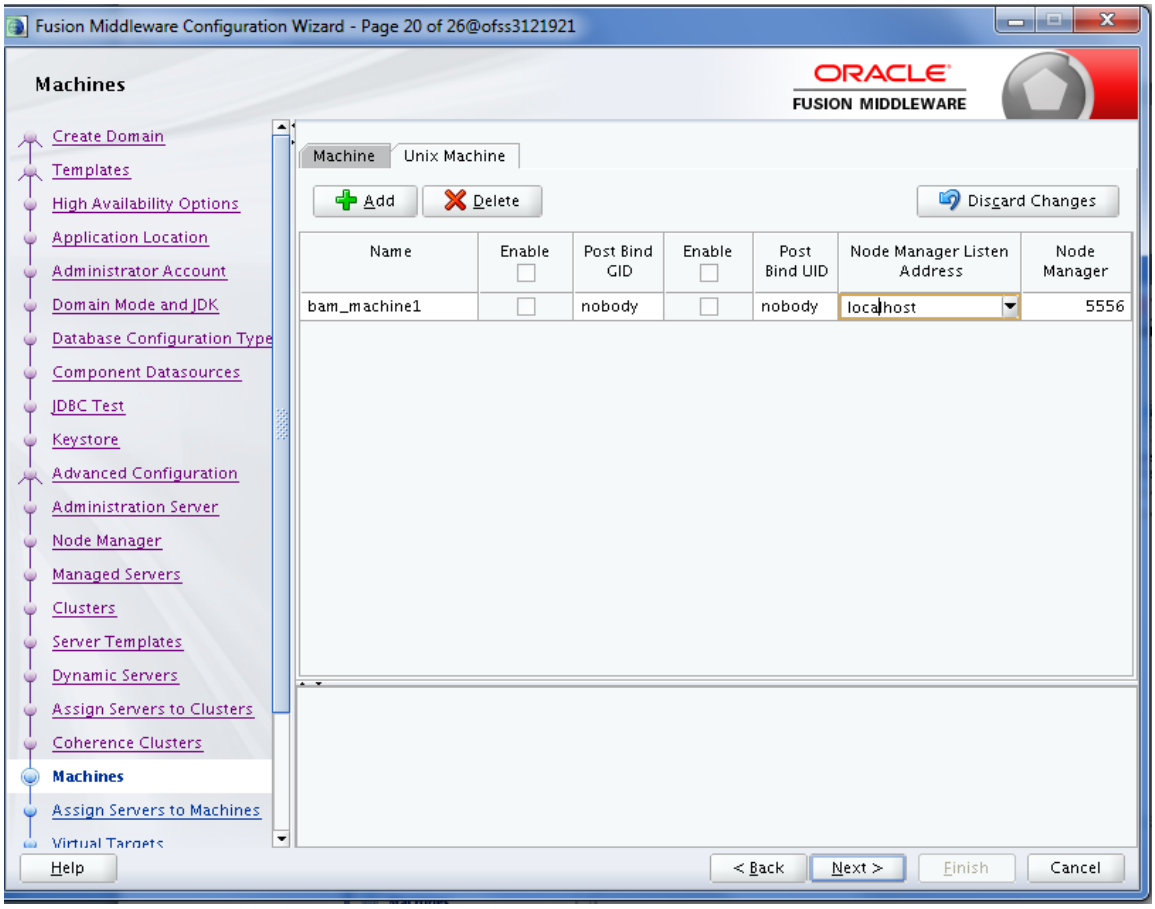
23. In the **Coherence Clusters** page, click **Next.**

Figure 6–19 Coherence Clusters page



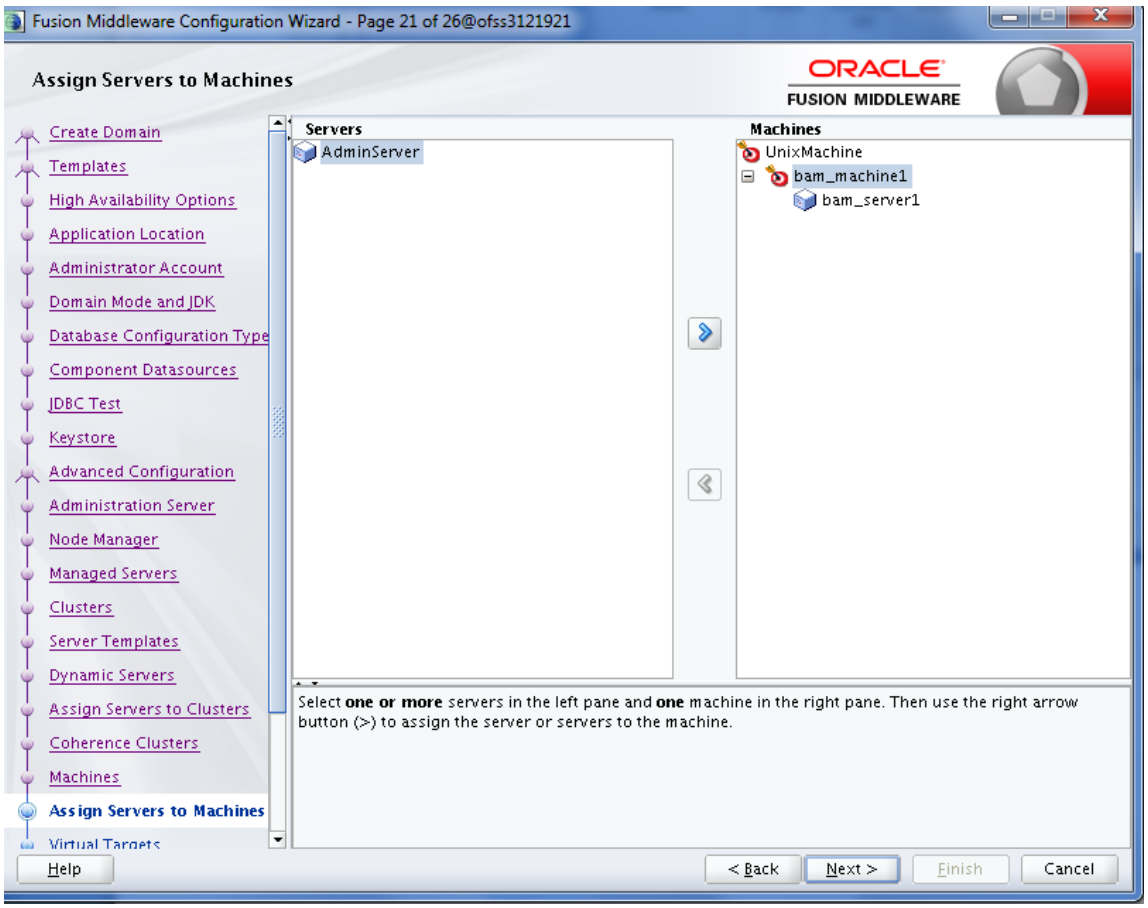
24. In the **Machines** page, add BAM machine and click **Next.**

Figure 6–20 Machines page



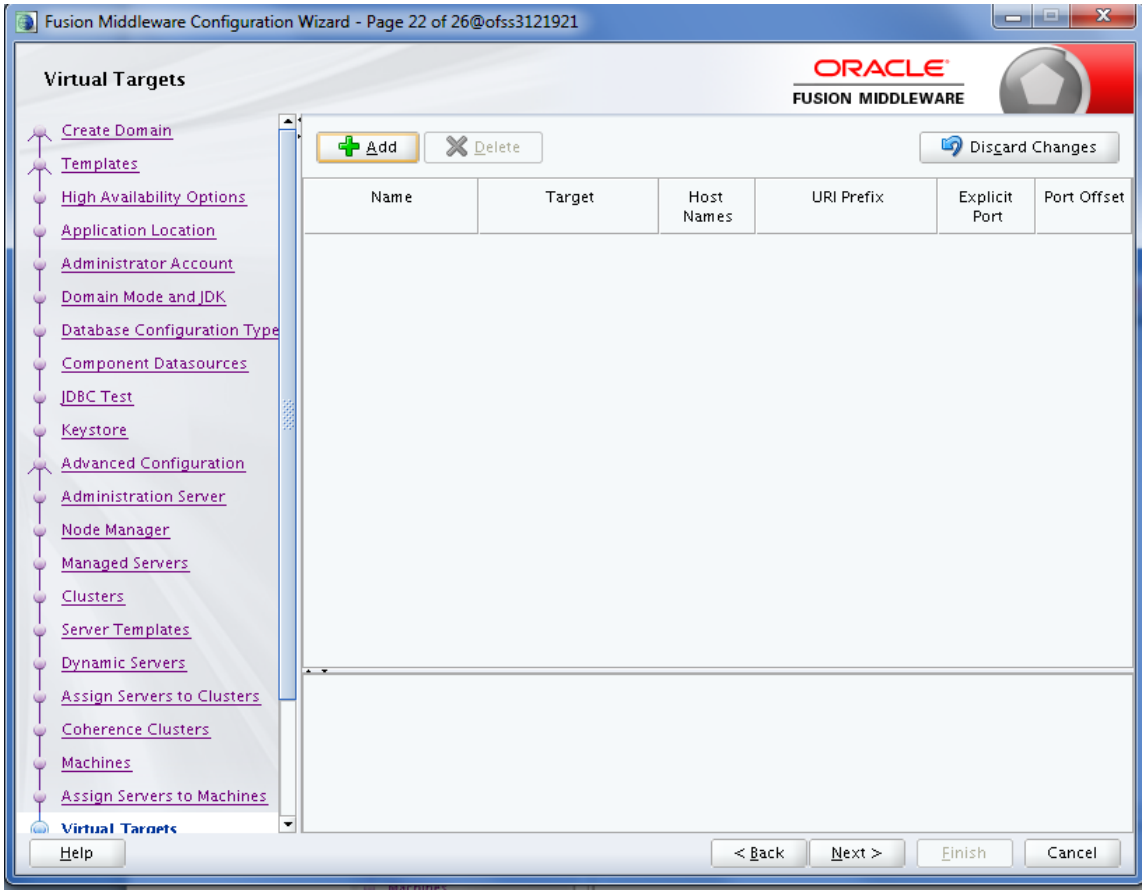
25. In the Assign Servers to Machines page, add BAM server to BAM machine and click **Next.**

Figure 6–21 Assign Servers to Machines page



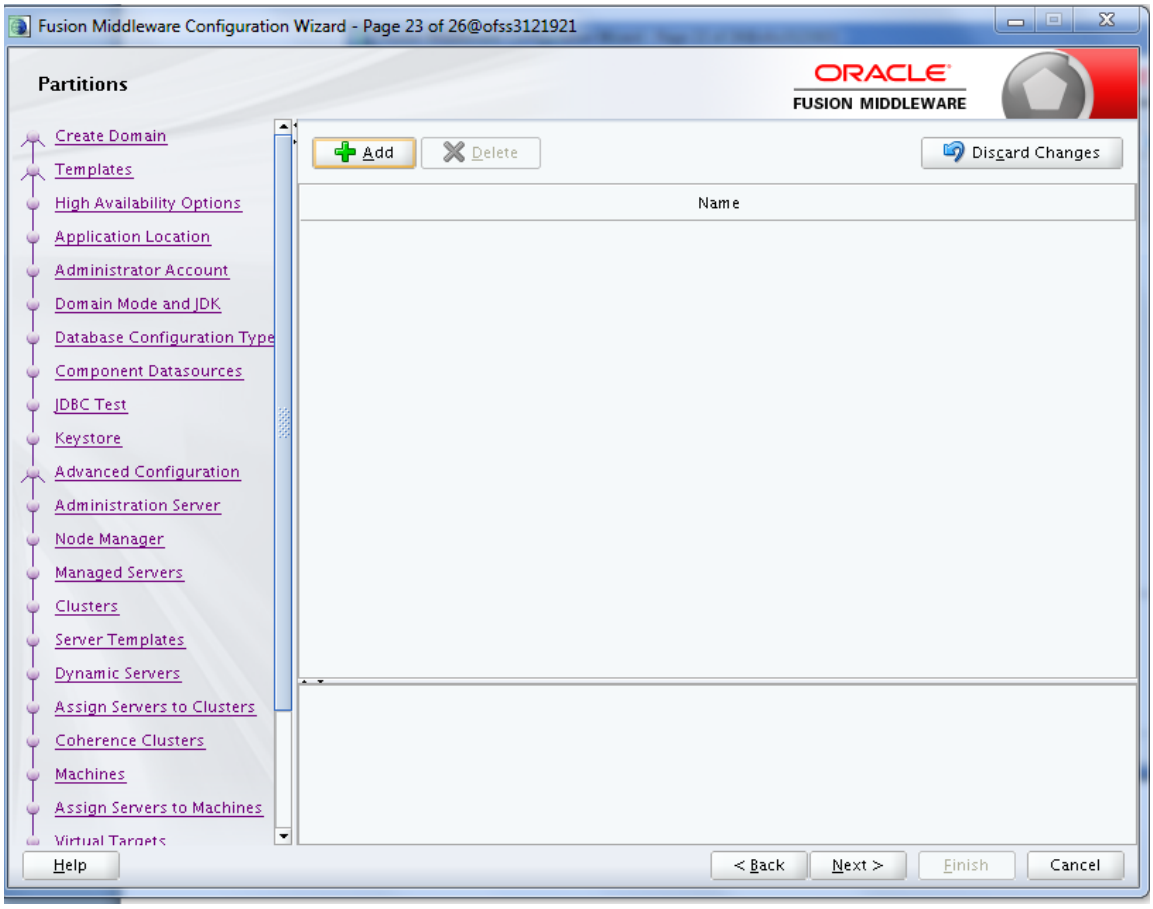
26. In the **Virtual Targets** page, click **Next.**

Figure 6–22 Virtual Targets page



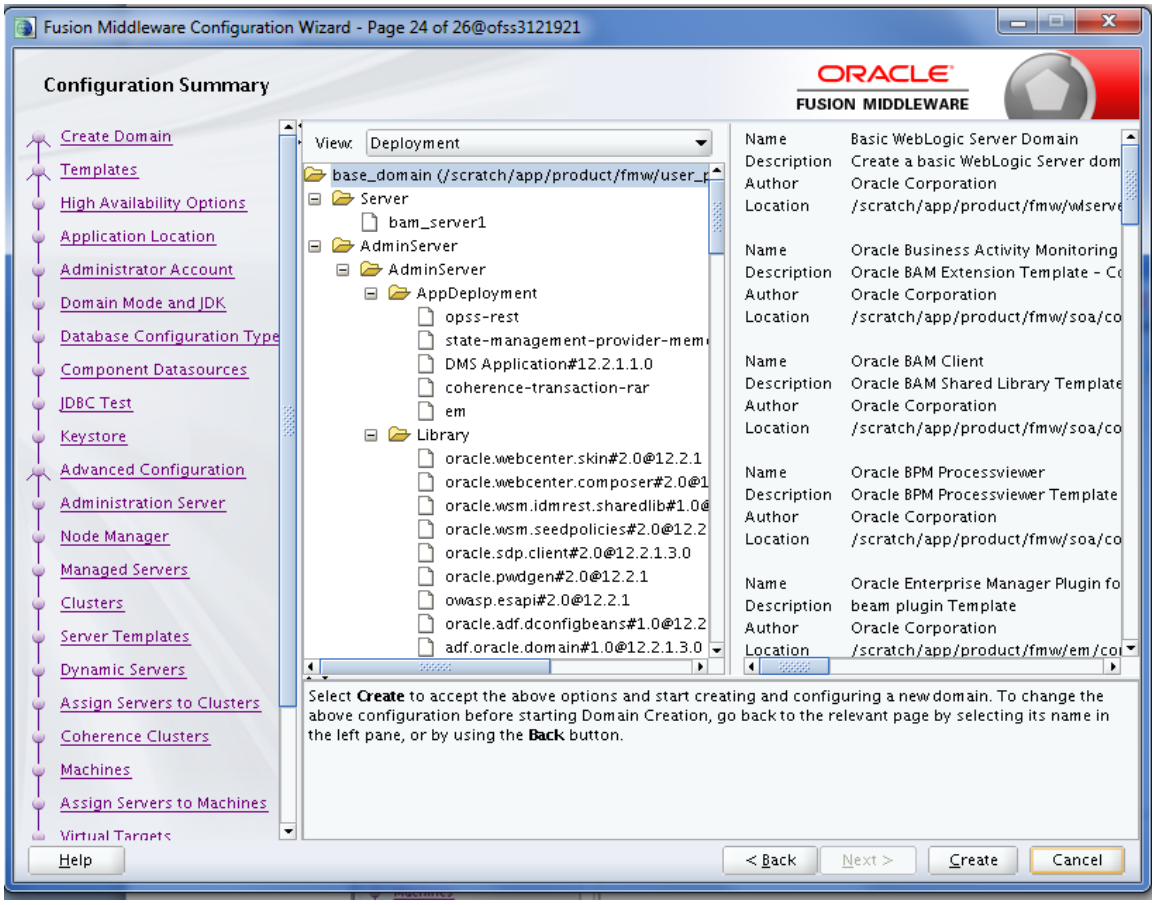
27. In the **Partitions** page, click **Next.**

Figure 6–23 Partitions page



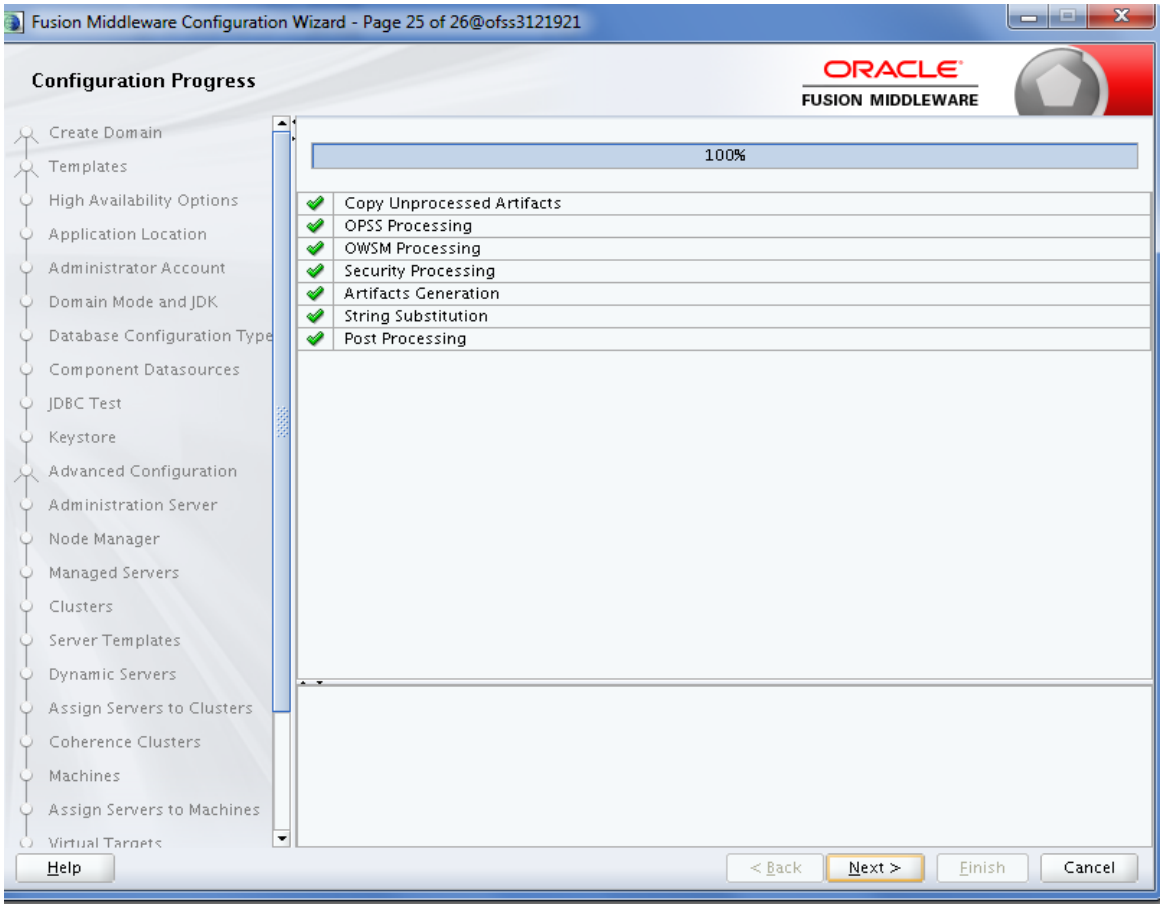
28. In the **Configuration Summary** page, click **Create**.

Figure 6–24 Configuration Summary page



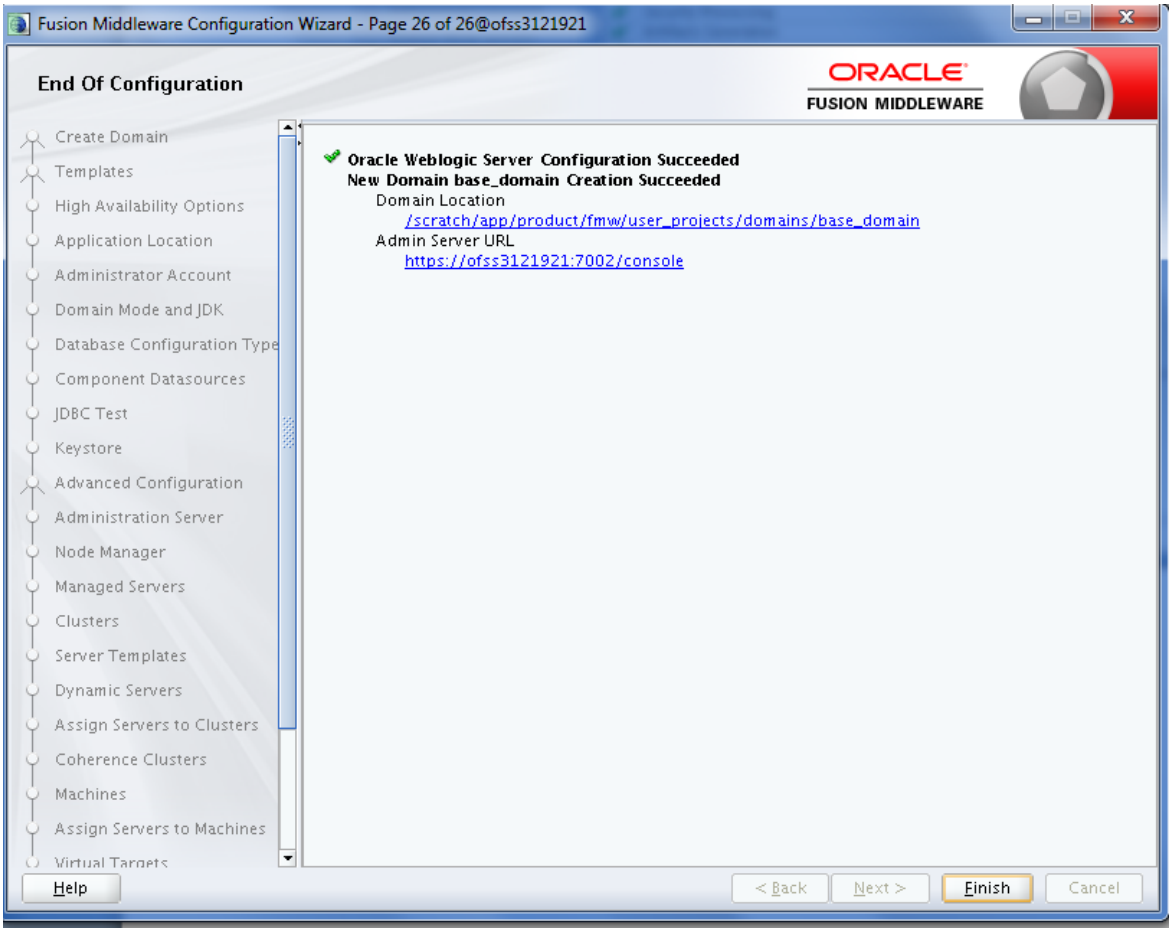
29. In the **Configuration Progress** page, once the progress bar is 100%, click **Next**.

Figure 6–25 Configuration Progress page



30. In the **End of Configuration** page, click **Finish**.

Figure 6–26 End of Configuration page



6.2 Post Installation Configuration

This section describes the post installation configuration procedure for BAM using OBEO Localization SOA Media Pack.

Checklist for Post Installation Procedure

Before proceeding with the post installation, ensure the following:

1. Apply the grant on middleware home through WLST.

   ```
   grantPermission(appStripe=None, principalClass=None,
   principalName=None, codeBaseURL='file:/<middleware_home>/-',
   permClass='java.security.AllPermission', permTarget=None,
   permActions=None)
   ```

   Example:

   grantPermission(appStripe=None, principalClass=None, principalName=None, codeBaseURL='file:/scratch/app/product/fmw/-', permClass='java.security.AllPermission', permTarget=None, permActions=None)

2. Start the admin server.

```
$cd <MIDDLEWARE_HOME >/user_projects/domains/domain_name/bin
$./startWeblogic.sh
```

3. Start the managed server "bam_server1".

```
$cd <MIDDLEWARE_HOME>/user_projects/domains/domain_name/bin
$./startManagedWebLogic.sh <managed server name>
t3://localhost:<admin server port>
```

Post Installation Configuration

Perform the following steps.

1. Copy the “obpus-ui-soa.zip” or “obpau-ui-soa.zip” file to a machine where BAM domain is created.
2. Unzip the “obpus-ui-soa.zip” or “obpau-ui-soa.zip” file. Following three files will be extracted:
   - Namely a zip file “obpinstall-ui-soa.zip”
   - Installation script “installobpsoa.sh”
   - Install configuration property file “installobpsoa.properties”
3. Create a folder called target and unzip obpinstall-ui-soa.zip file.
4. Create a folder called obpinstall/obp/ob.bam under < BAM_MW_HOME >.
5. Unzip bam.zip under < BAM_MW_HOME >/obpinstall/obp/ob.bam/.
6. Update the following values in BAMCommandConfig.xml.tmpl present under target folder:

```
<host>#BAM_SERVER_LISTEN_ADDRESS#</host>
<port>#BAM_SERVER_LISTEN_PORT#</port>
<username>#WEBLOGIC_USERNAME#</username>
<password>#WEBLOGIC_PASSWORD#</password>
<dbusername>#SOA_INFRASTRUCTURE_SCHEMA_USER#</dbusername>
<dburl>jdbc:oracle:thin:@#DB_IP#:#DB_PORT#:#DB_SERVICE_
NAME#</dburl>
```

7. Copy BAMCommandConfig.xml.tmpl to $BAM_MW_HOME/soa/bam/bin/BAMCommandConfig.xml
8. cp –r BAMCommandConfig.xml.tmpl $BAM_MW_HOME/soa/bam/bin/BAMCommandConfig.xml
9. EXPORT BAM_MW_HOME=/scratch/app/product/fmw
10. Go to target directory and execute below command.

```
chmod 777 bam.sh
sh bam.sh $BAM_MW_HOME
```

11. Restart the bam managed server "bam_server1".

```
$cd <MIDDLEWARE_HOME>/user_projects/domains/domain_name/bin
$./startManagedWebLogic.sh <managed server name>
t3://localhost:<admin server port>
```

12. Log in to BAM Composer http: //$IP:PORT/bam/composer/faces/login.

Figure 6–27 BAM Composer page

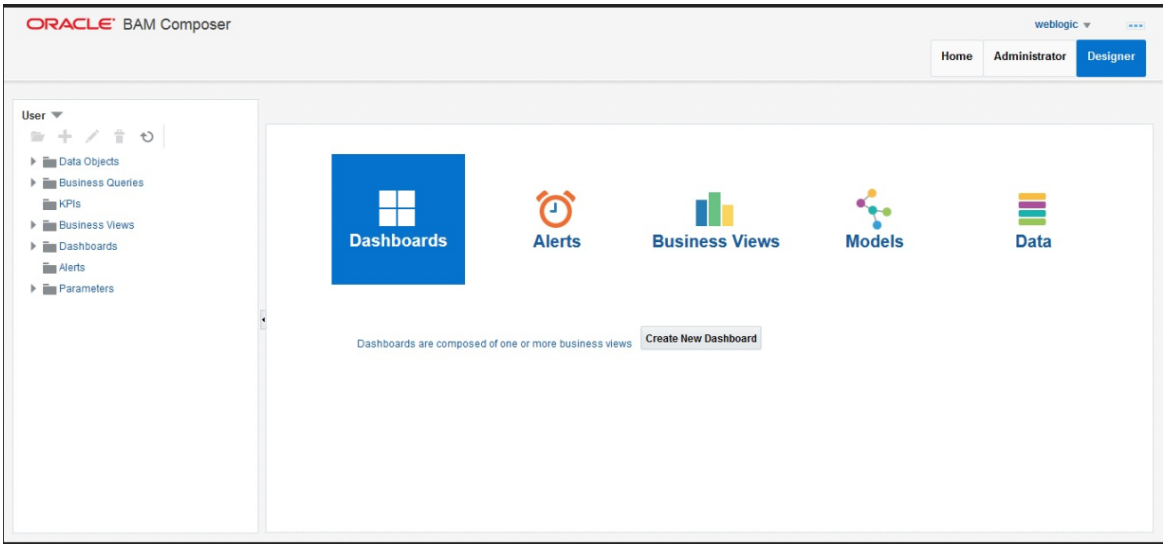


Figure 6–28 BAM Composer page (contd)

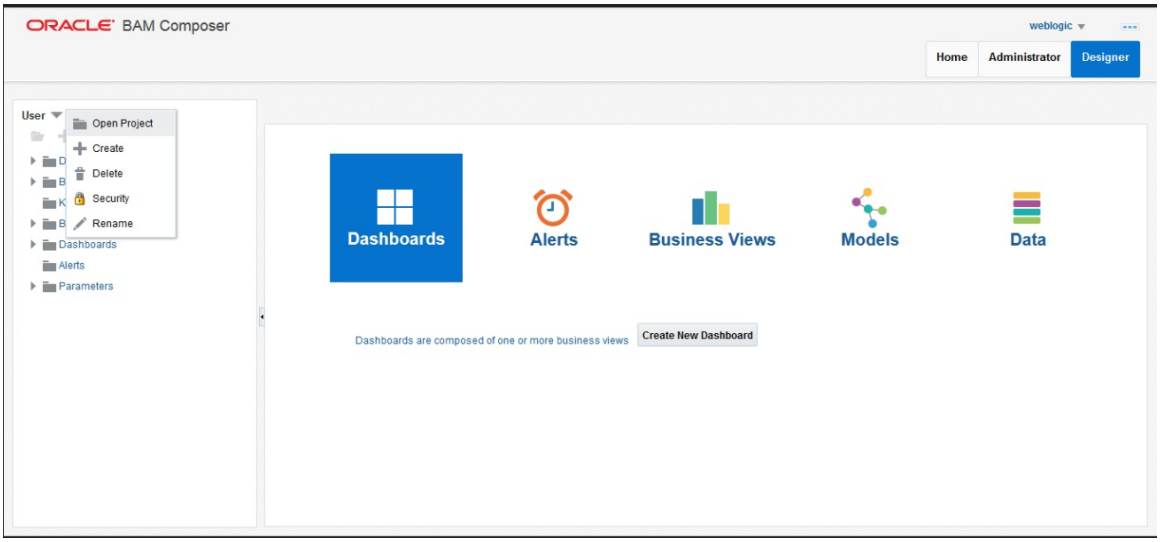
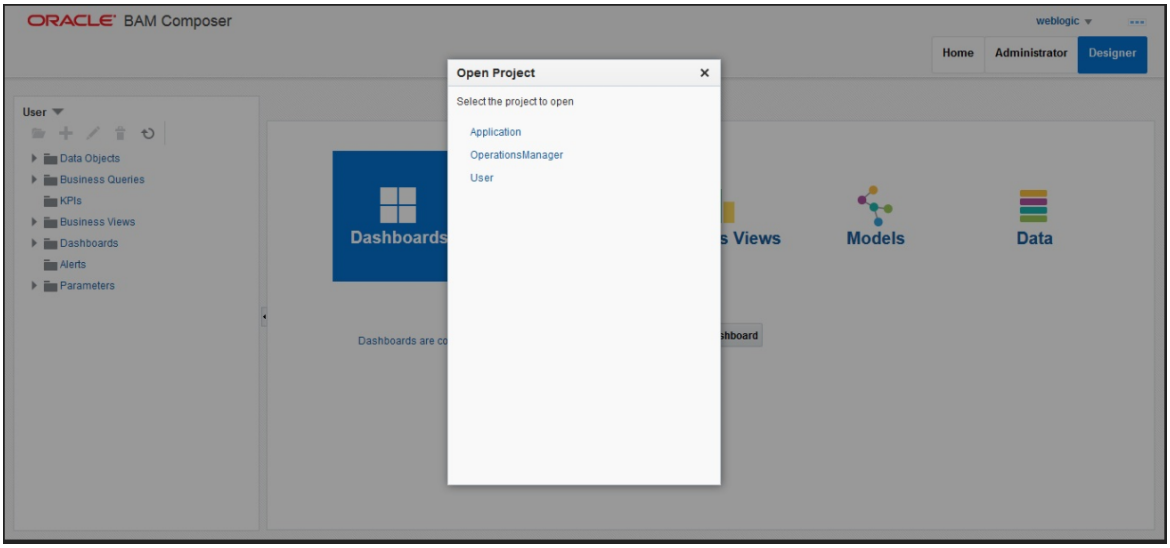


Figure 6–29 BAM Composer page



7 Standalone Database Setup

This chapter details the steps involved in setting up Oracle Banking Enterprise Originations database.

7.1 Pre-Installation Steps

The following steps should be completed prior to the process of executing the installation steps for the Oracle Banking Enterprise Originations DB mentioned in Section 7.2 OBEO Database Setup – RCU Installation:

1. Oracle Database 19c Enterprise Edition Release 19.8 is installed on the database server.
2. Obtain the tar file dbScripts_us.tar.gz or dbScripts_au.tar.gz (present in obpau-host.zip) from OBEO Host localization media pack and copy it onto the database server.
3. Ensure that the ONS service is started after DB installation where the OBEO Application schema needs to be created.

7.2 OBEO Database Setup – RCU Installation

The steps that should be performed to create the OBEO Host DB schema are provided in Section 7.3.1 Host DB Schema Creation and Verification

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

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

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

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

- UI_STB
- UI_OPSS
- UI_MDS
- UI_IAU_APPEND

- UI_IAU_VIEWER
- UI_WLS_RUNTIME

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

UI_MDS and UI_STB schemas are used by UI component.

HOST_MDS and HOST_STB schemas are used by HOST component.

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

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

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

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

7.3 OBEO 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.

7.3.1 Host DB Schema Creation and Verification

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

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

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

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

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

createobp.sql execution

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

7.3.2 HOST DB schema ddl execution

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

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

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

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

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

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

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

7.3.3 HOST DB Schema Seeding

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

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

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

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

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

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

Note

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

7.3.4 System Configuration DB Update Script Execution

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

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

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

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

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

7.3.5 Removing Preference Refresh Level

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

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

For example:

<Preference name="MiddlewareTaskMetadataDTOFieldConfig"

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

parent="jdbcpreference"

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

COD_ATTR_ID valuekey, FIELD_NAME AS valuestring FROM flx_fw_mw_tasks_dto_map"

syncTimeInterval="-1" />

7.3.6 Database Table Partitioning

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

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

8 OBEO and IPM Integration

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

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

- Section 8.1 IPM Application Setup for OBEO Content Management
- Section 8.2 IPM Configuration for Bulk Upload Process Setup
- Section 8.3 IPM Report Upload Setup

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

8.1 IPM Application Setup for OBEO Content Management

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

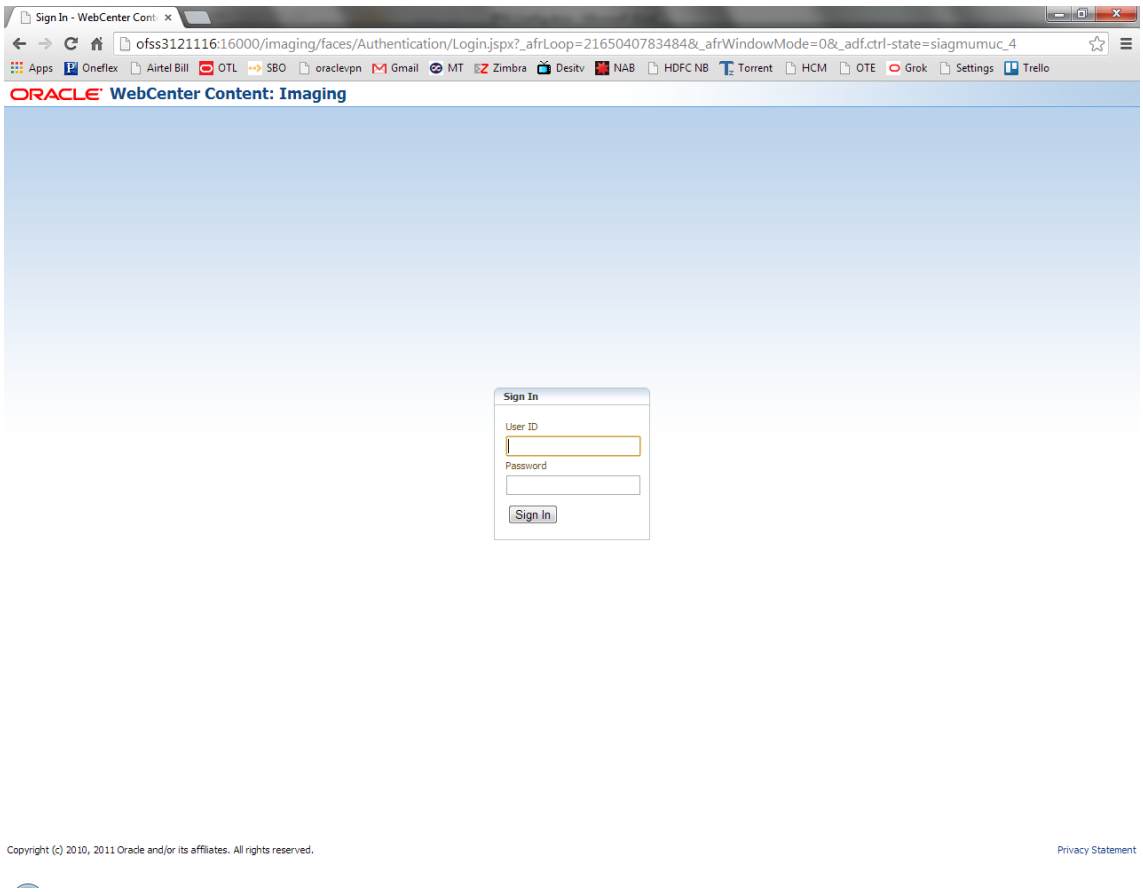
8.1.1 UCM Connection

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:

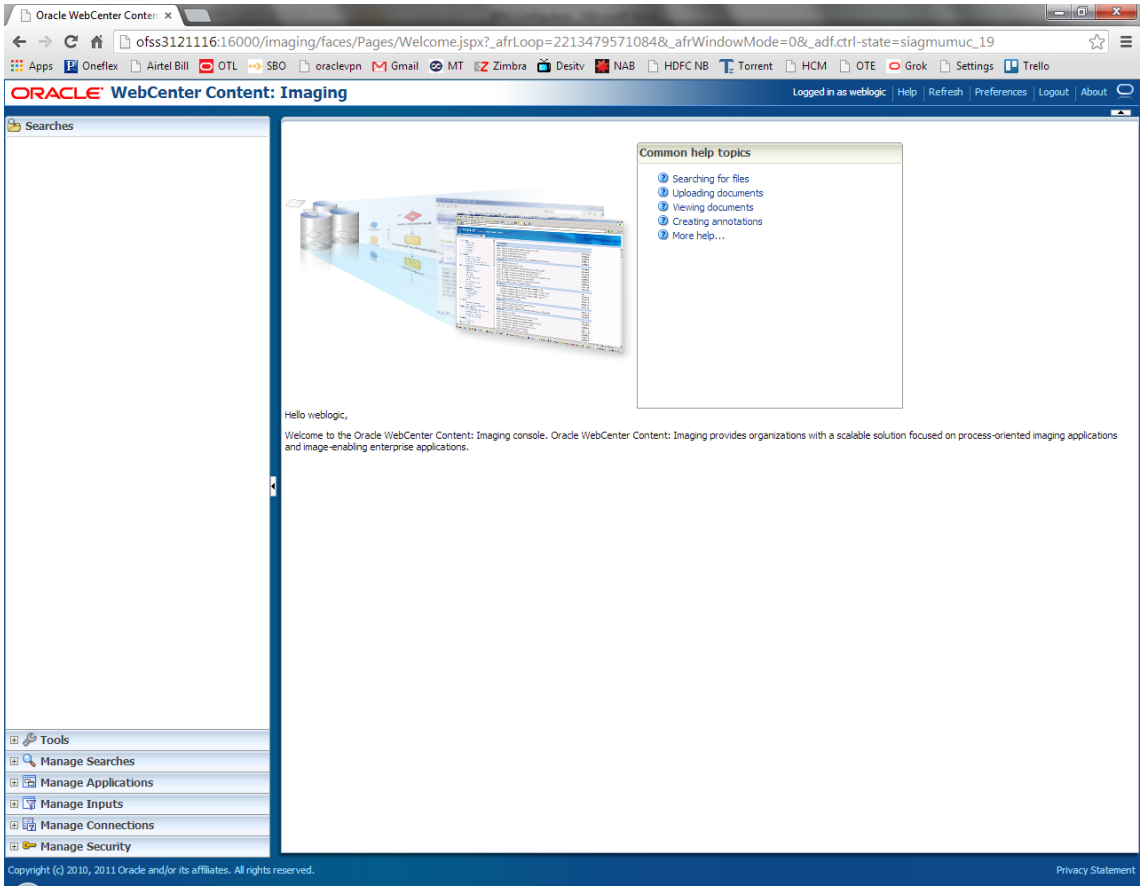
   http:// hostname:16000/imaging

Figure 8–1 IPM Imaging Console - Login page



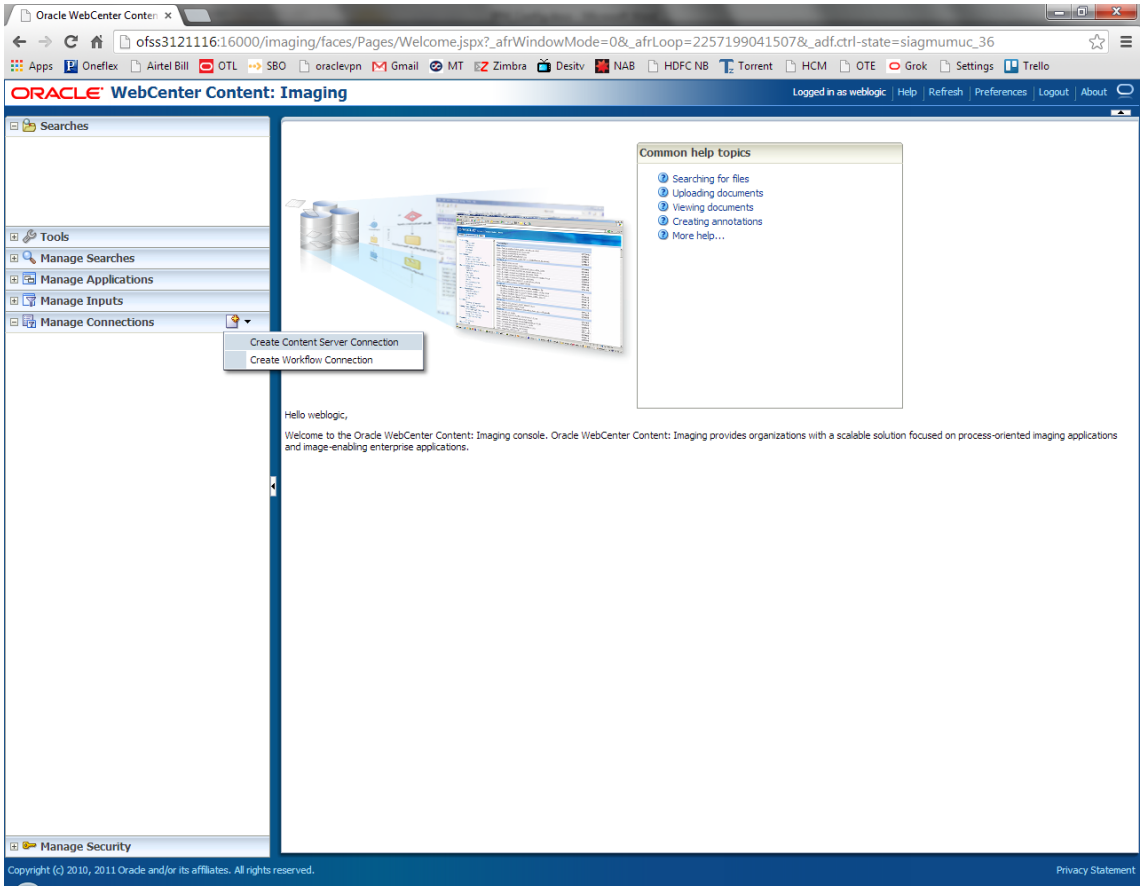
2. Enter the user ID and password set during IPM installation.

Figure 8–2 IPM - Welcome page



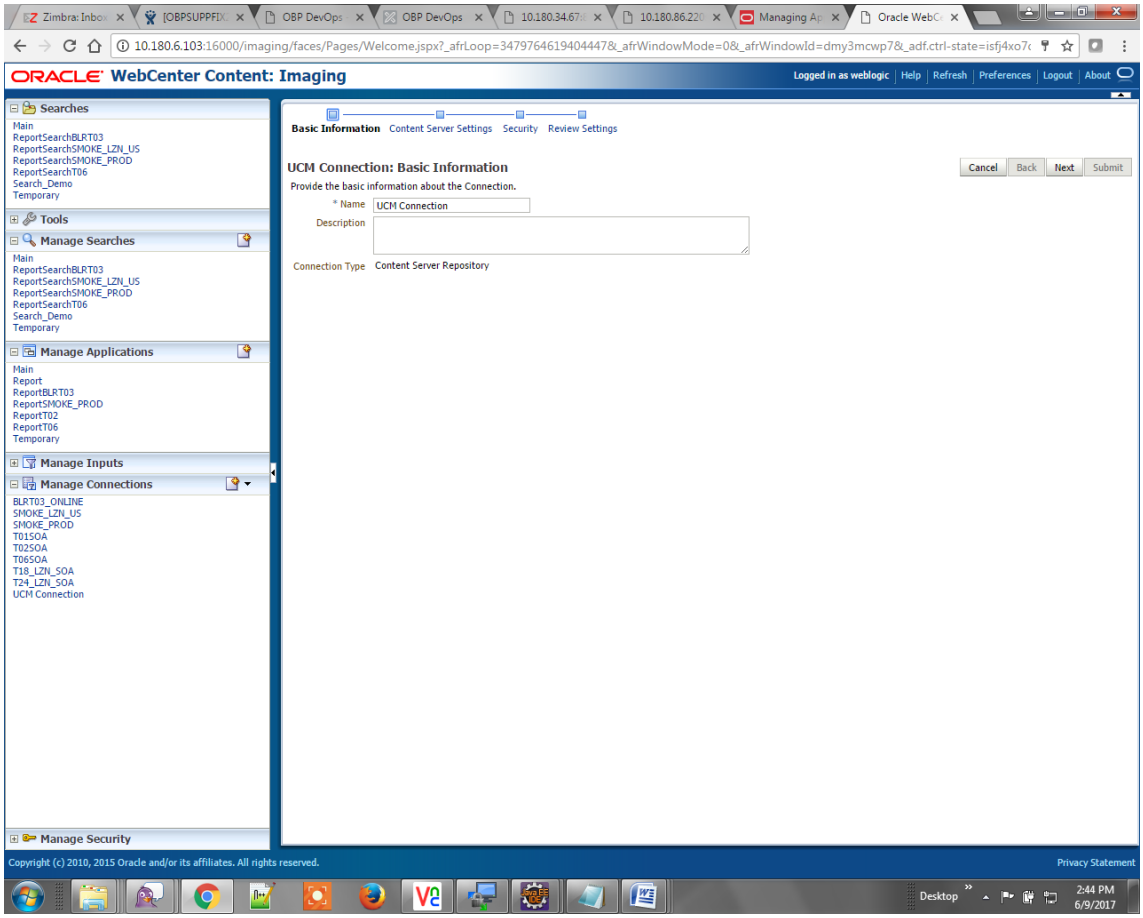
3. Navigate to Manage Connection and select Create Content Server Connection.

Figure 8–3 Create Content Server Connection



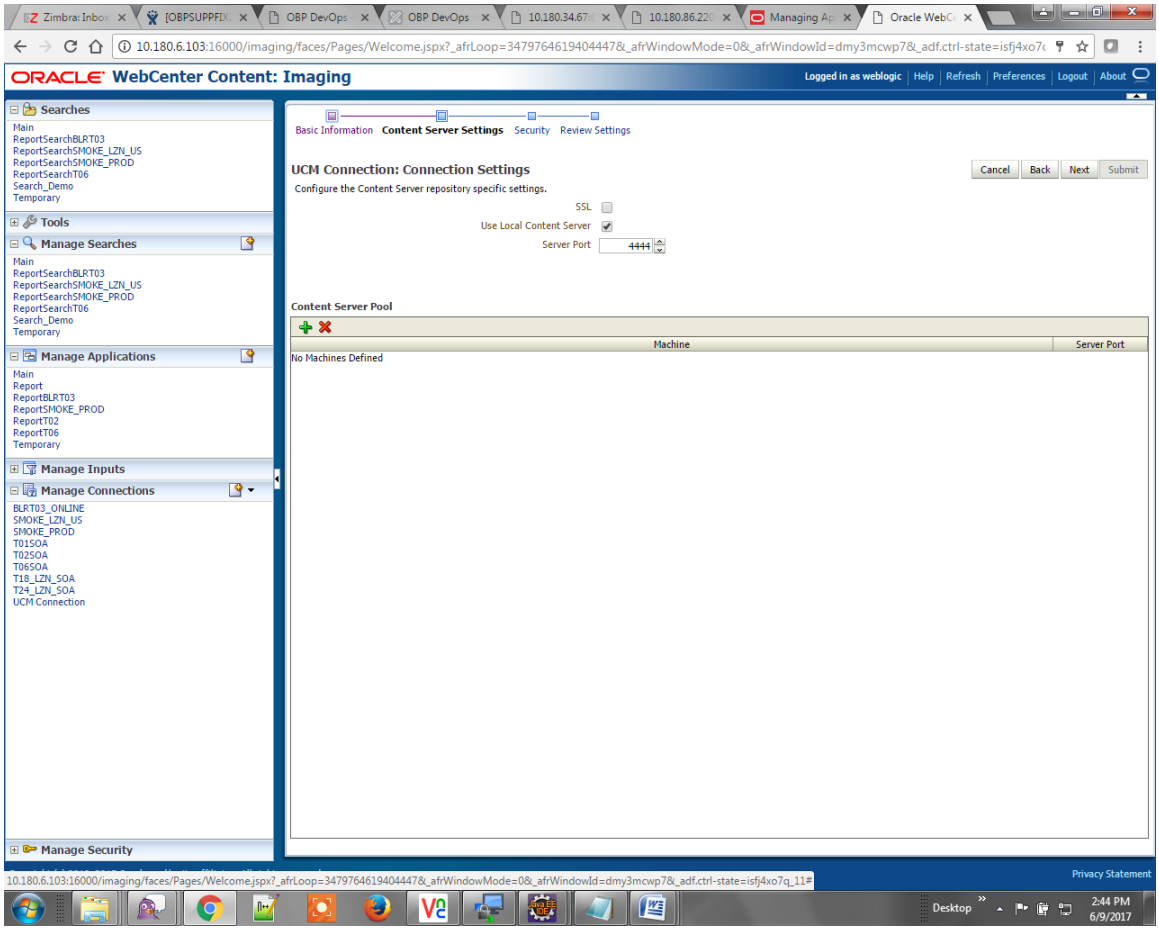
4. In the Basic Information stage, enter the name and description for Content Server Connection as UCM Connection and click Next.

Figure 8–4 UCM: Basic information



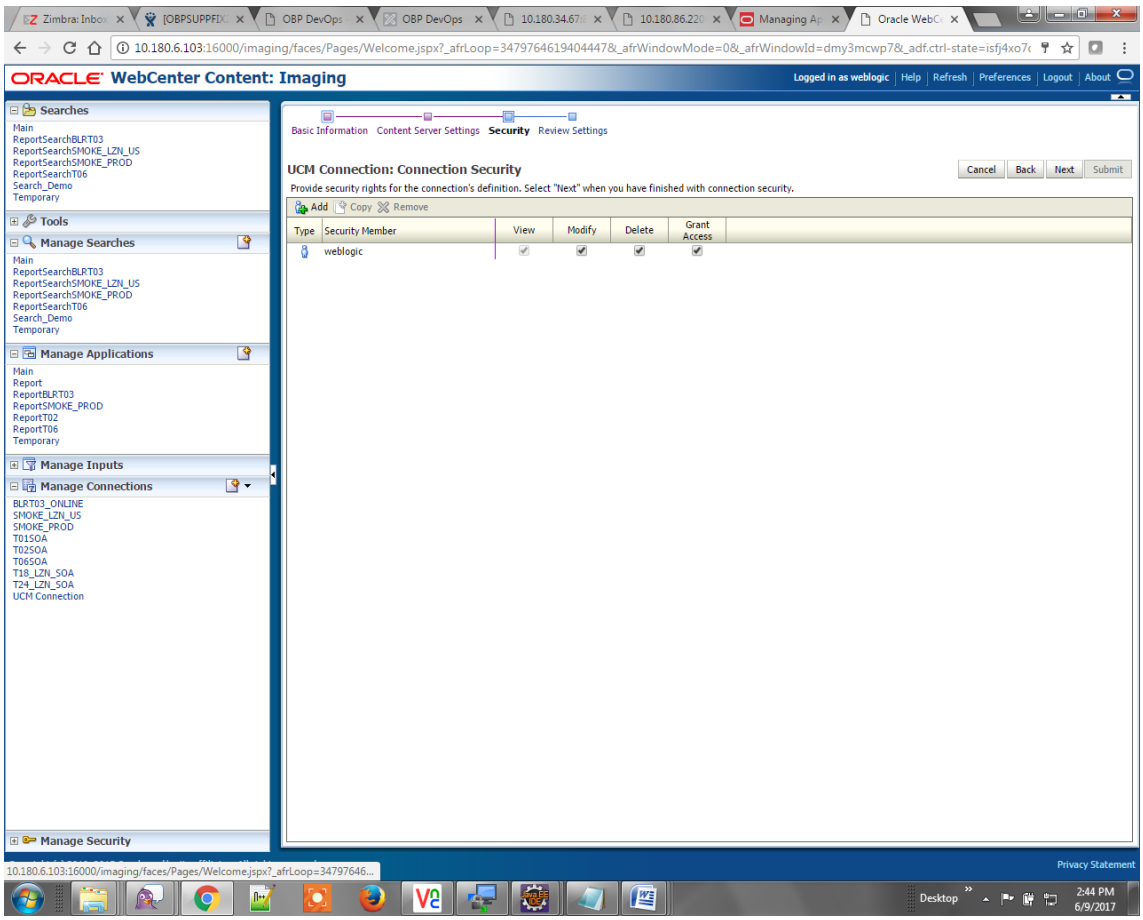
5. In the Content Server Settings page, select the Use Local Content Server check box and select the Server Port as 4444. Click Next.

Figure 8–5 UCM: Connection Settings



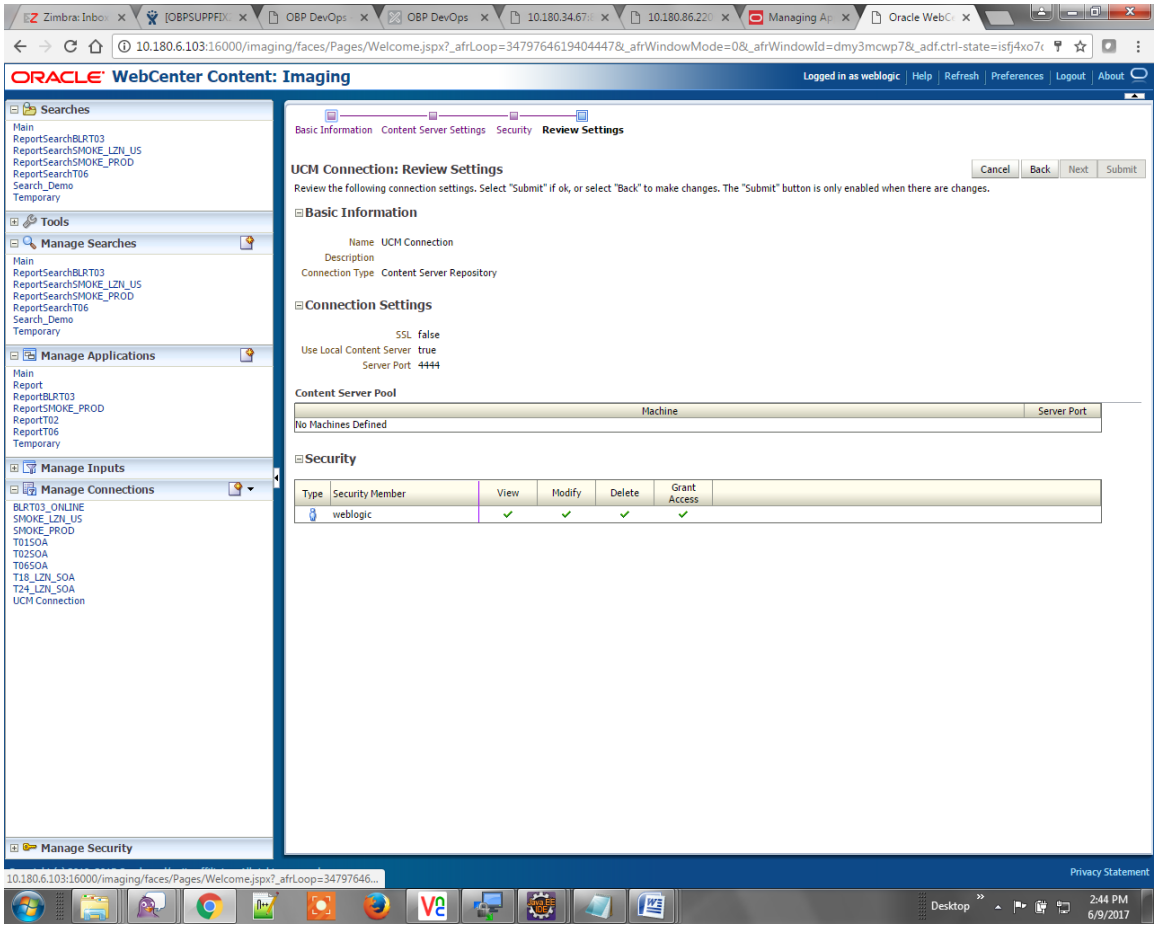
6. In the Security stage, select security rights for connection definition as shown below and click Next. If weblogic security member is not present, create it by clicking Add.

Figure 8–6 UCM: Connection Security



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

Figure 8–7 UCM: Review Settings



8.1.2 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/en/middleware/webcenter/content/12.2.1.4/admin-image/managing-applications.html#GUID-4A1A138D-FFEC-4FBB-A6D3-7F4FA4BDE06A.

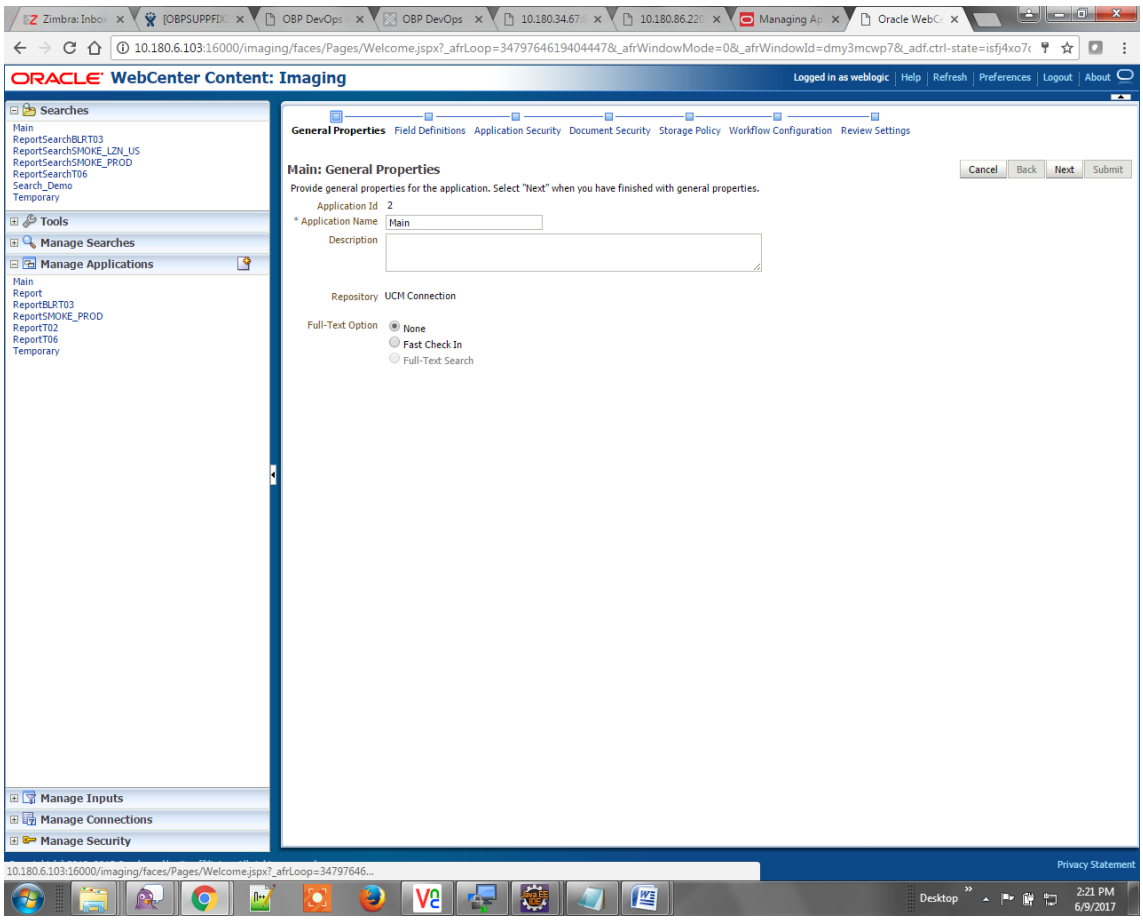
Create a main application and a temporary application in IPM.

8.1.2.1 Manage Application Configuration

To manage application configuration:

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

Figure 8–8 Main: General Properties



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

Figure 8–9 Main: Field Definitions

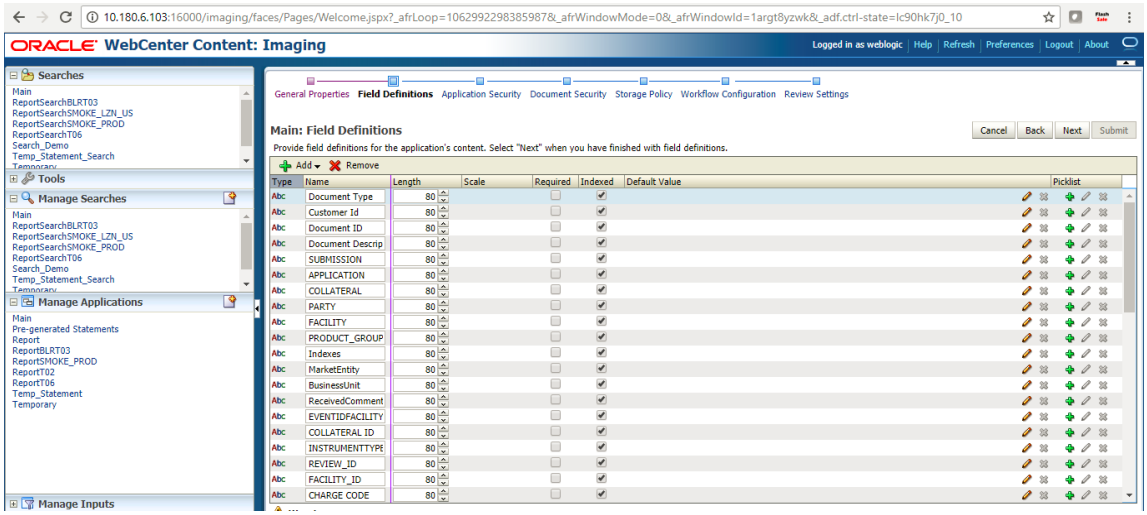
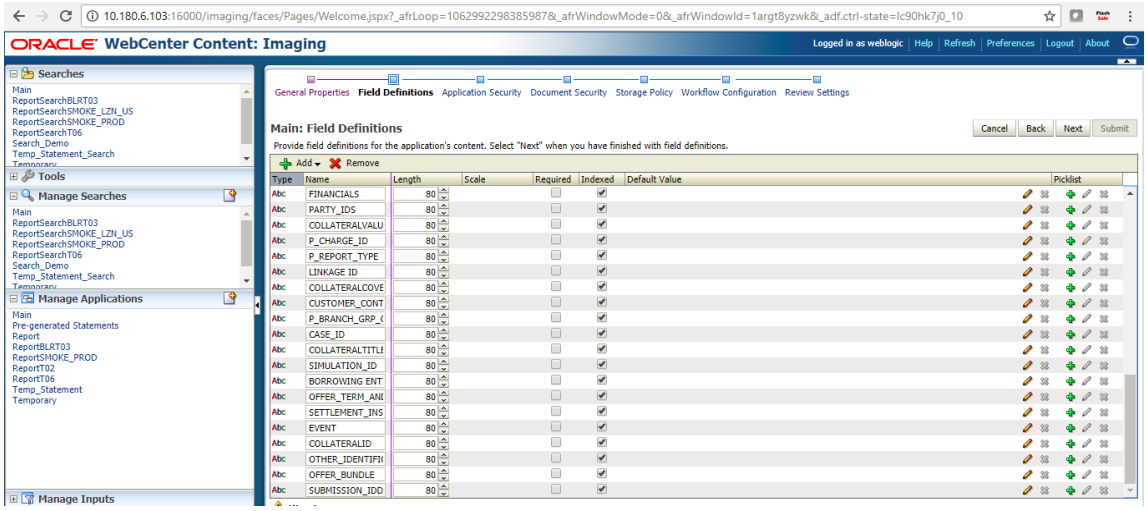


Figure 8–10 Field Definitions (cont.)



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

Figure 8–11 Main: Application Security

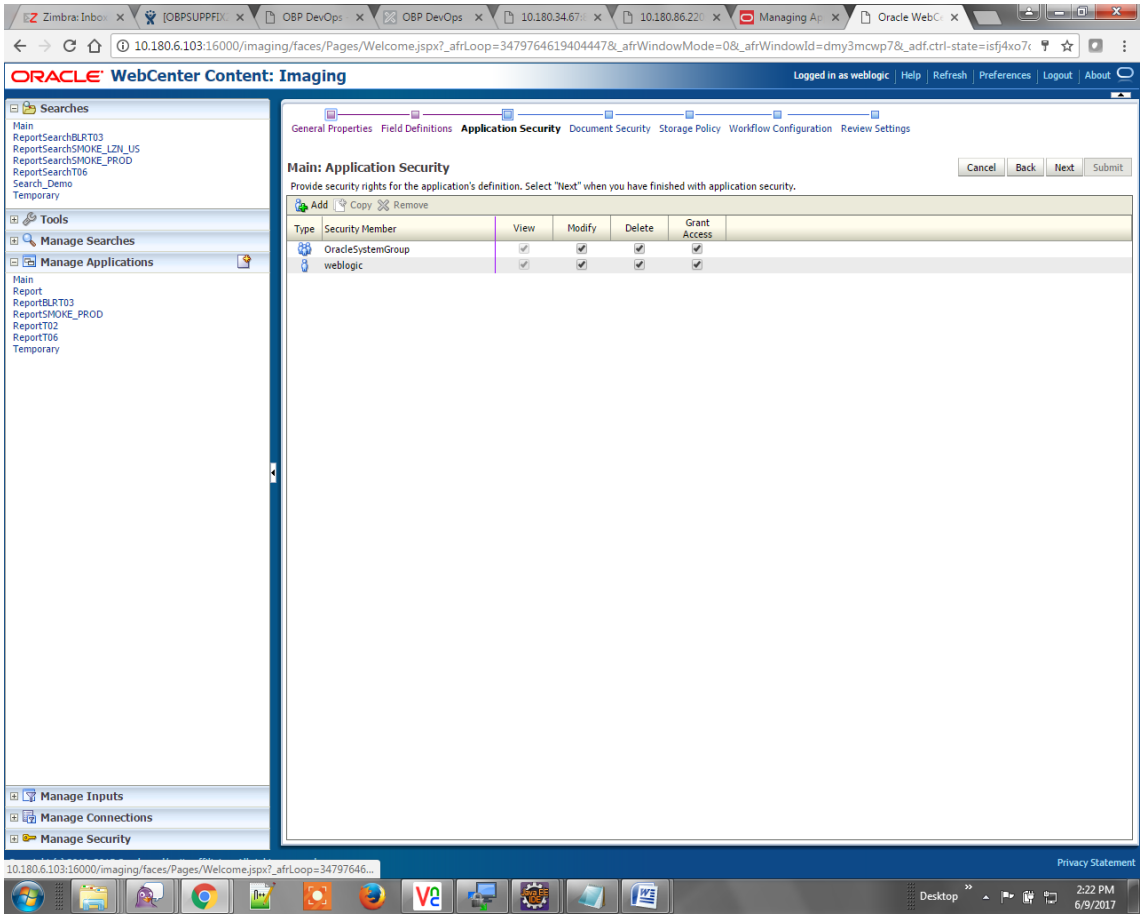
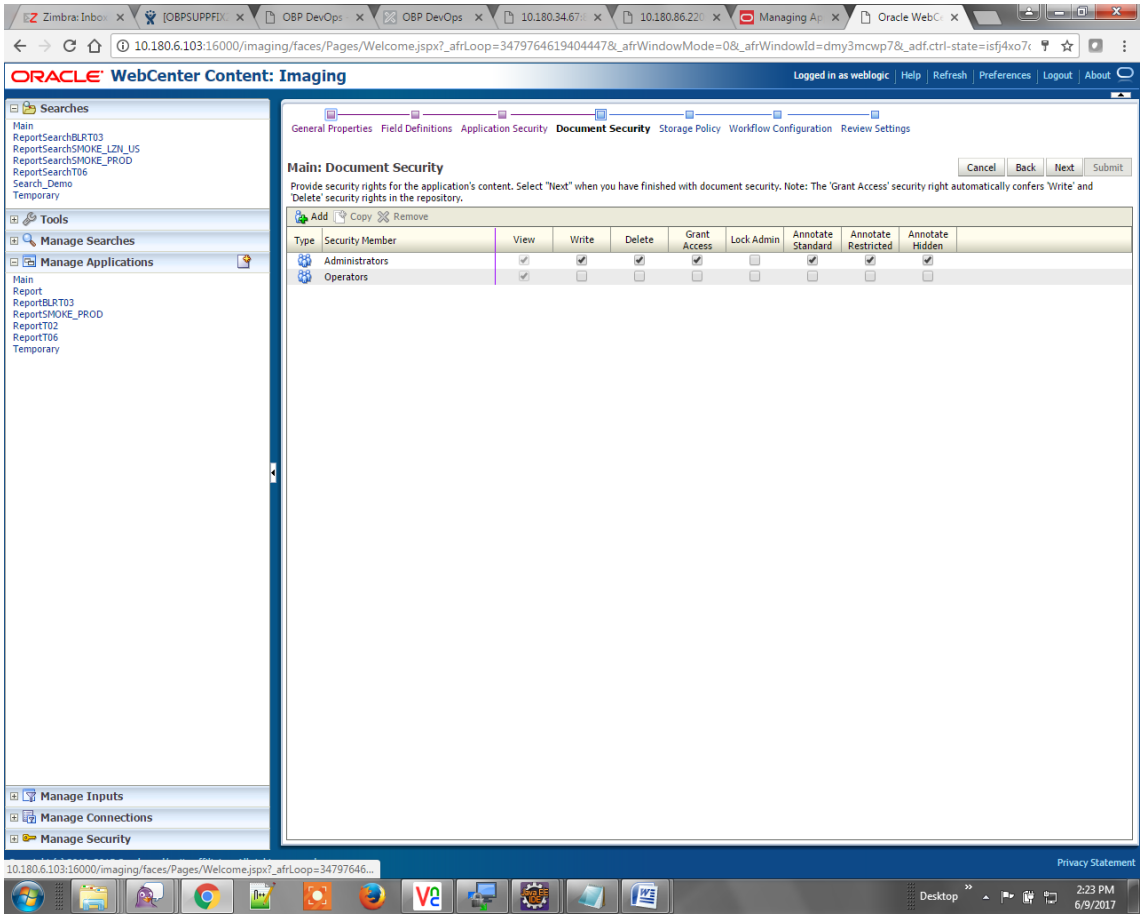
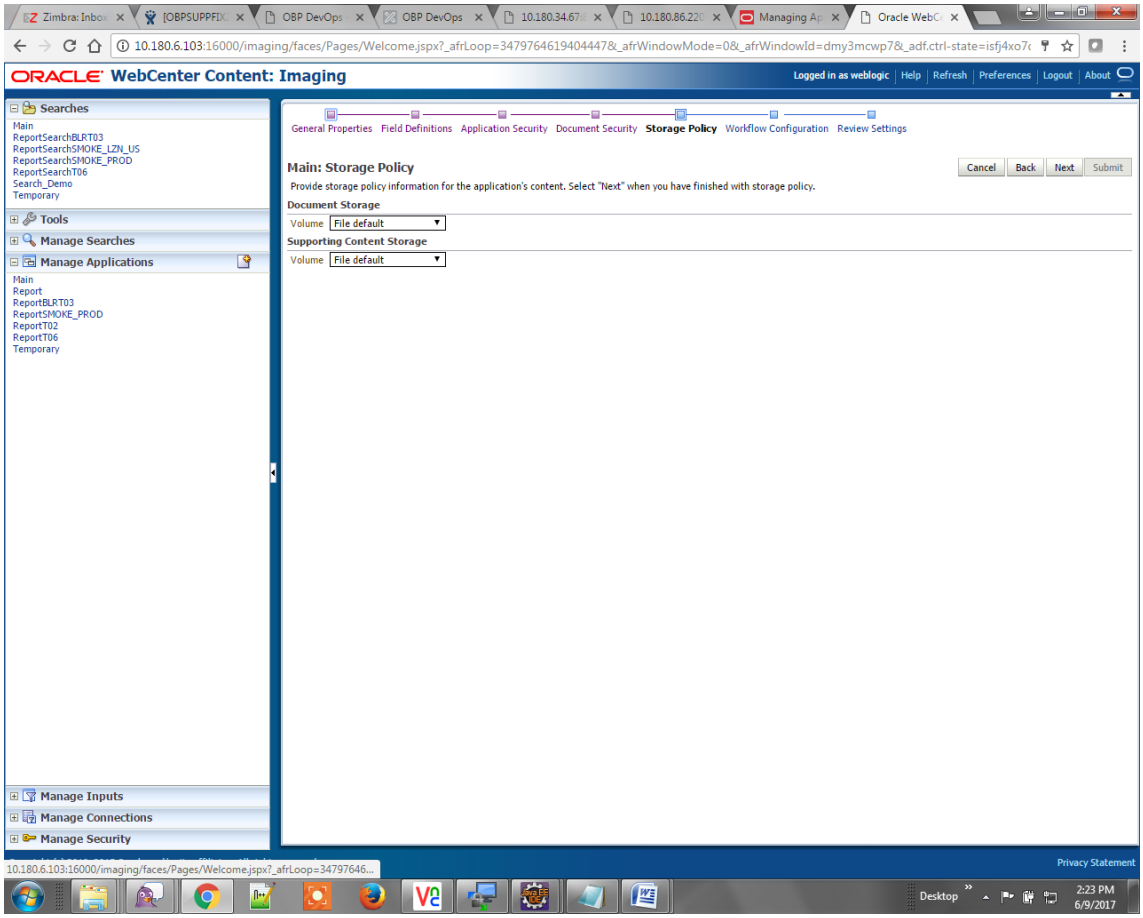


Figure 8–12 Main: Document Security



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

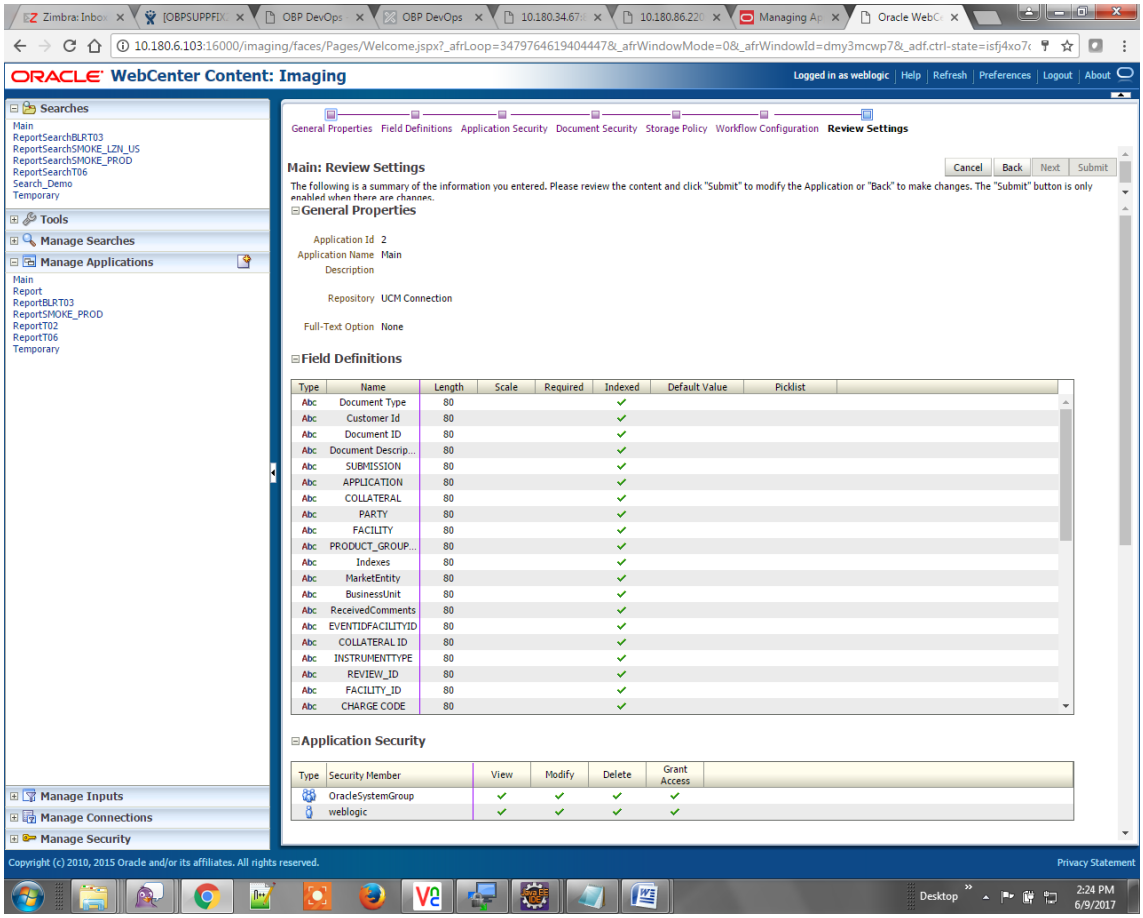
Figure 8–13 Main: Storage Policy



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

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

Figure 8–14 Main: Review Settings

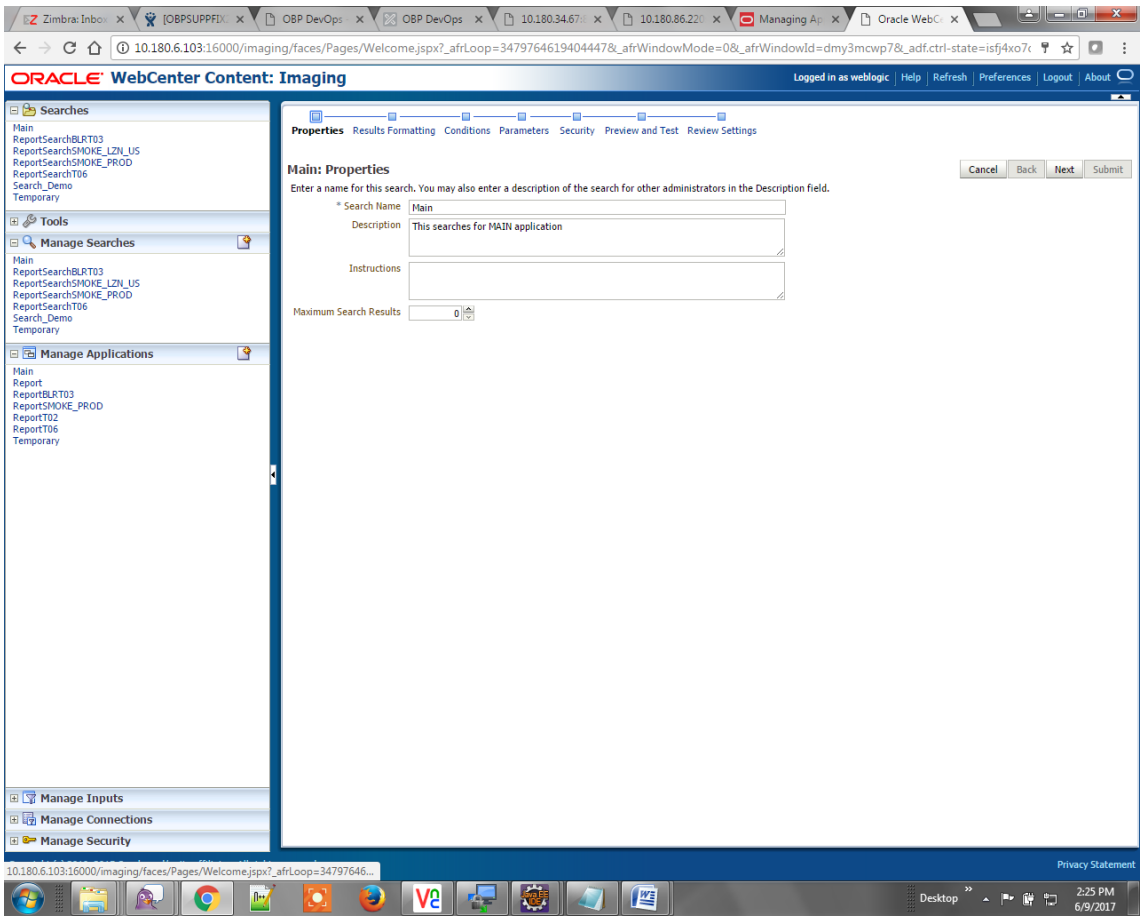


8.1.2.2 Manage Searches

To manage searches:

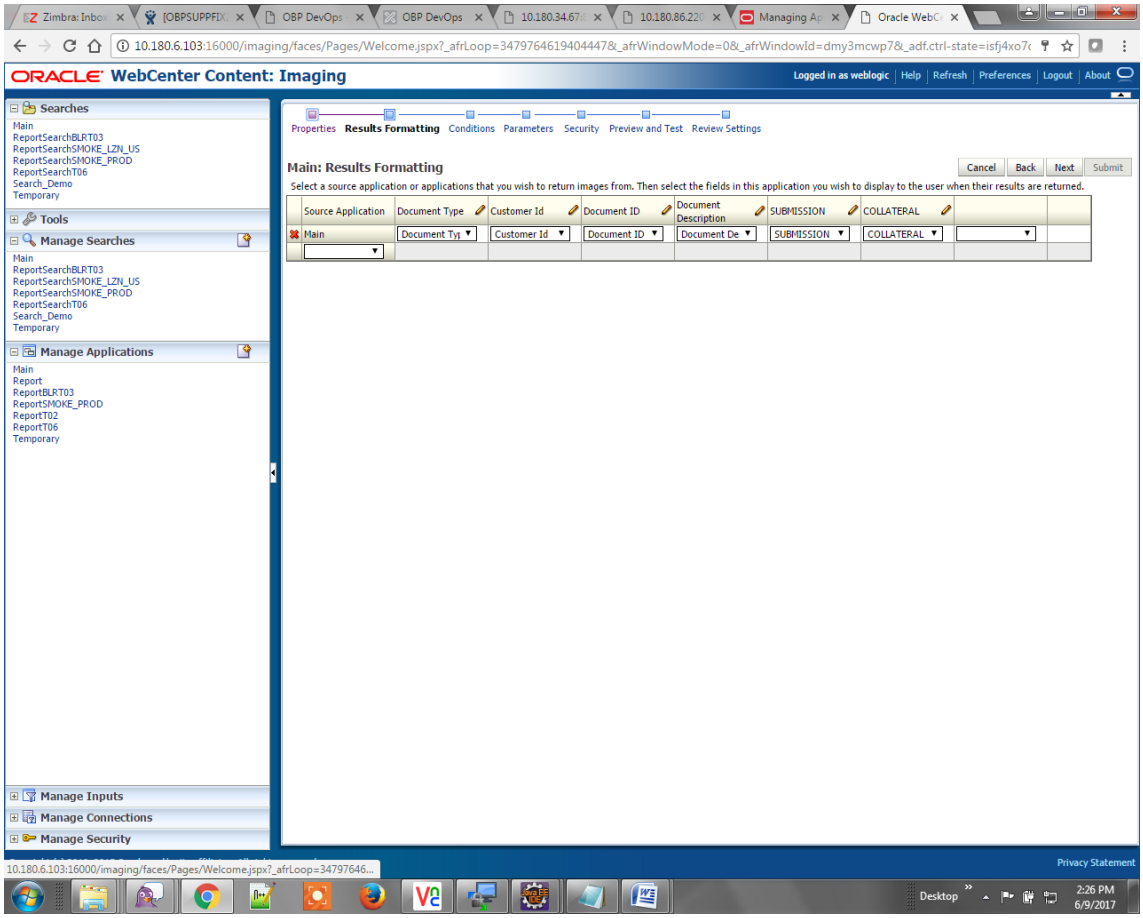
1. Click Manage Searches option and enter the search name with description.

Figure 8–15 Main: Properties



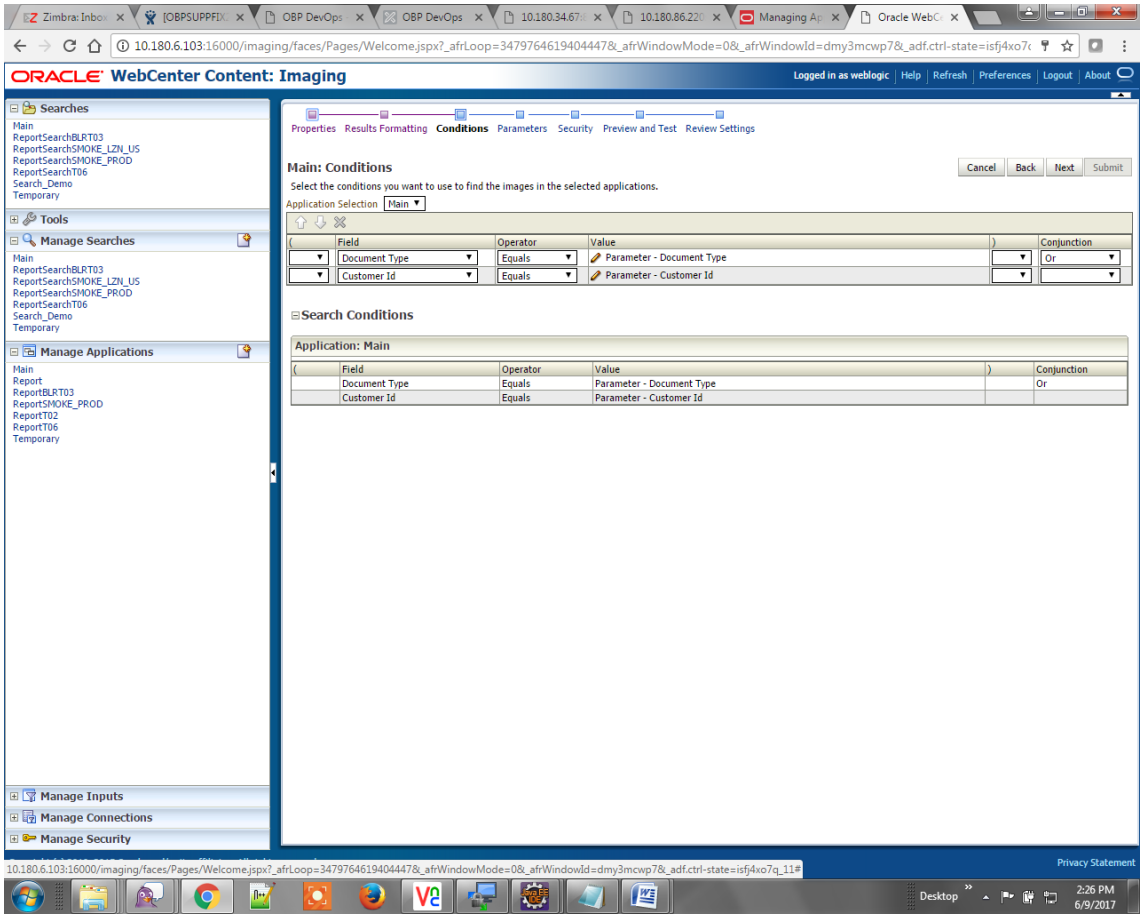
2. Click **Next.**
3. Select the source application along with its field details in the Results Formatting page.

Figure 8–16 Main: Results Formatting



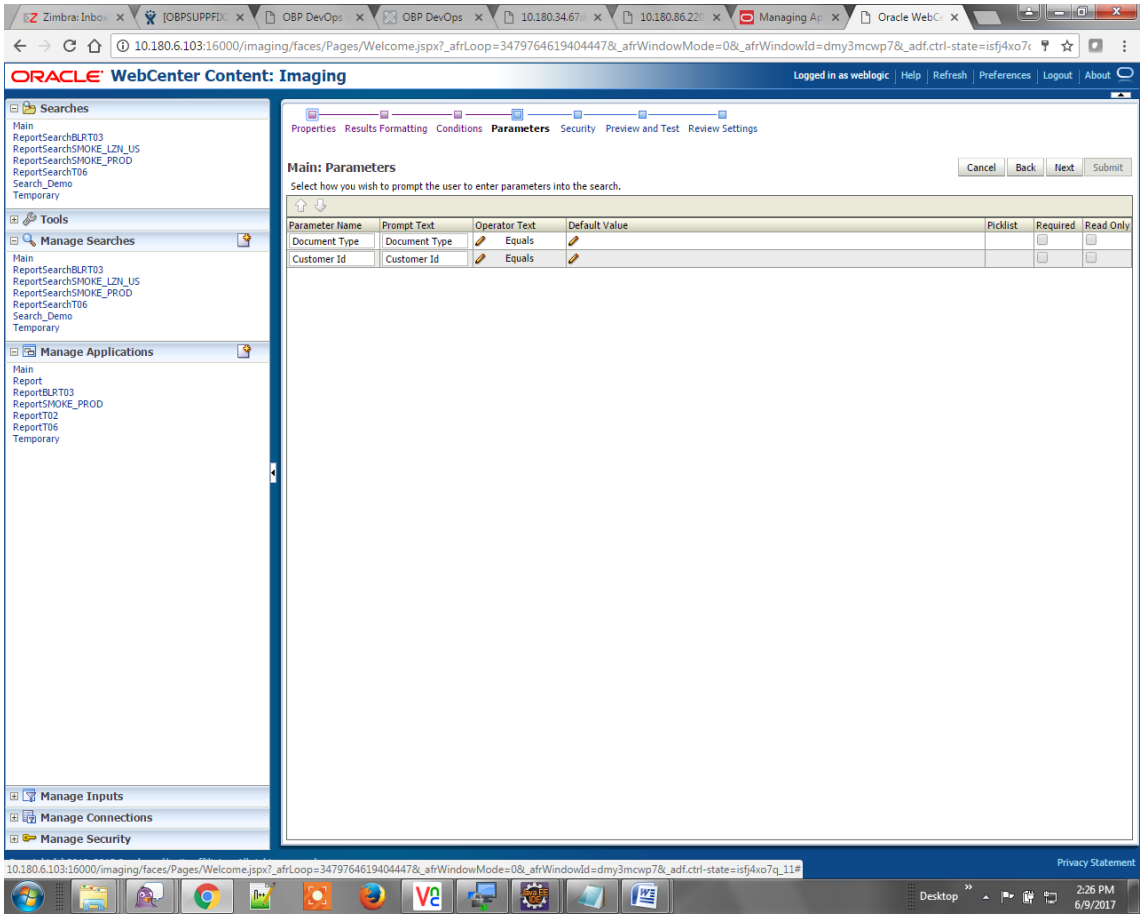
4. Select the appropriate conditions in the Conditions page as shown below.

Figure 8–17 Main: Conditions



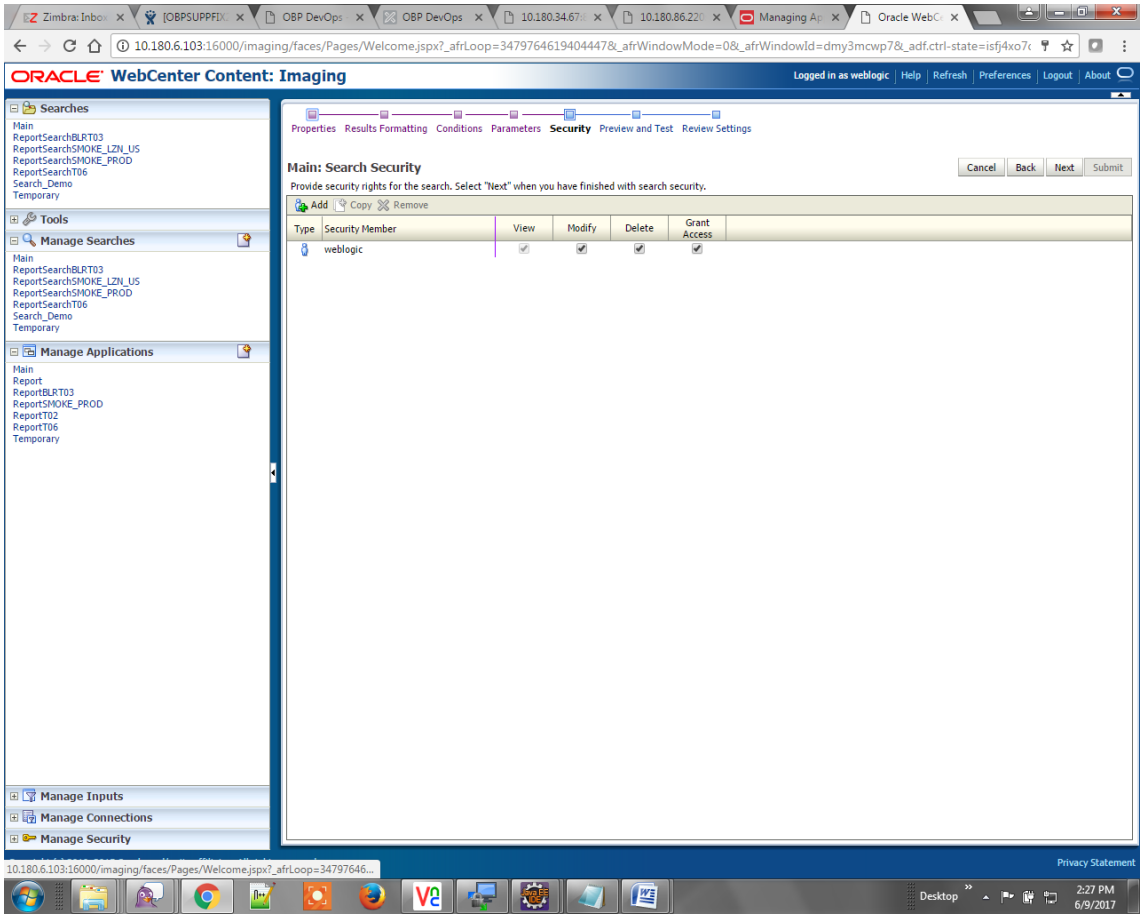
5. Select the appropriate settings in the Parameters page as shown below.

Figure 8–18 Main: Parameters



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

Figure 8–19 Main: Search Security



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

Figure 8–20 Main: Preview and Test

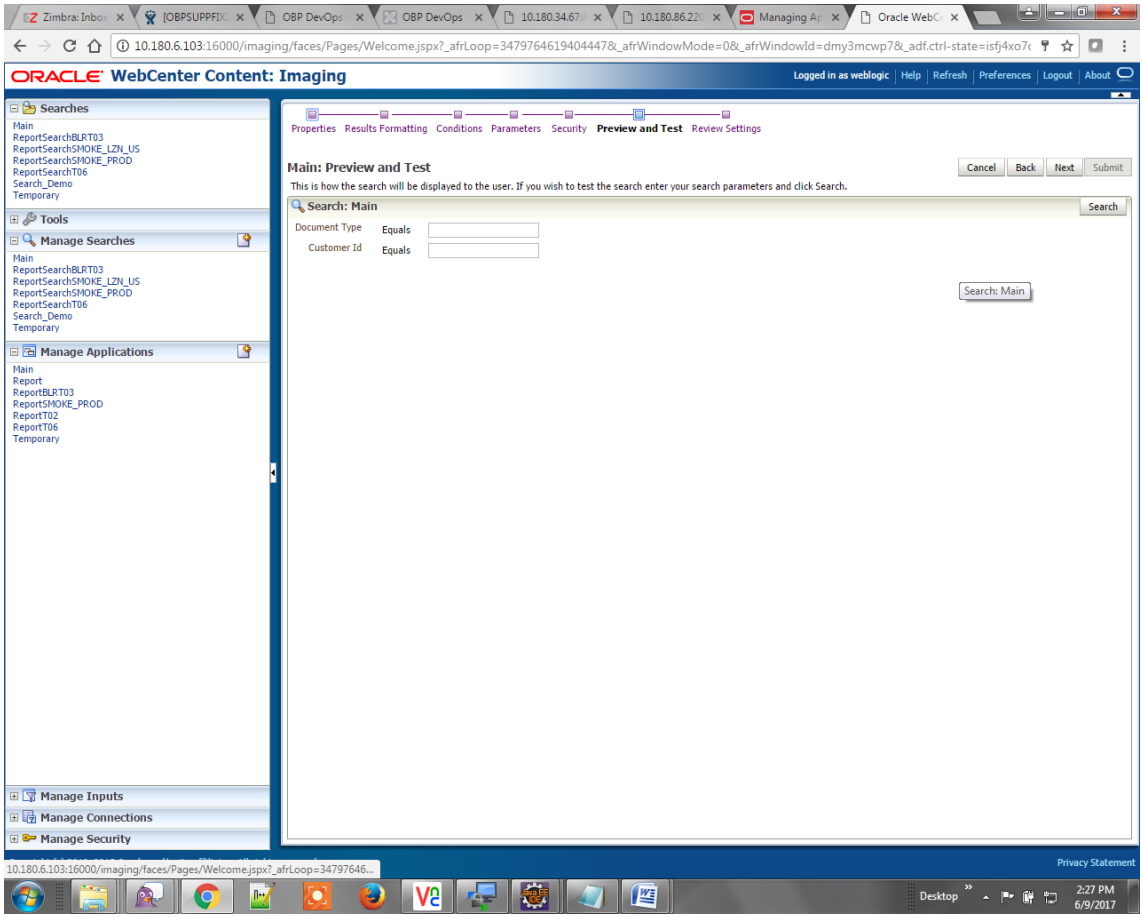
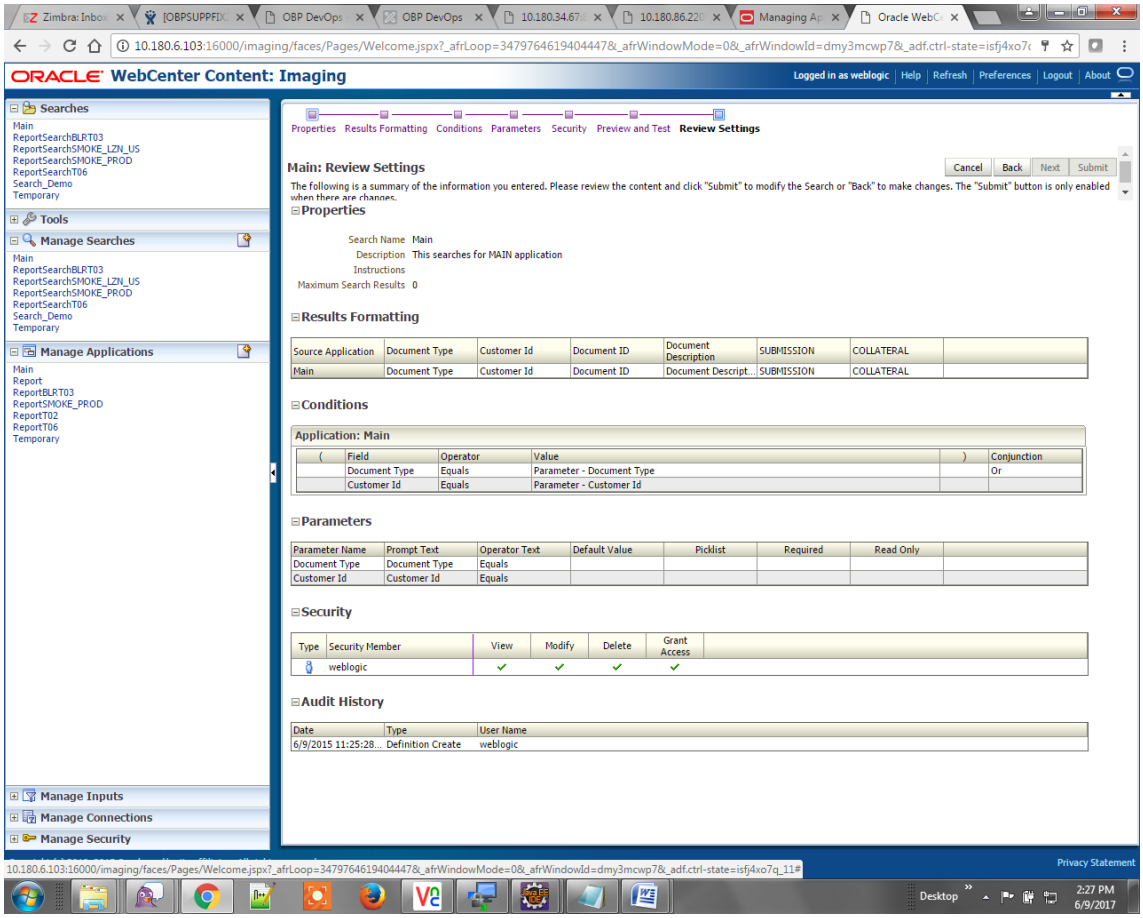


Figure 8–21 Main: Review Settings



8.1.3 Temp Application Configuration

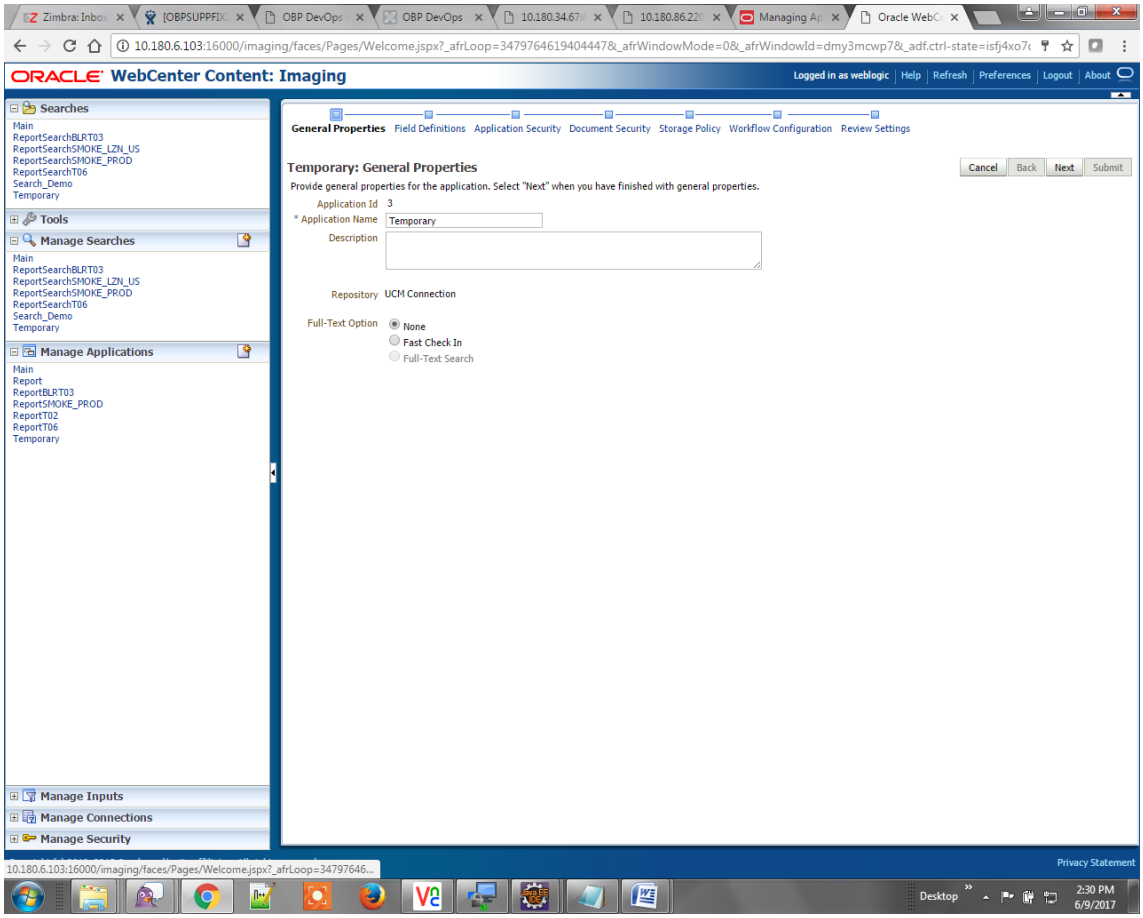
This section provides details about the temp application configuration.

8.1.3.1 Manage Application Configuration

To manage application configuration:

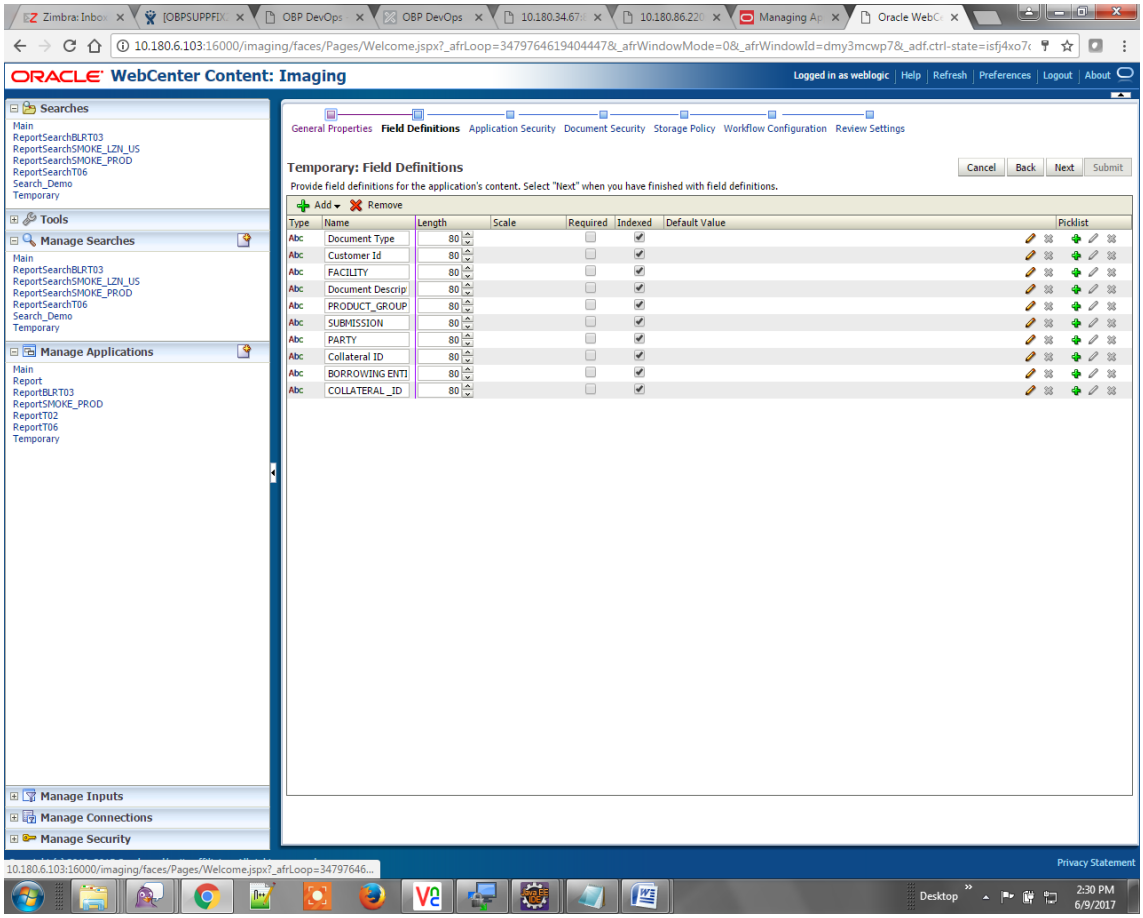
1. Select the Create New Application option.
2. Enter the general properties and click **Next.**

Figure 8–22 Temporary: General Properties



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

Figure 8–23 Temporary: Field Definitions



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

Figure 8–24 Temporary: Application Security

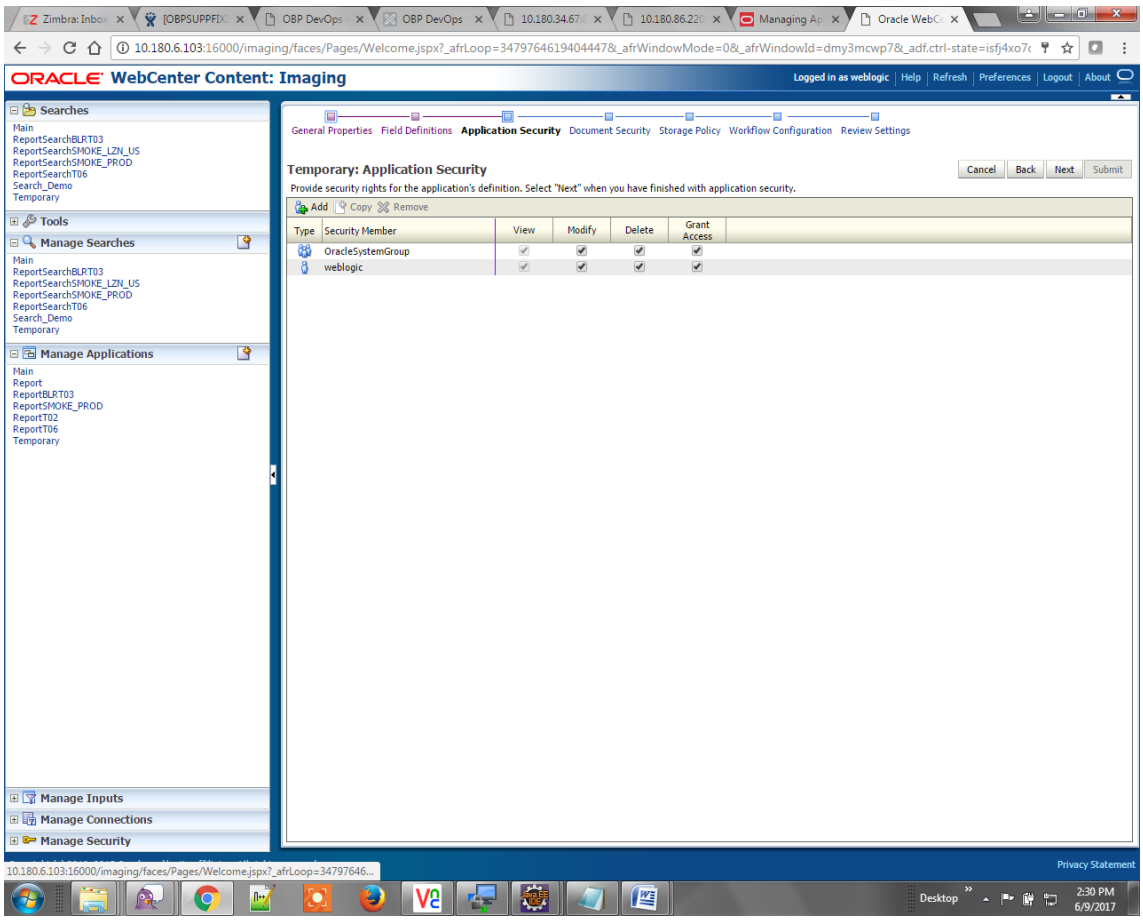
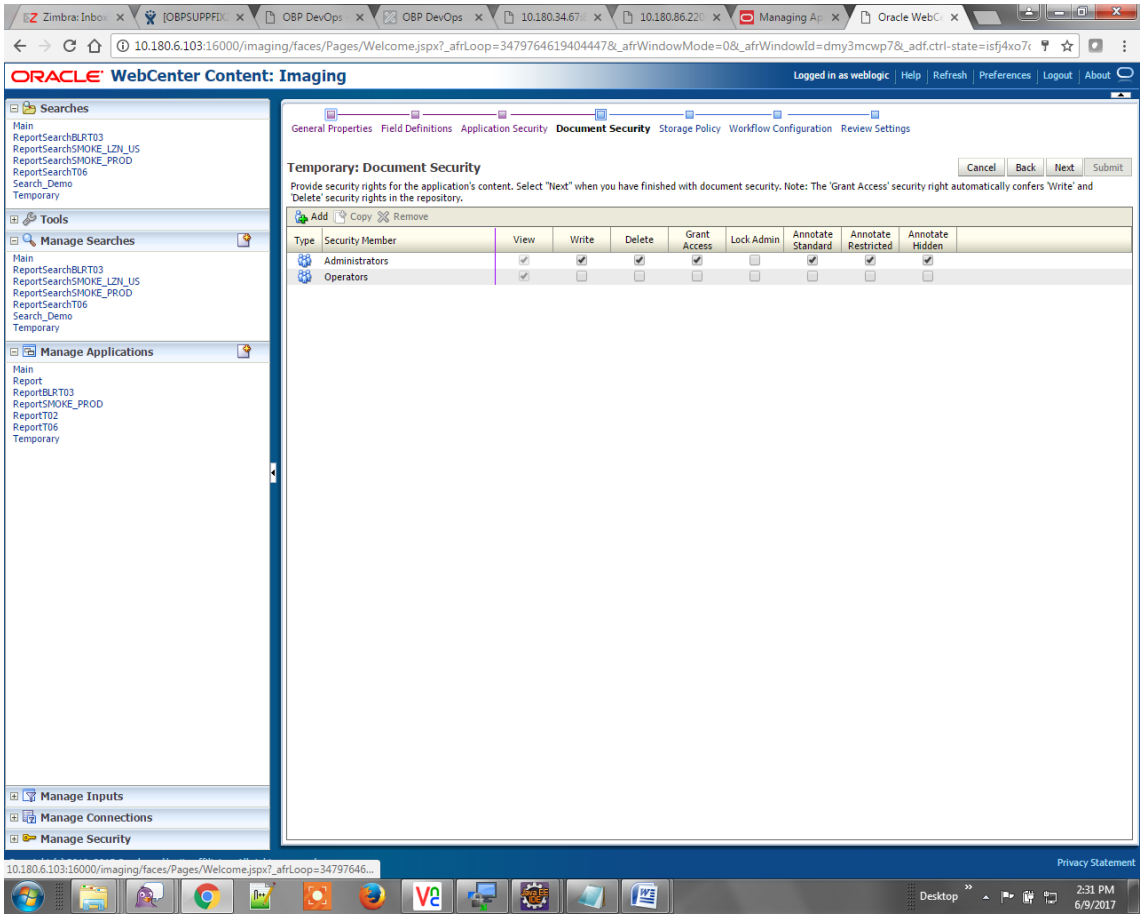
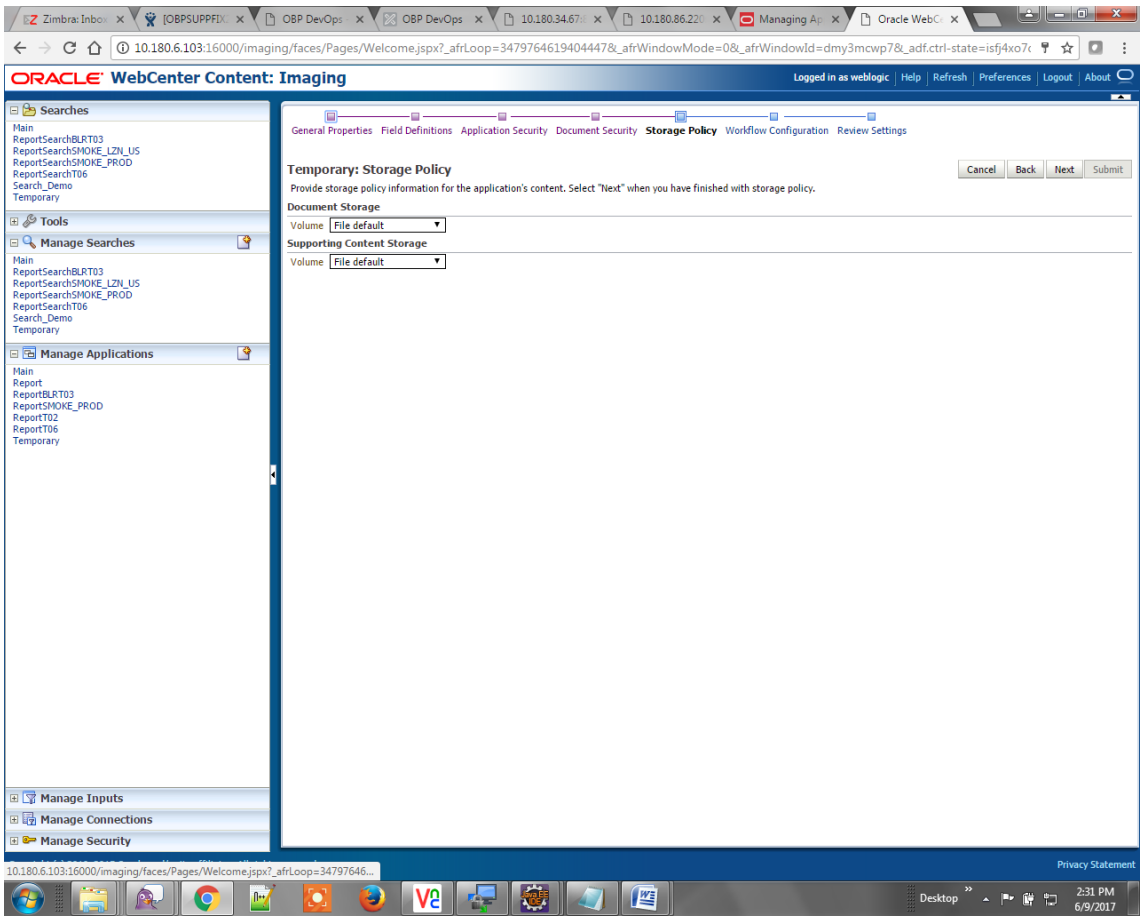


Figure 8–25 Temporary: Document Security



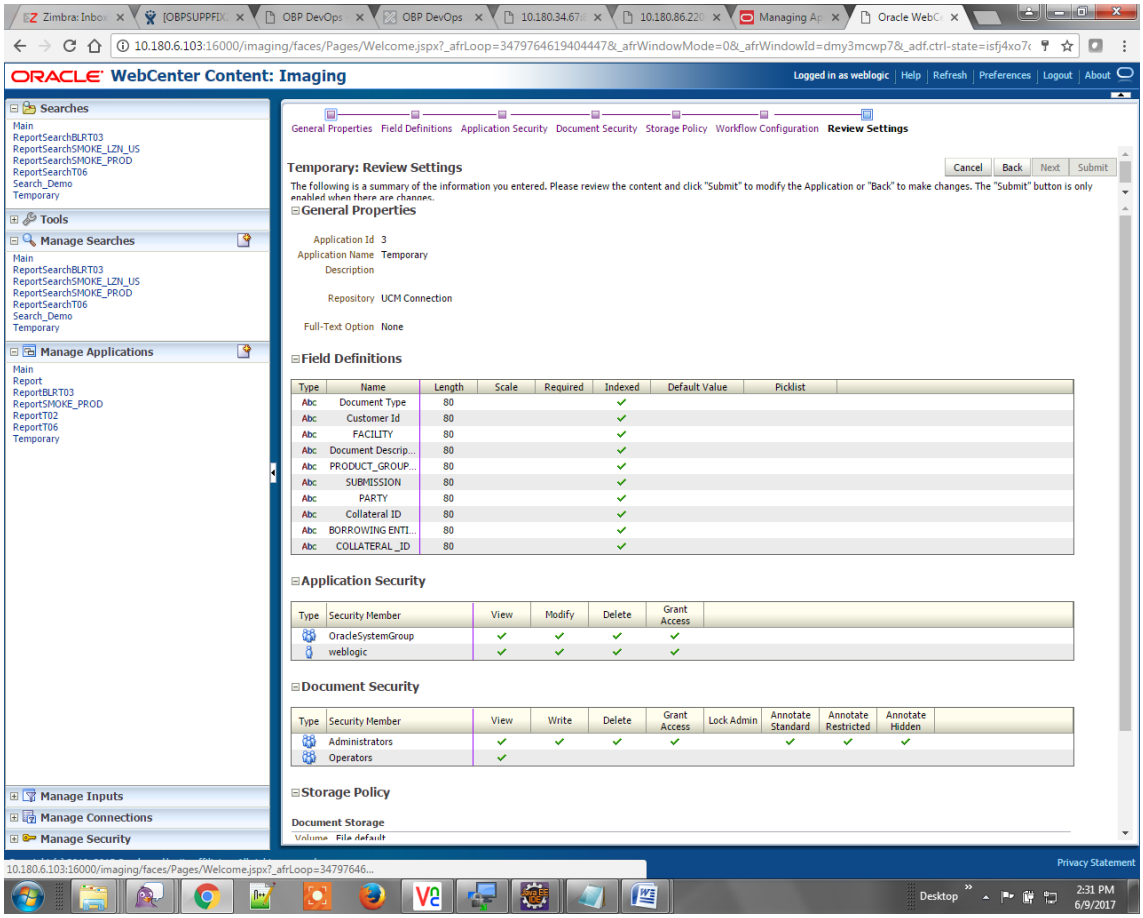
5. In the Storage Policy page, select the file default option has shown below.

Figure 8–26 Temporary: Storage Policy



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

Figure 8–27 Temporary: Review Settings

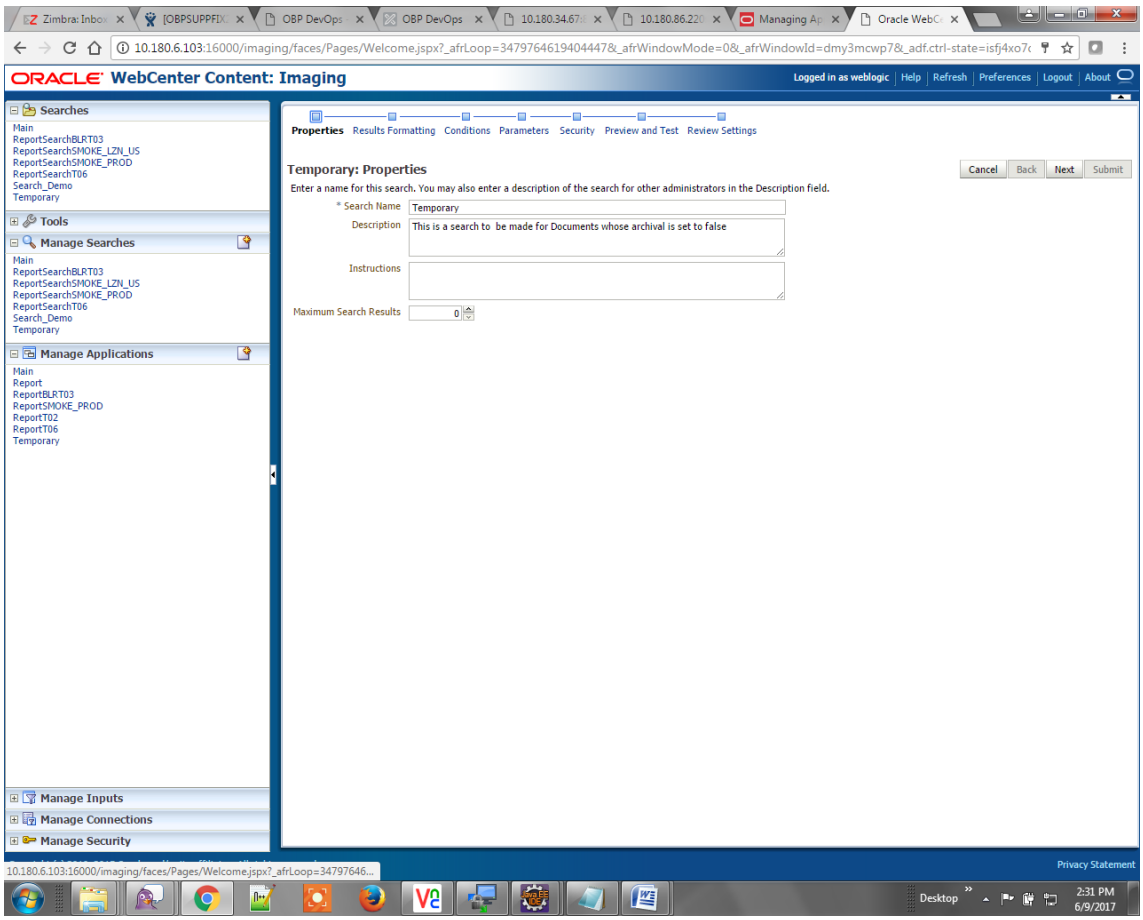


8.1.3.2 Manage Searches

To manage searches:

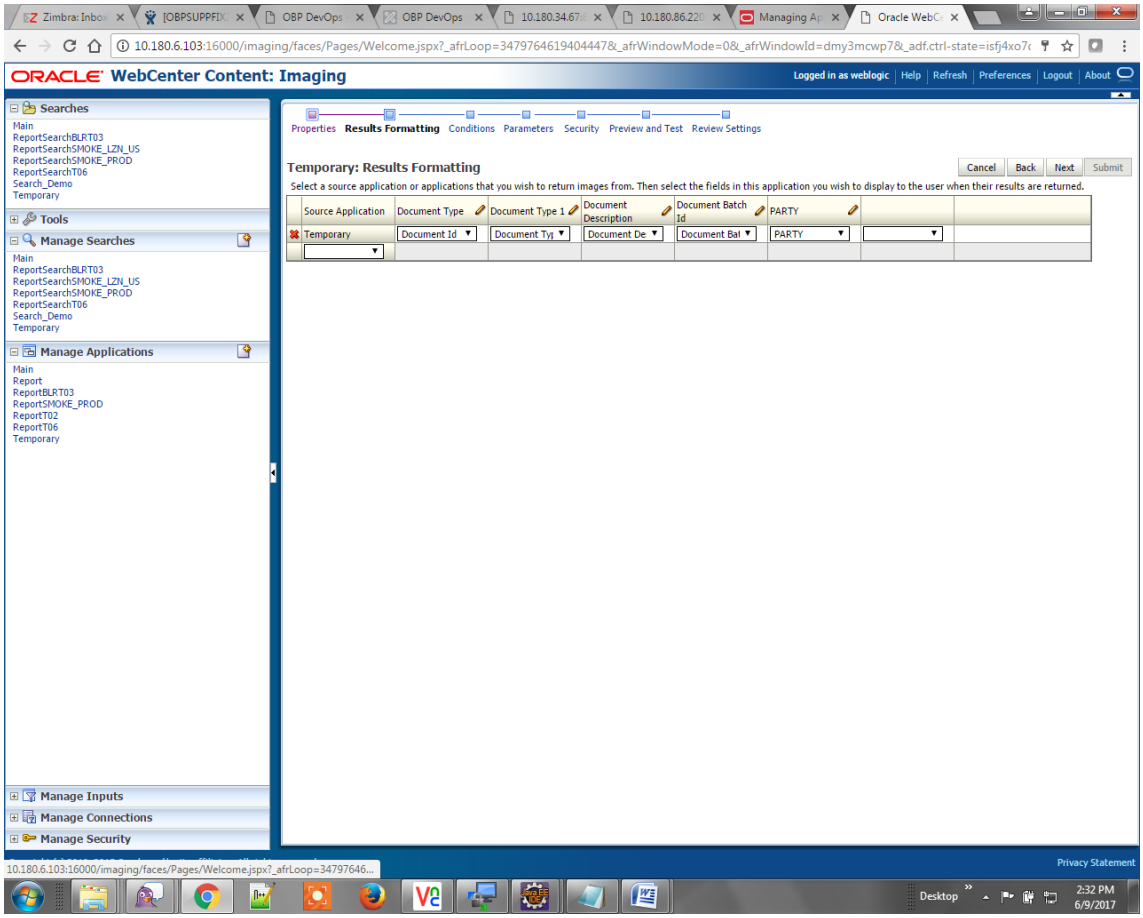
1. Click the Manage Searches option and enter the search name with description.

Figure 8–28 Temporary: Properties



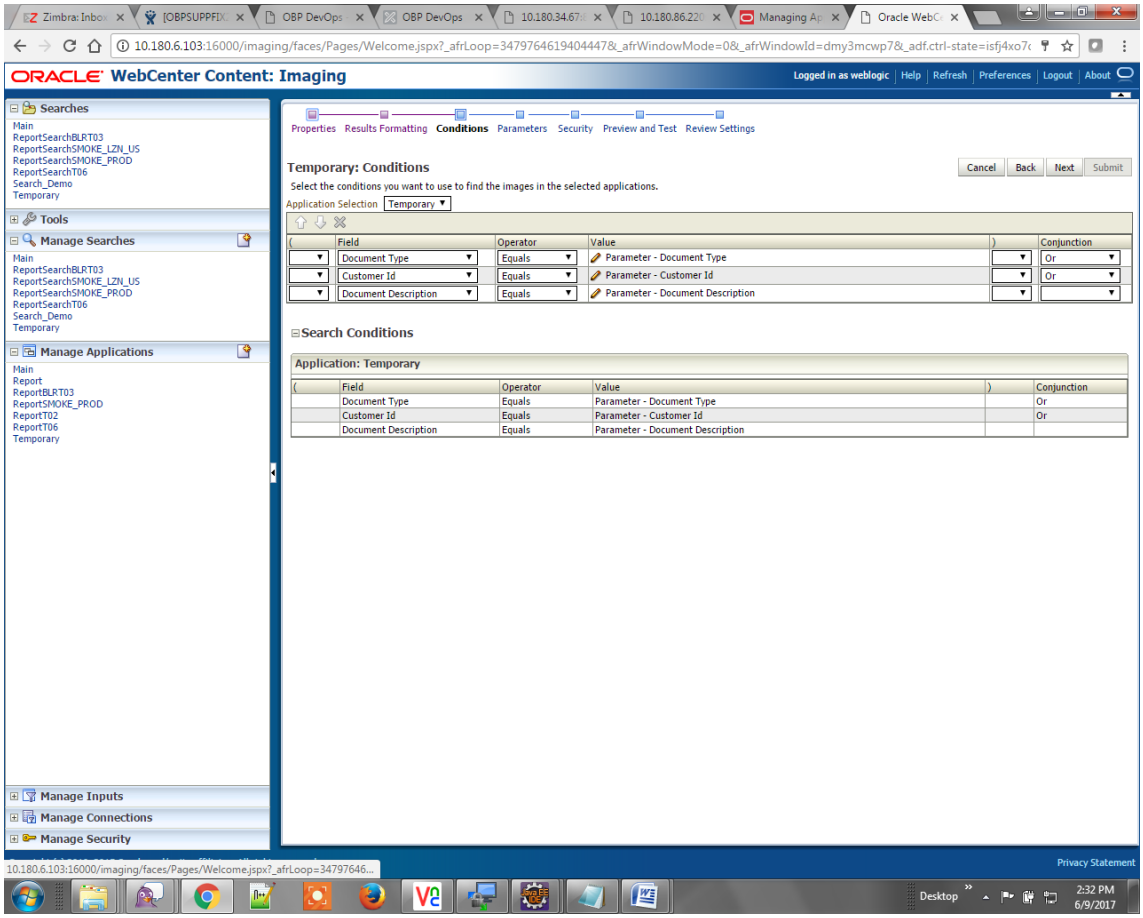
2. Select the source application along with its field details in the Results Formatting page.

Figure 8–29 Temporary: Results Formatting



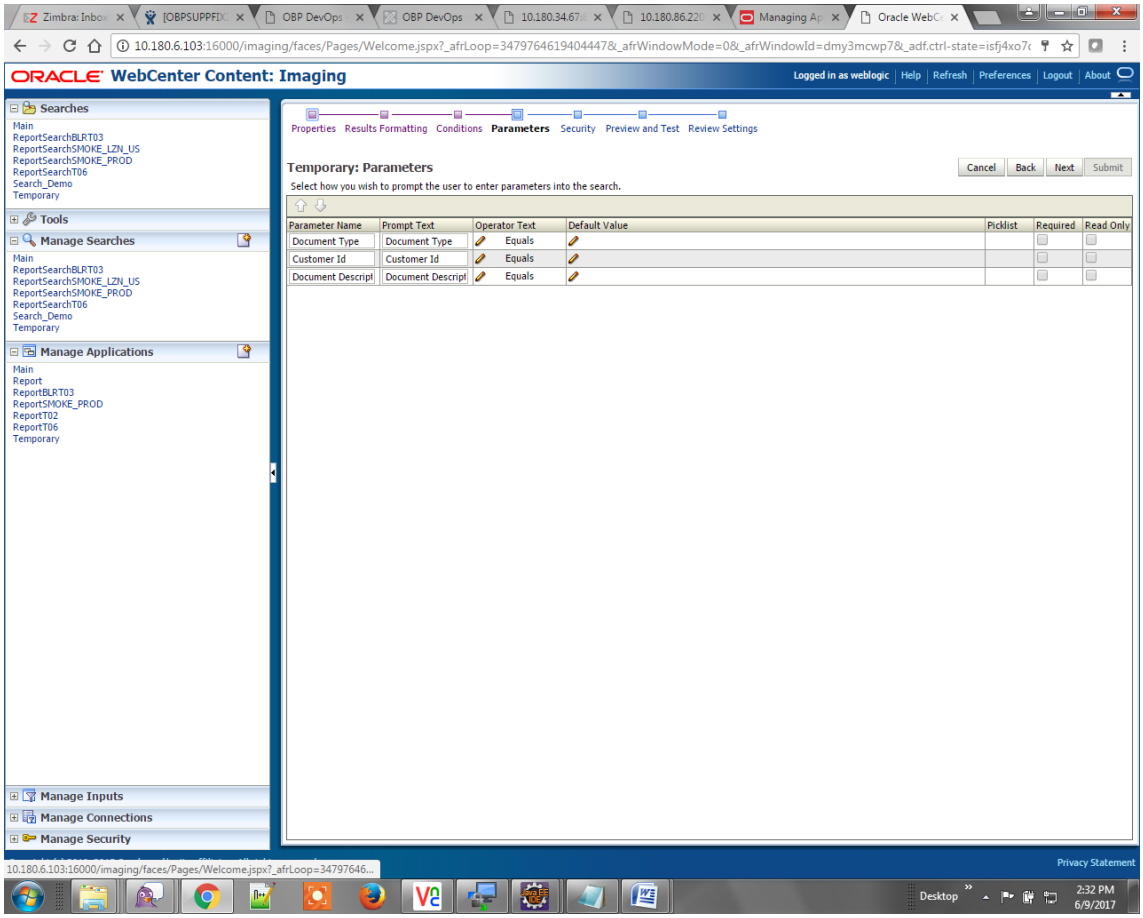
3. Select the appropriate conditions in the Conditions page as shown below.

Figure 8–30 Temporary: Conditions



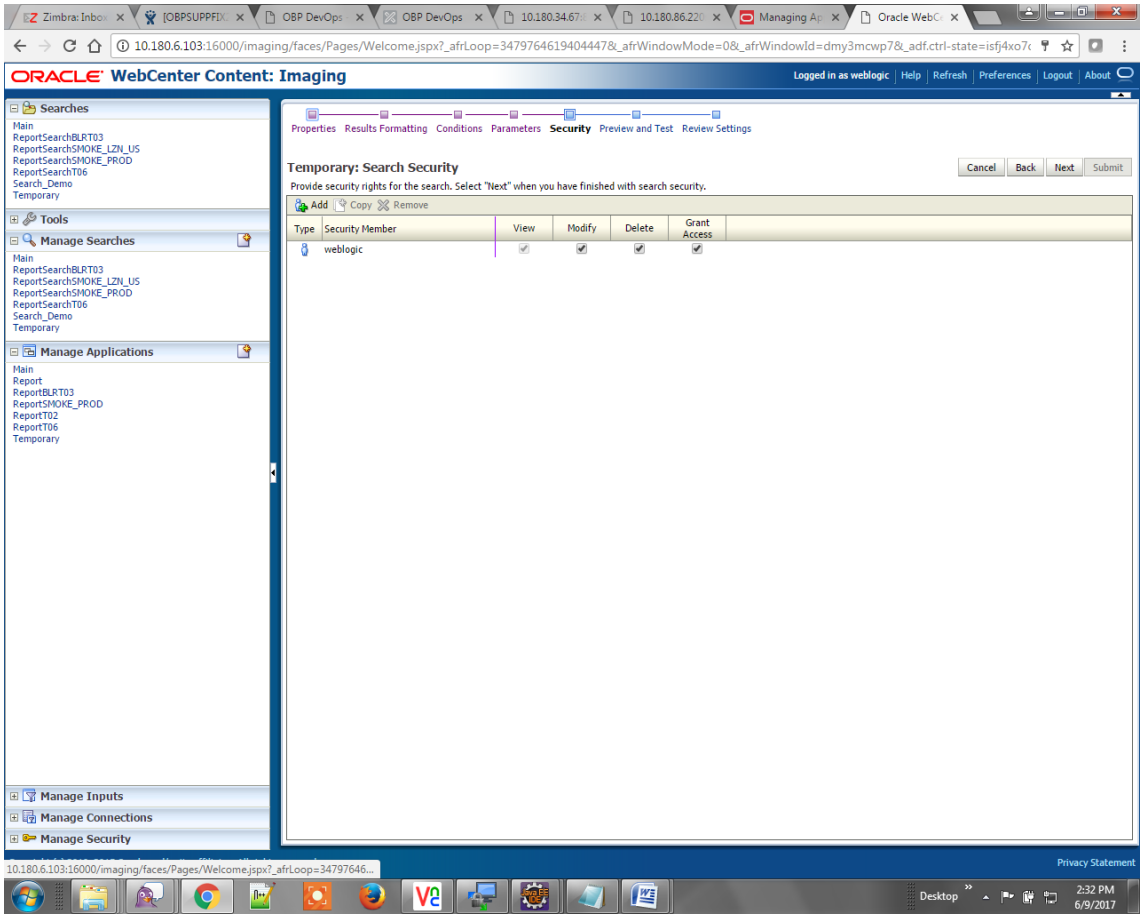
4. Select the appropriate settings in the Parameters page as shown below.

Figure 8–31 Temporary: Parameters



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

Figure 8–32 Temporary: Search Security



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

Figure 8–33 Temporary: Preview and Test

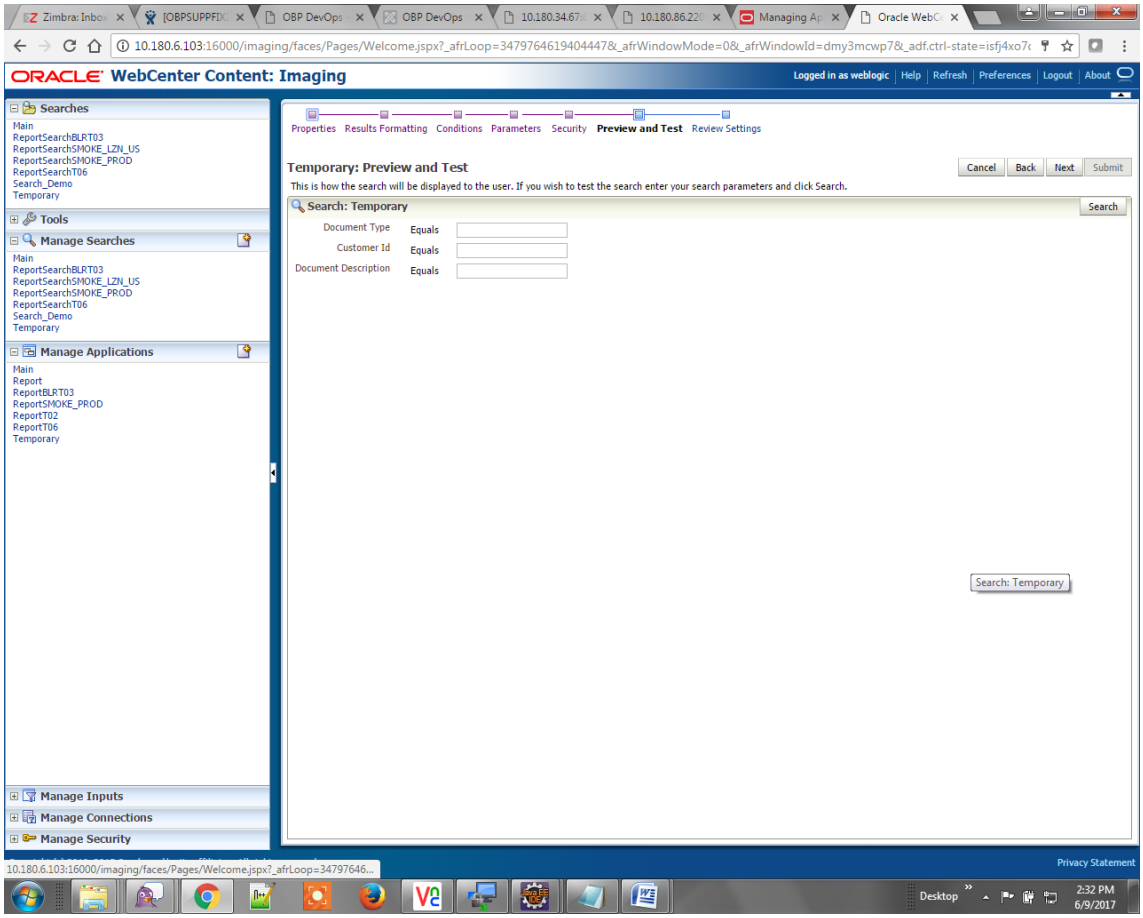
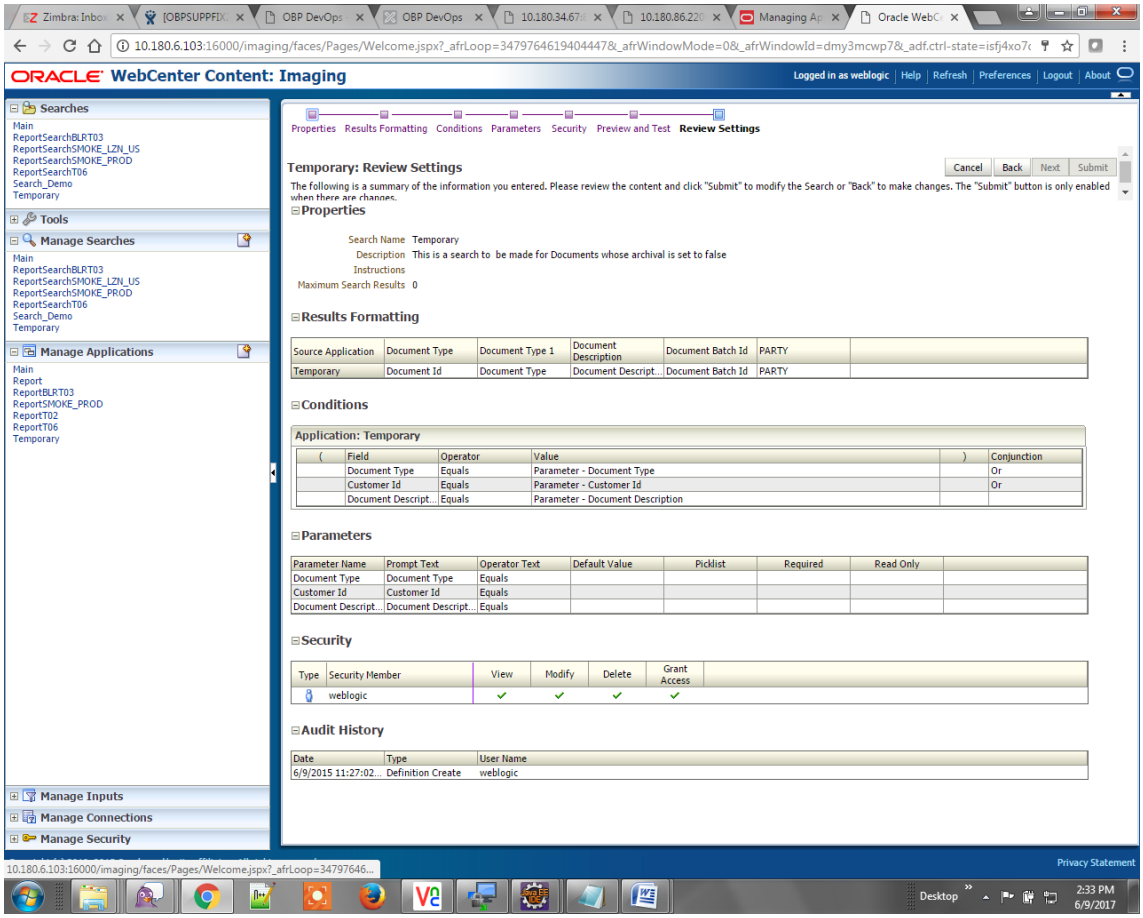


Figure 8–34 Temporary: Review Settings



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

8.2 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 OBEO for the document record.

8.2.1 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.

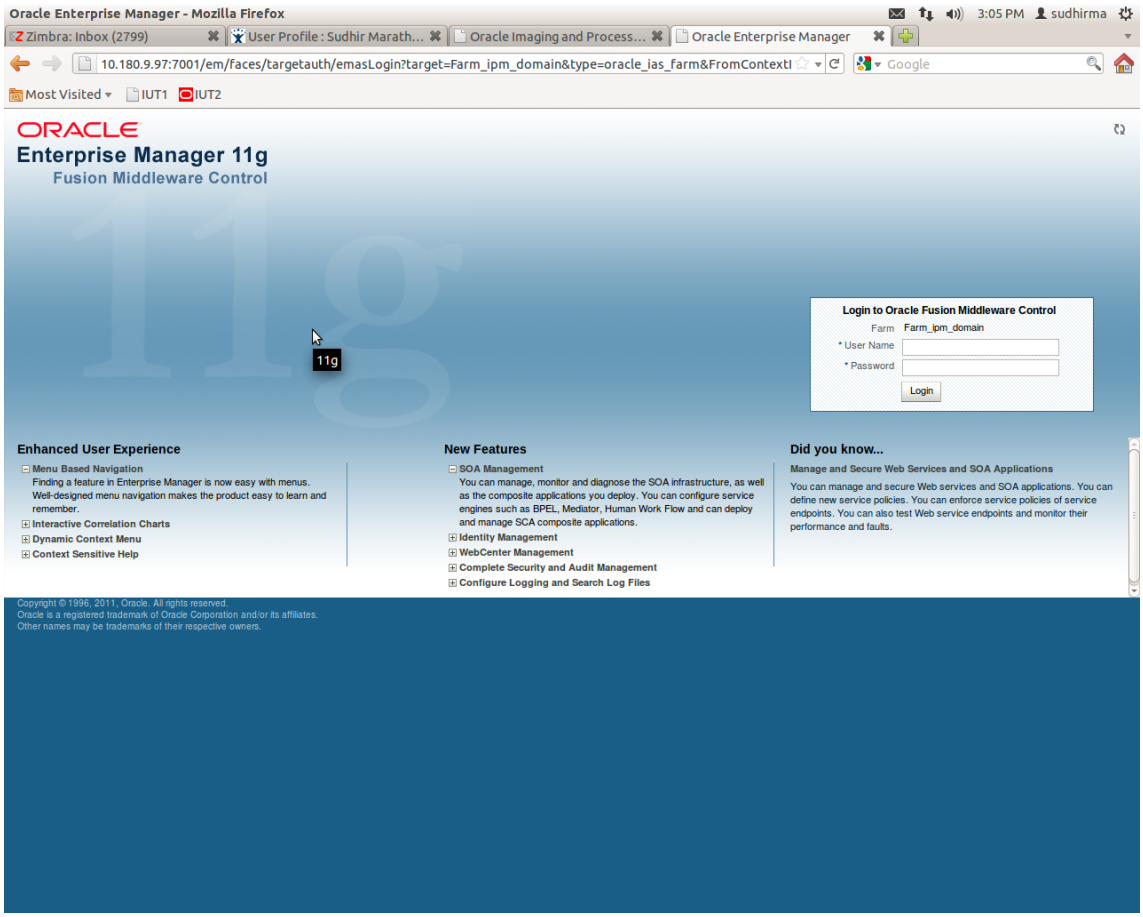
8.2.2 Setting up the Connection Name

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:

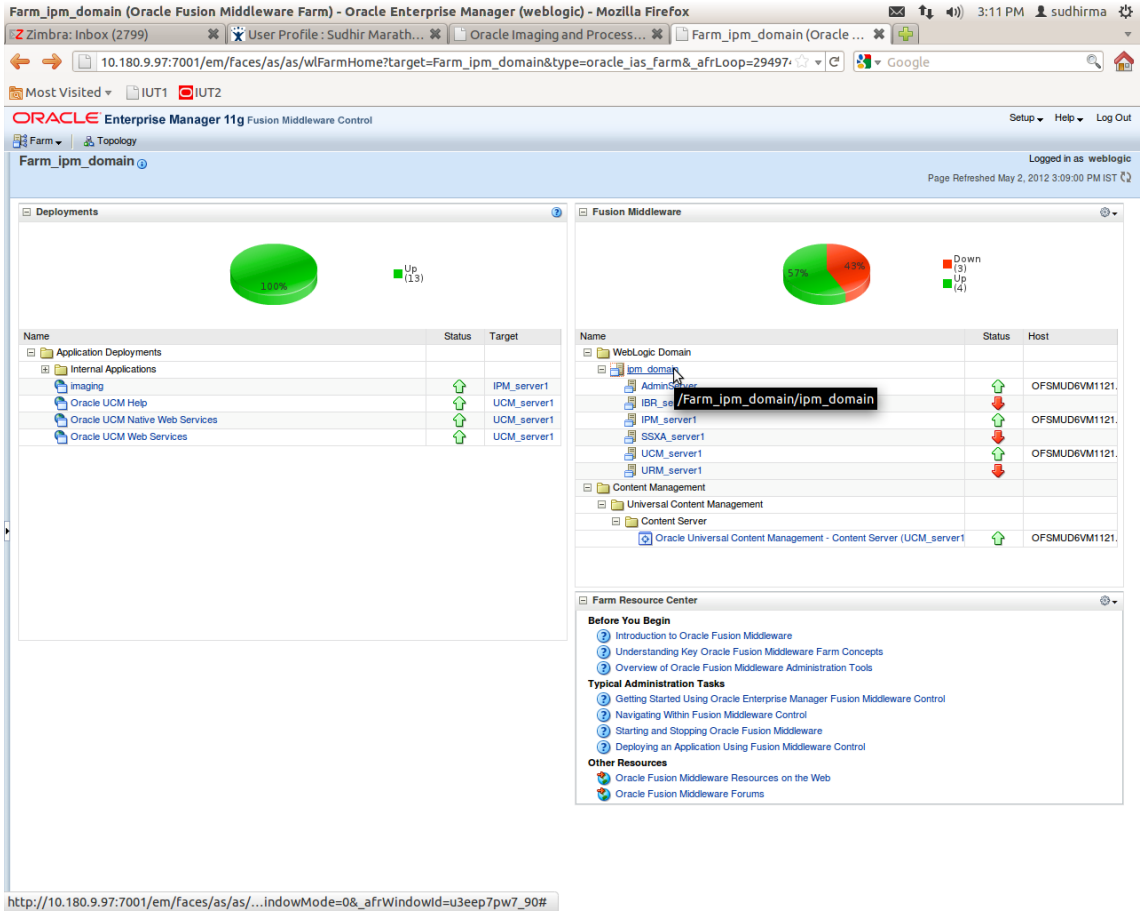
1. Log in to Enterprise Manager (EM) console.

Figure 8–35 EM Console Login



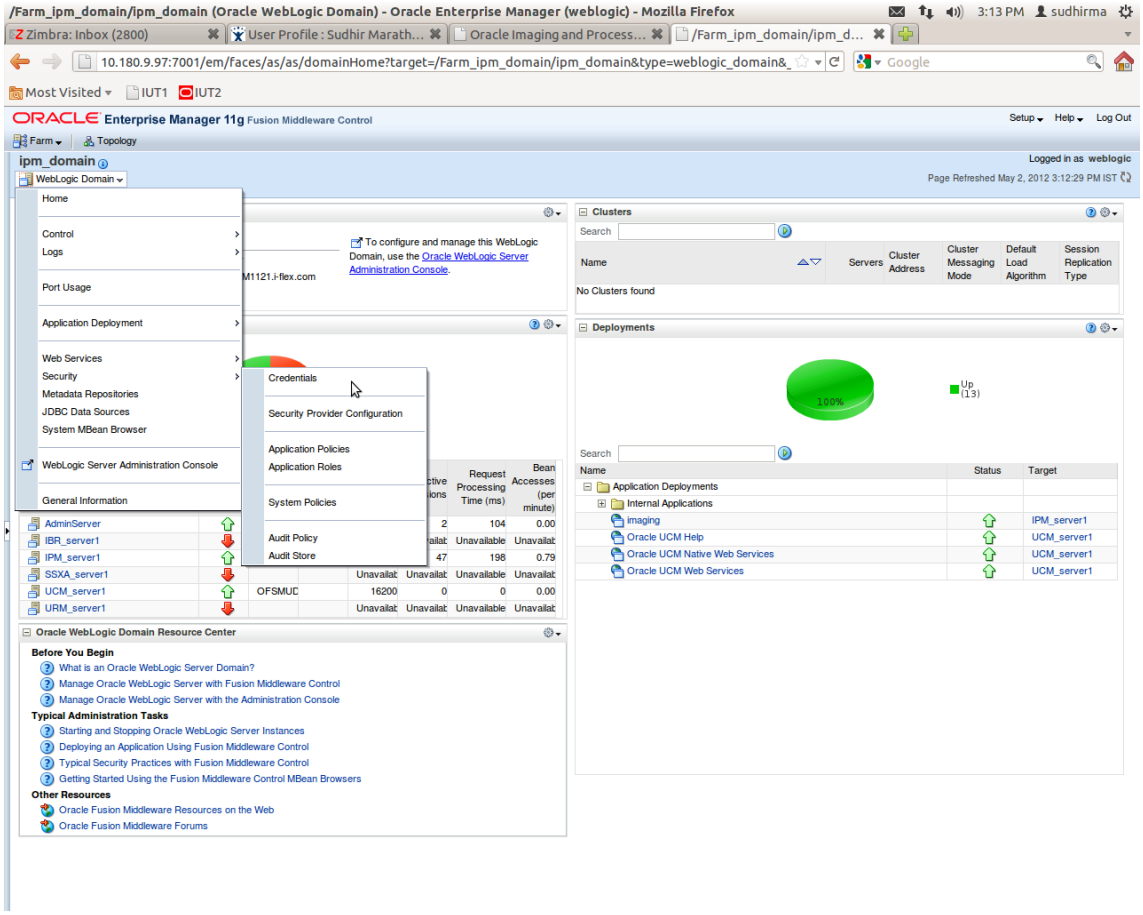
2. In the Name section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 8–36 Click Weblogic Domain: ipm domain



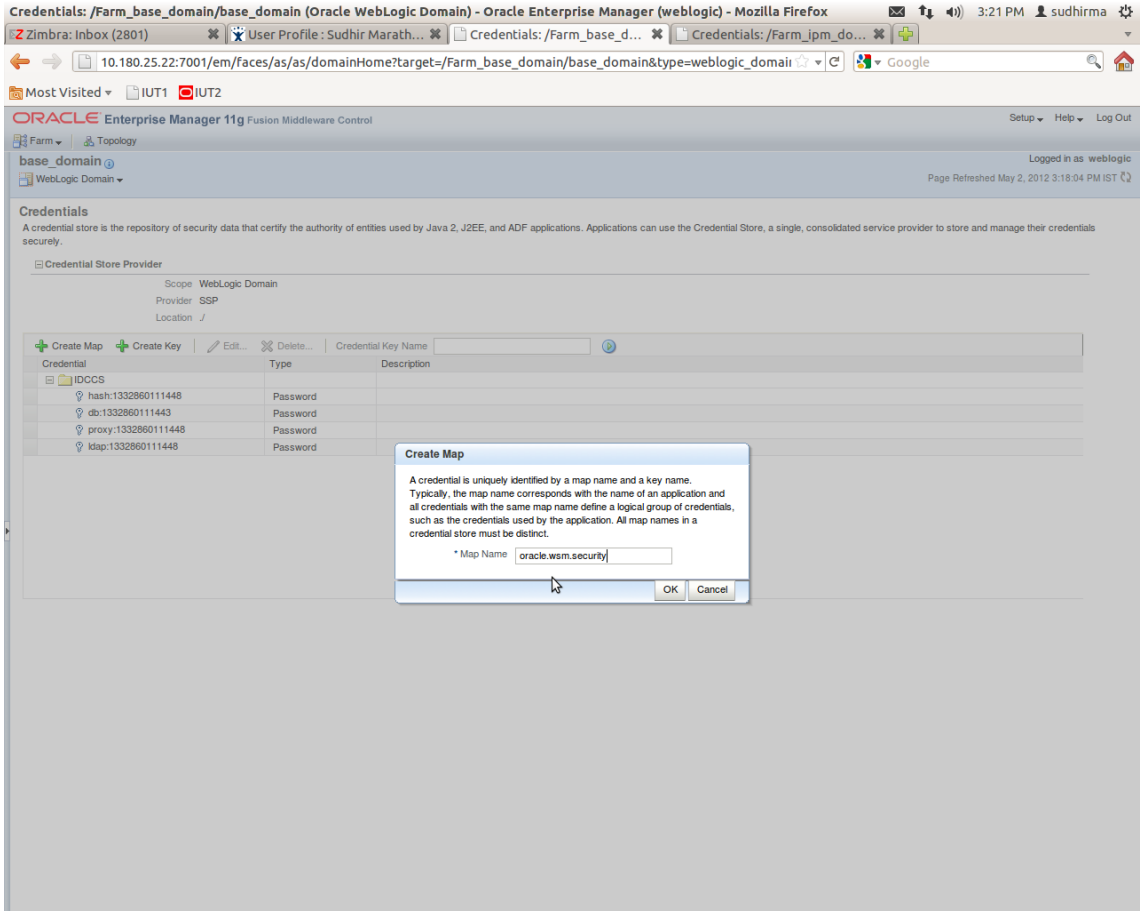
3. In the top menu, **click Weblogic Domain**. The corresponding menu appears.
4. Navigate to **Security > Credentials**. The Credentials page appears.

Figure 8–37 Navigate to Weblogic Domain --> Security --> Credentials



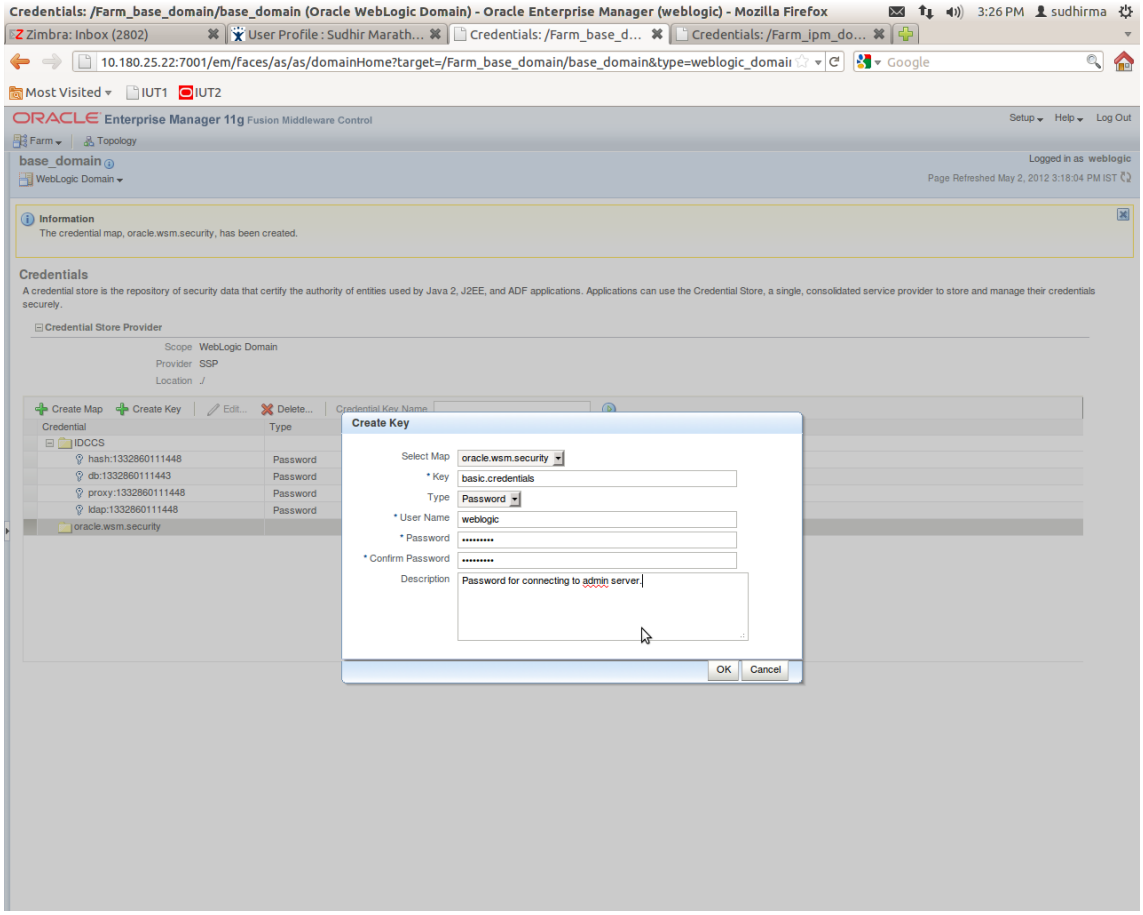
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 8–38 Create Map oracle.wsm.security



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

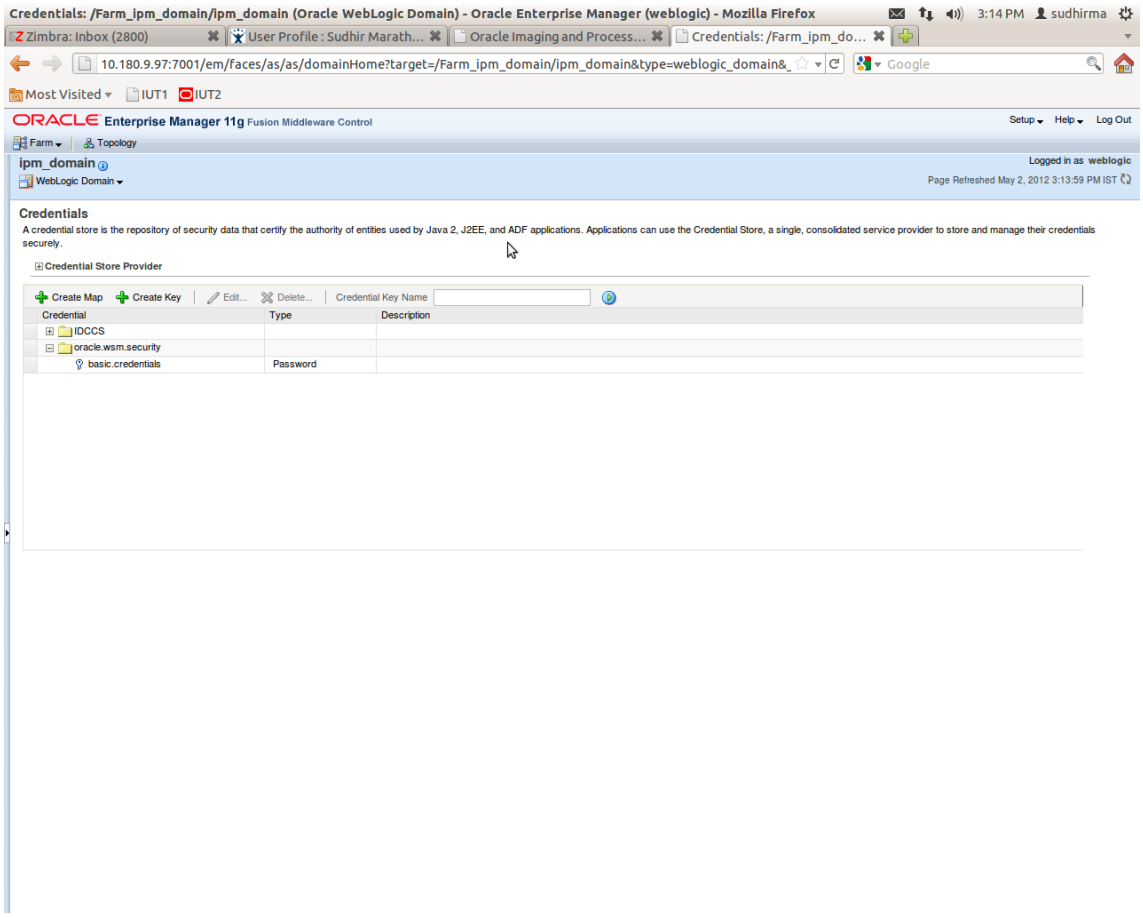
Figure 8–39 Create Key basic.credentials



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 8–40 ipm_domain: Credentials Created

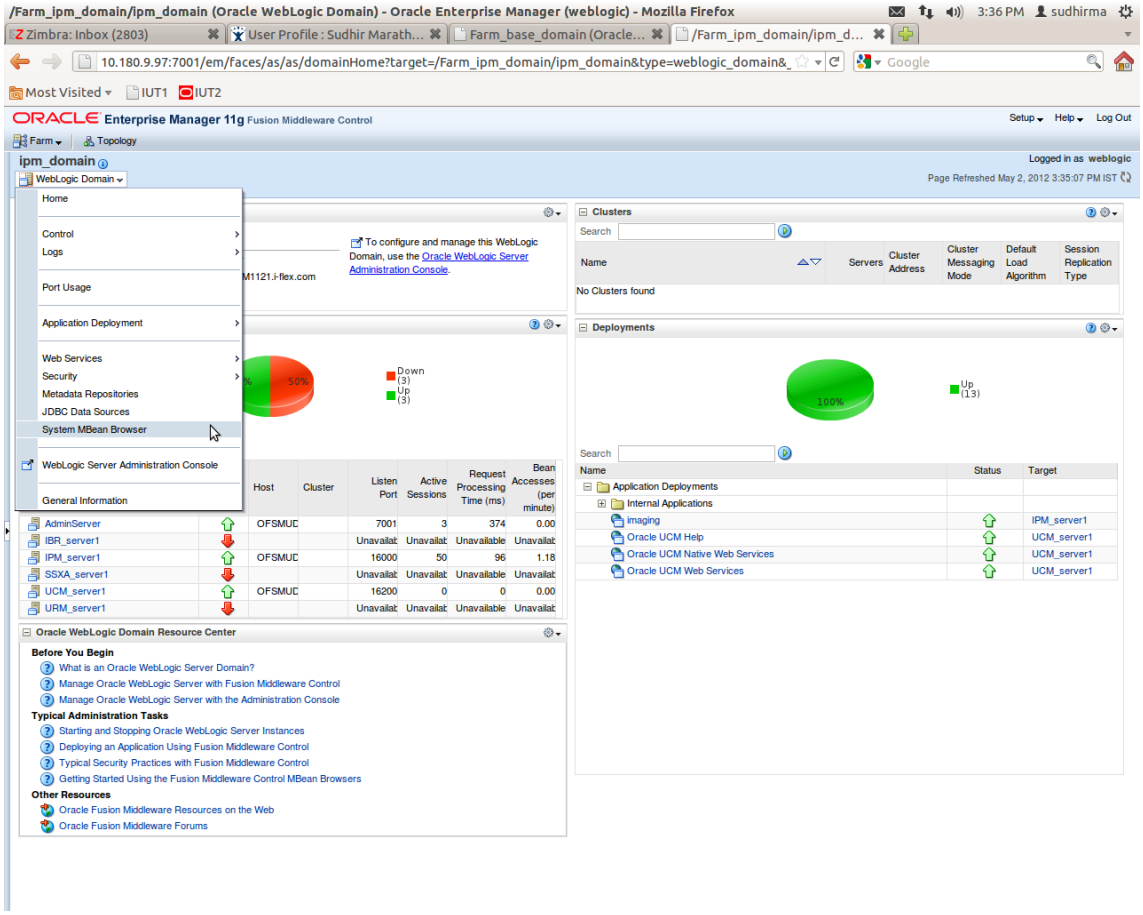


8.2.3 Setting up Input Agent Path

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.

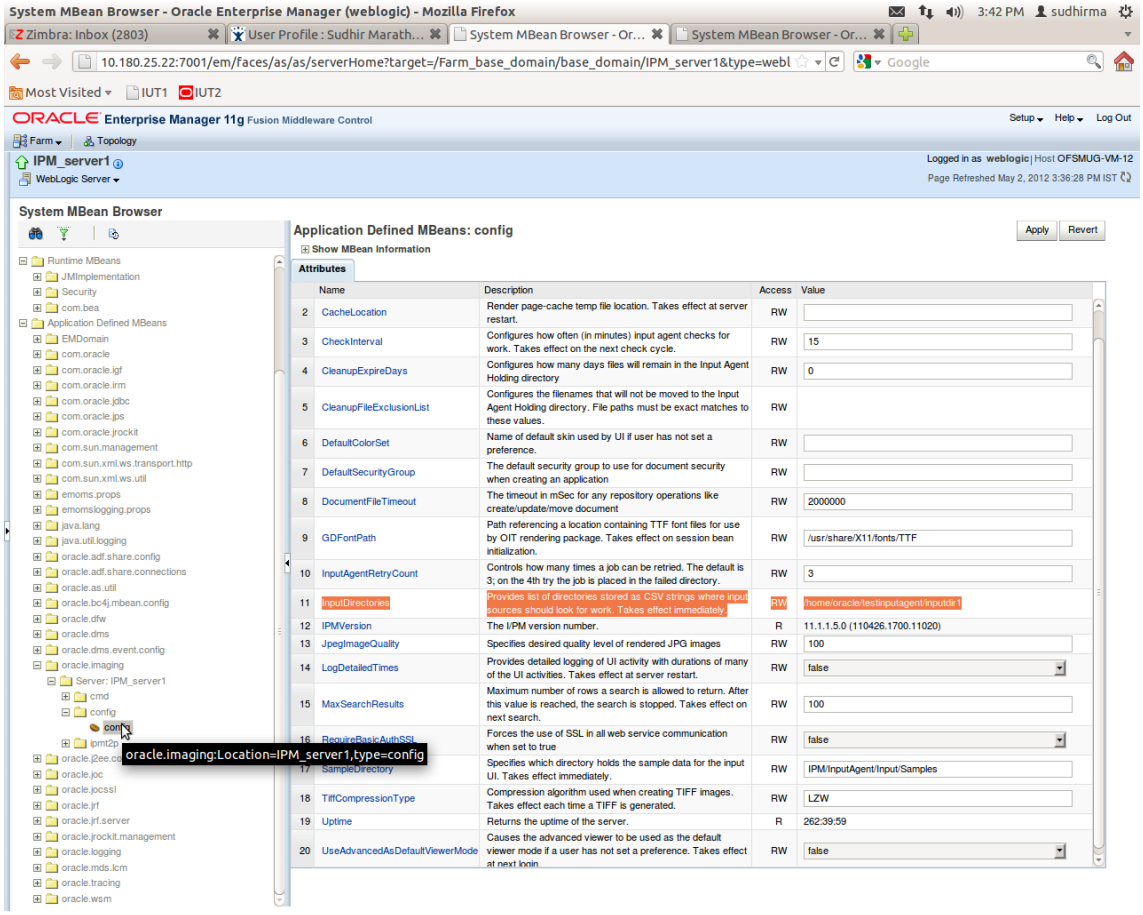
Figure 8–41 Navigate to Weblogic Domain --> System MBean Browser



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 8–42 InputDirectories: Enter Input Agent Path



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

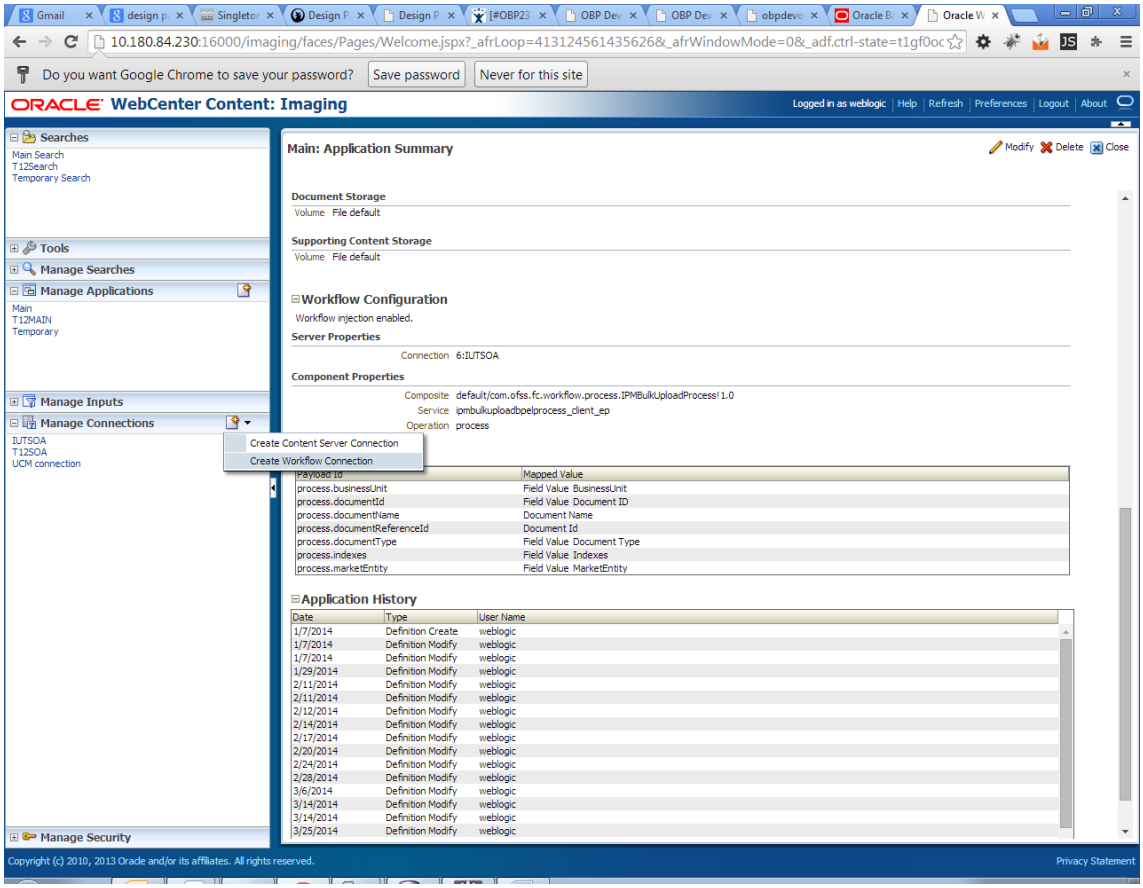
7. Restart IPM server.

8.2.4 Create SOA Connection

To create a SOA Connection:

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

Figure 8–43 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.

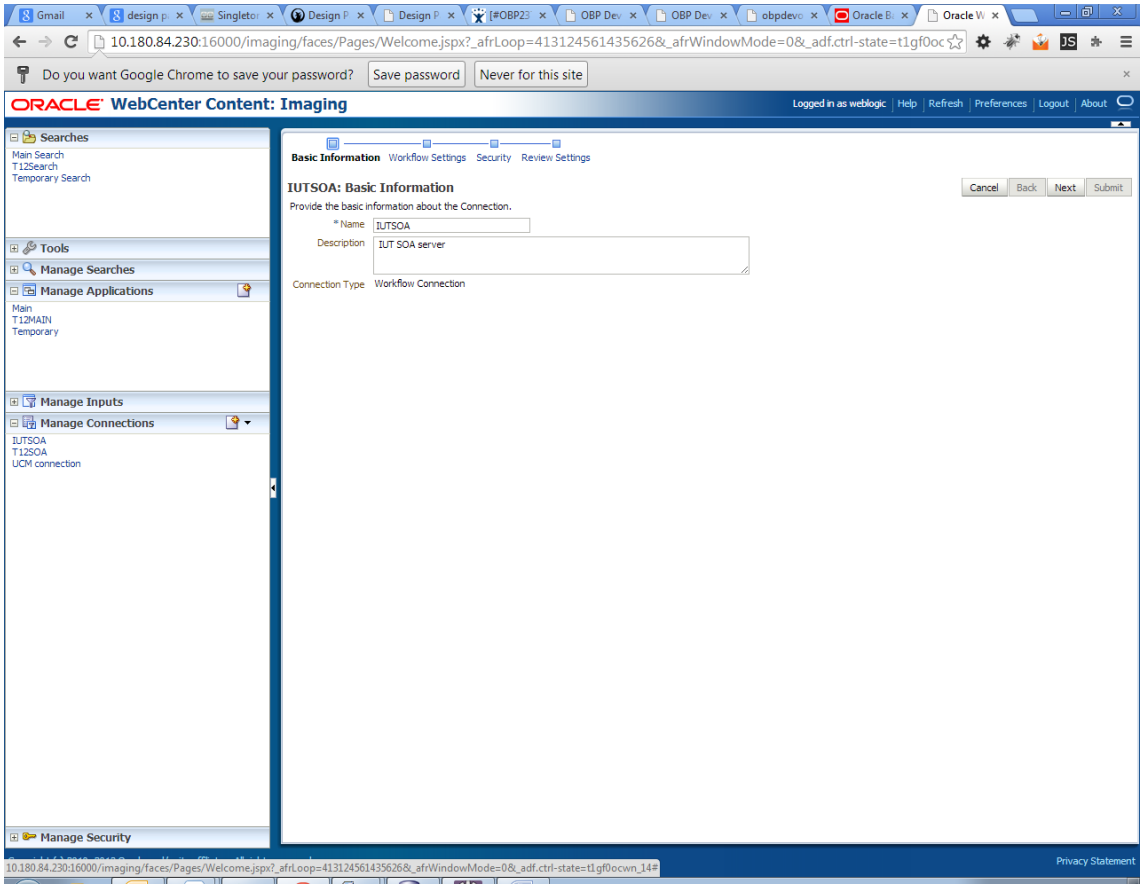
   `OBP_IPM_SOA_CONN_NAME`

   `SOA_MANAGED_SERVER_LISTEN_ADDRESS`

   `SOA_MANAGED_SERVER_LISTEN_PORT`

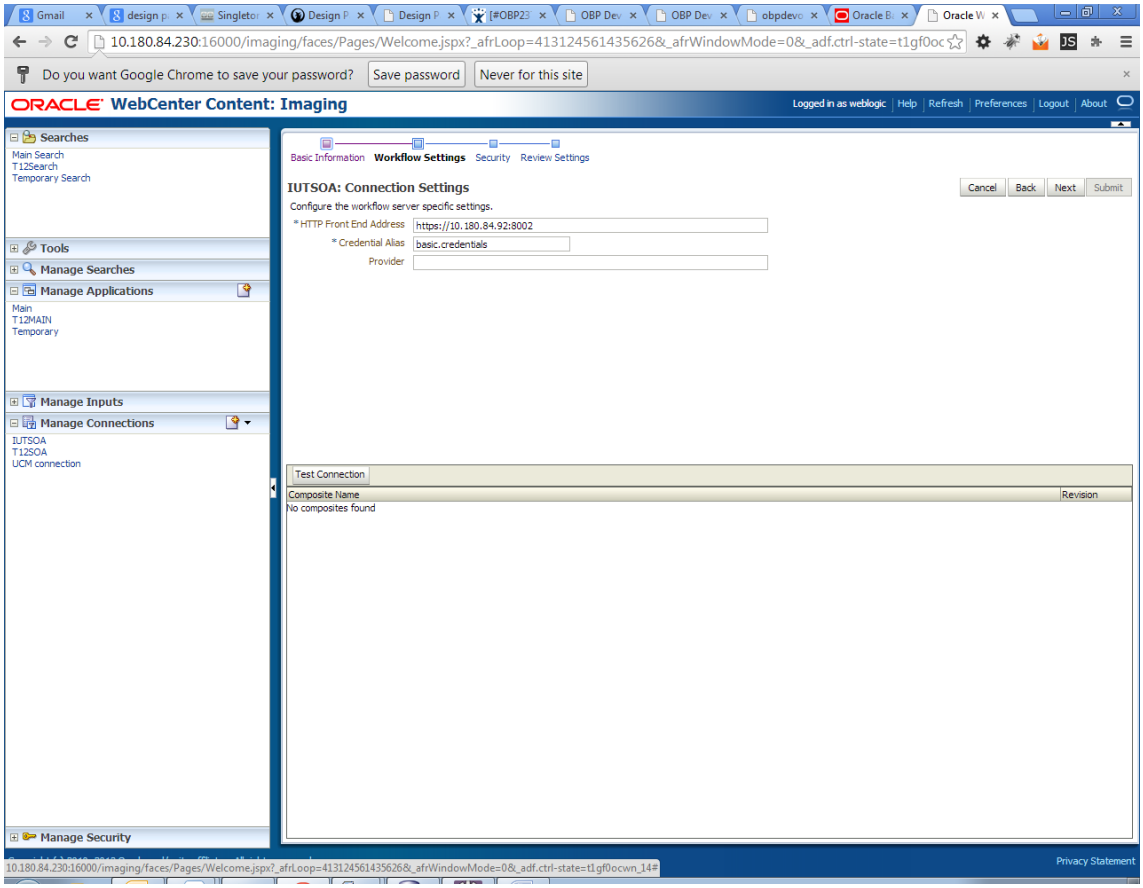
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 8–44 IUTSOA: Basic Information



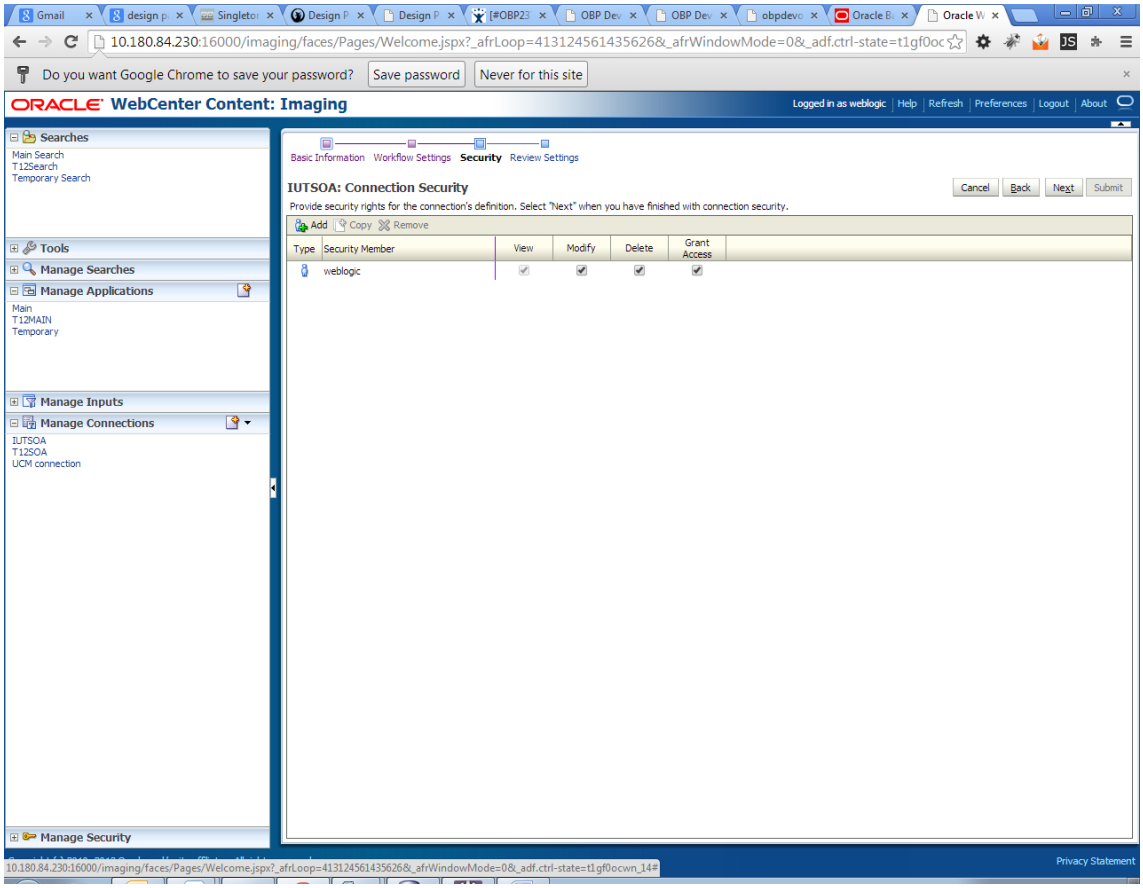
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 8–45 IUTSOA: Workflow Settings



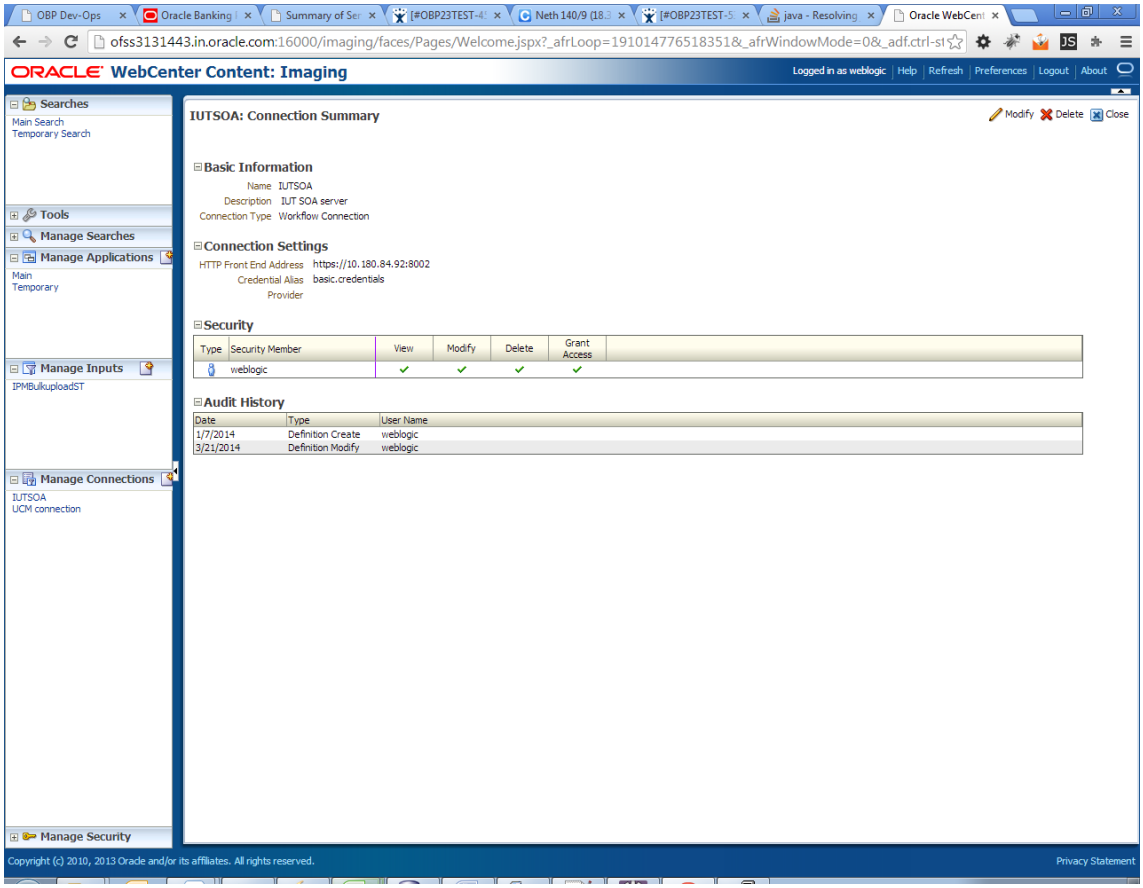
6. In the **Credential Alias** field, enter the value as **basic.credentials**.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 8–46 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 8–47 IUTSOA: Review Settings

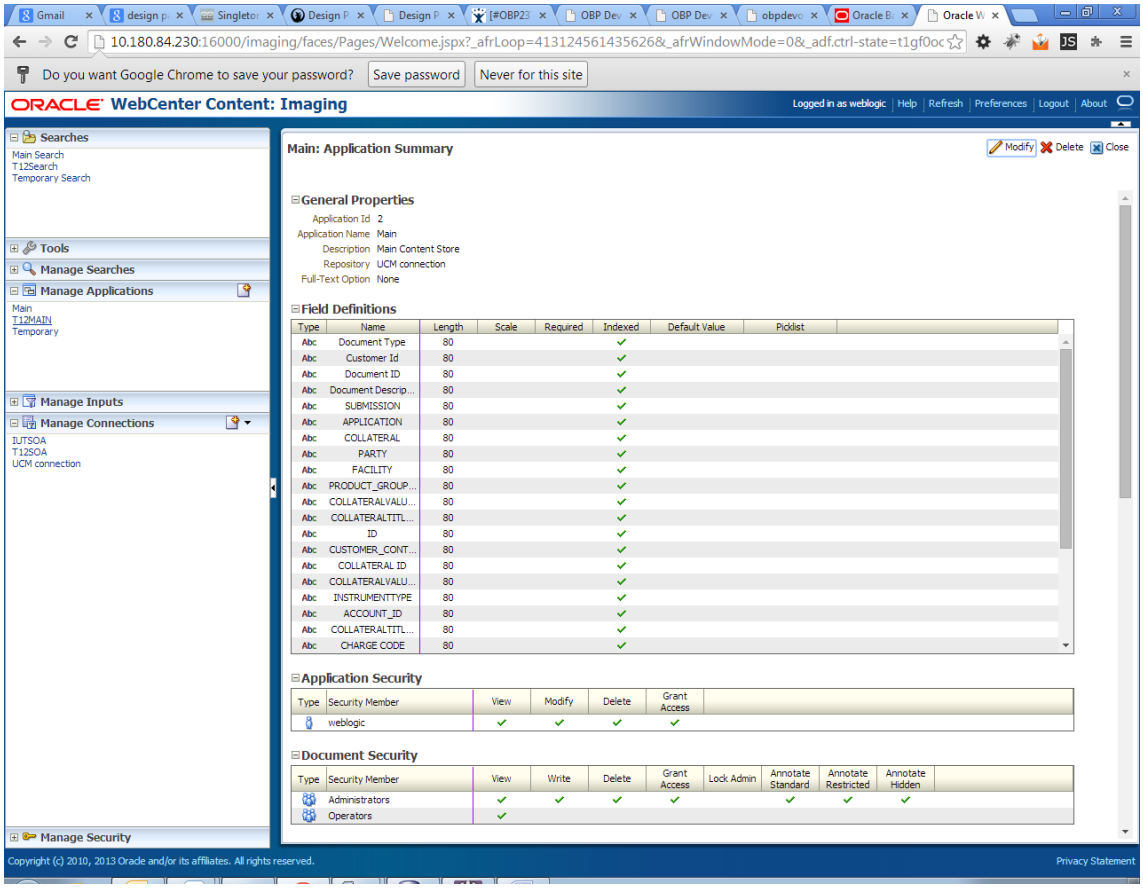


8.2.5 Manage Workflow Configuration

To manage workflow configuration:

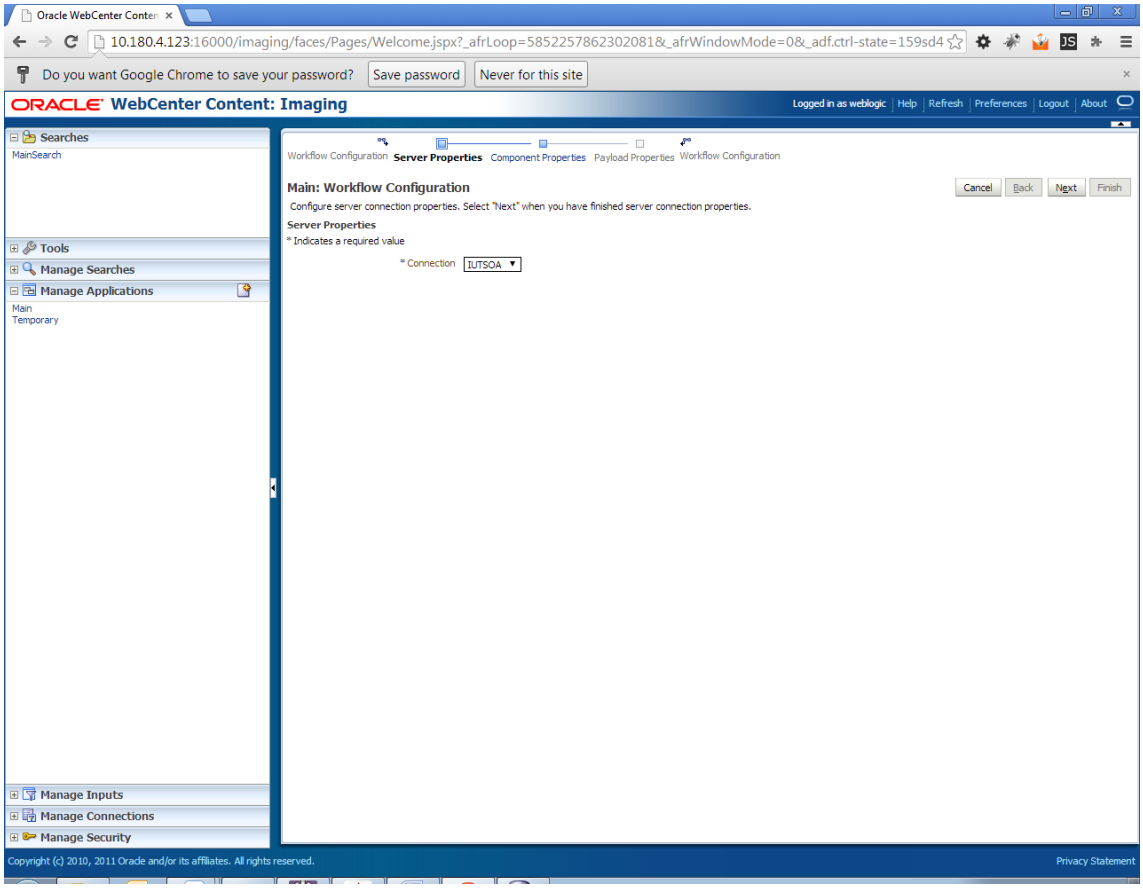
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Applications** section.

Figure 8–48 Main: Application Summary



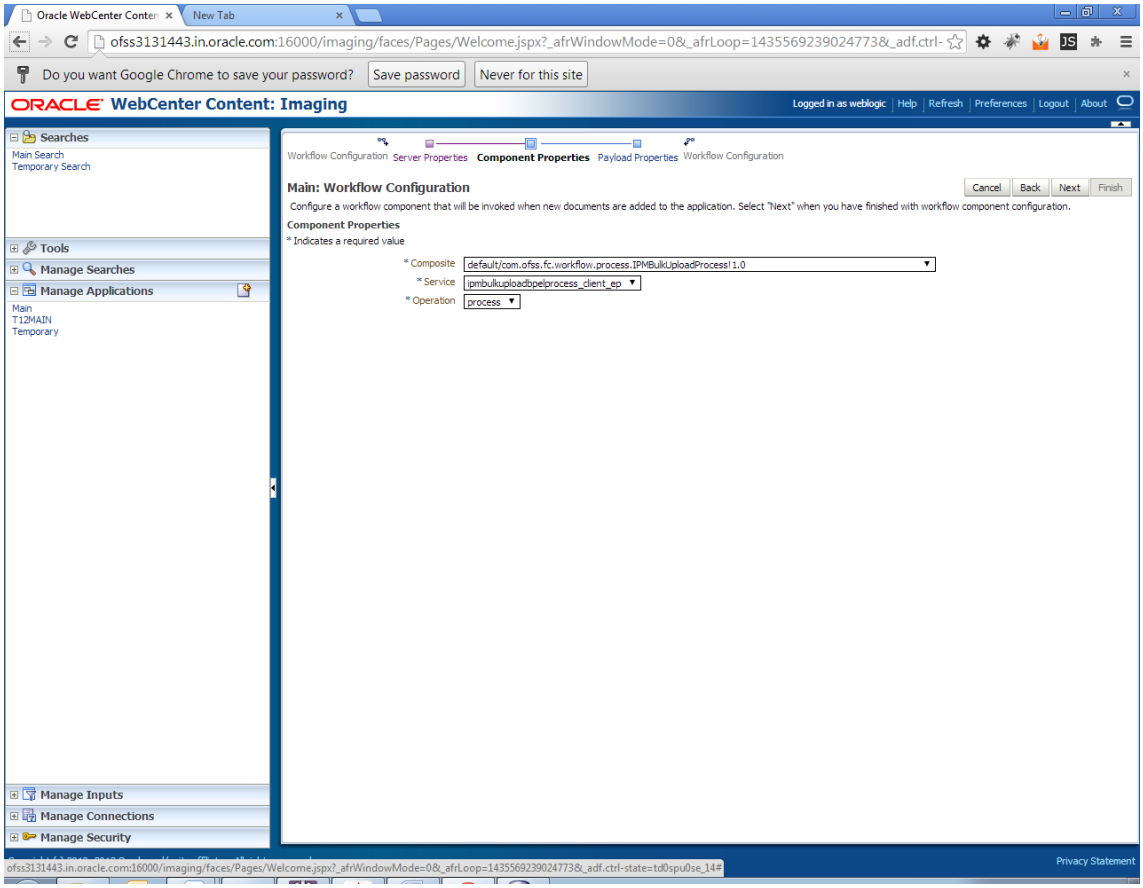
3. Select the application for which workflow configuration has to be done as shown in Figure 8–48.
4. Click **Modify.**
5. Navigate to the Workflow Configuration section.
6. Click the **Add/Modify** button.
7. In the Server Properties section, select the connection (IUTSOA) which was created in **Manage Connections** section from the **Connection** list.

Figure 8–49 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.**

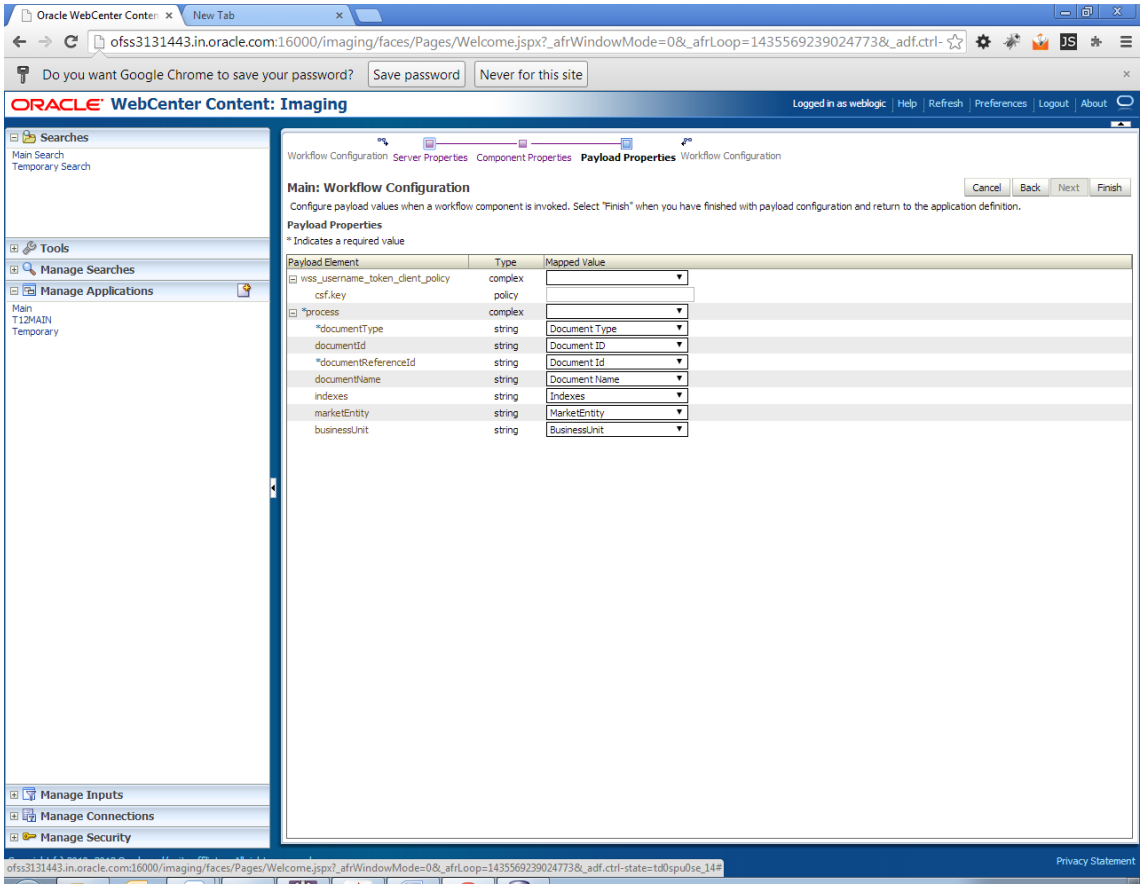
Figure 8–50 Manage Applications - Component Properties



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.

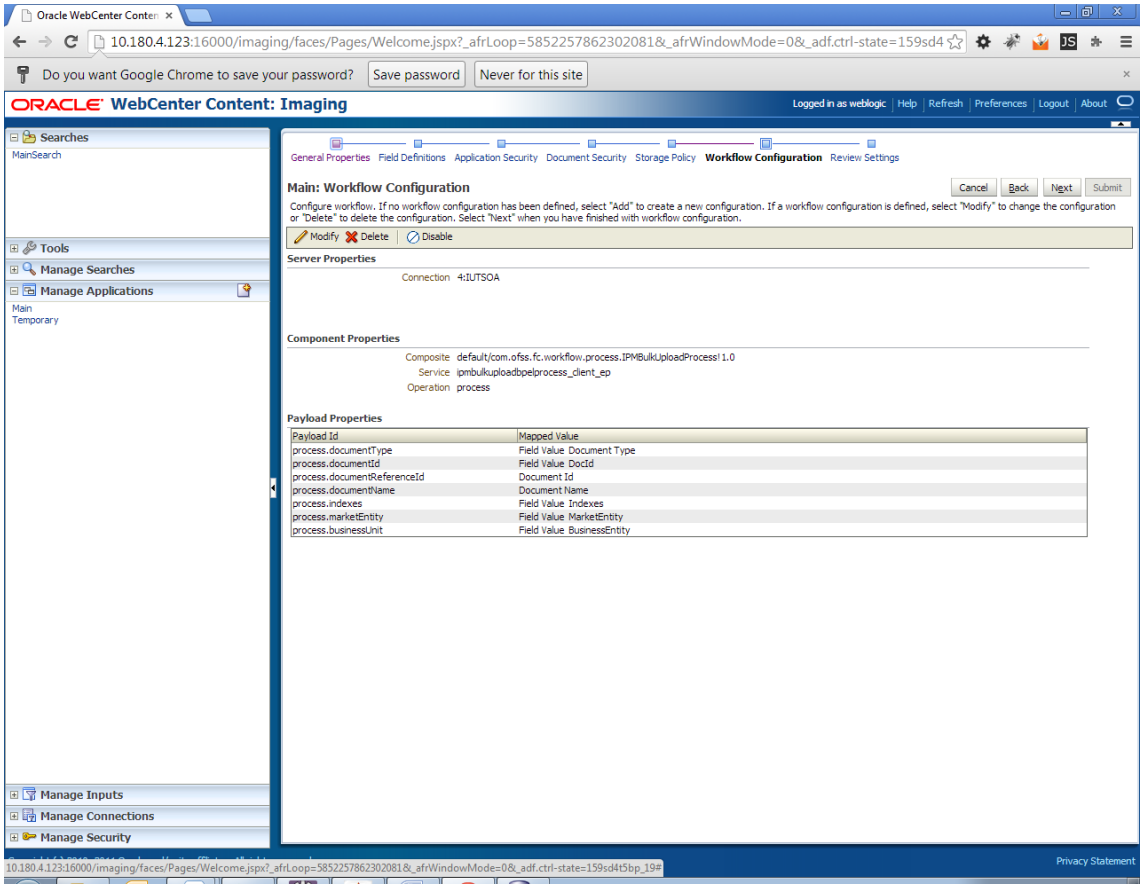
> **Note**
>
> The document ReferenceId is mapped to Document Id (IPM internal field), whereas documentId is mapped to doc Id which is application field.

Figure 8–51 Manage Applications - Payload Properties



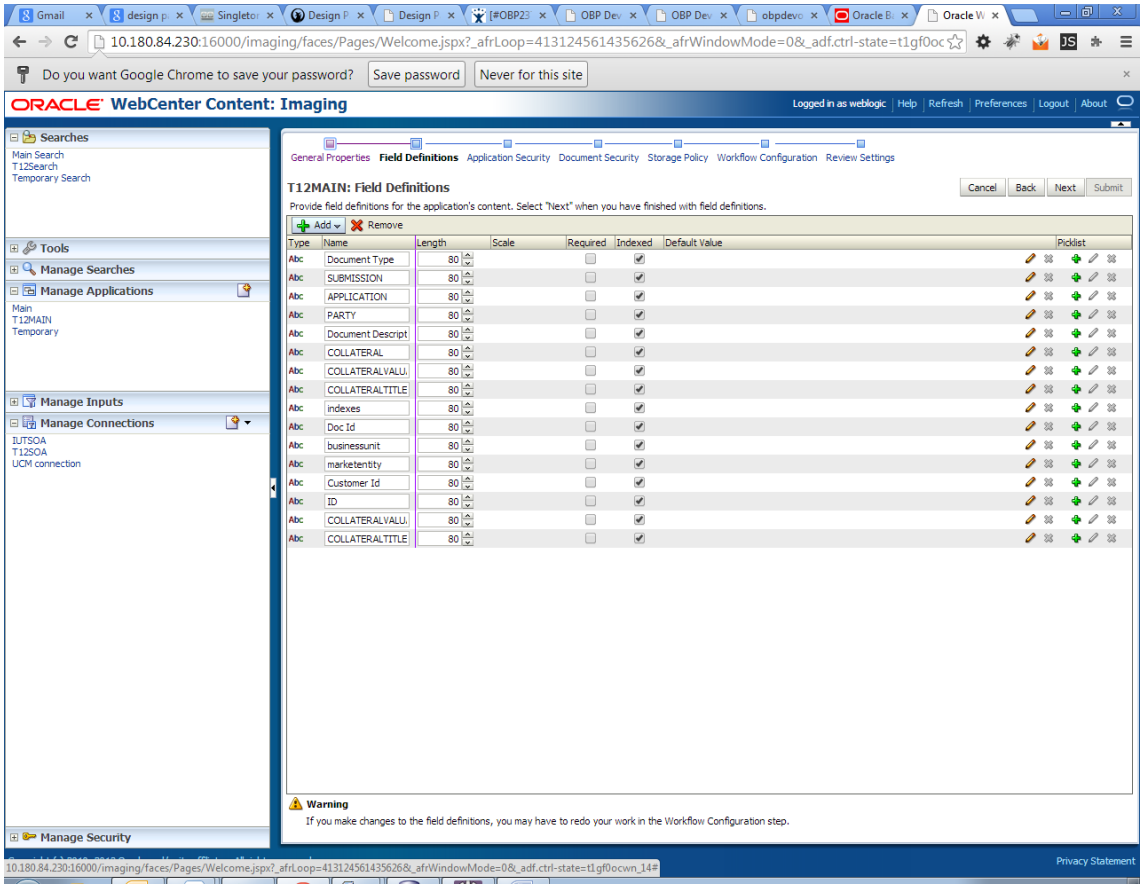
16. Click **Next.**
17. Complete the Workflow Configuration. Click **Next.**

Figure 8–52 Manage Applications - Workflow Configuration



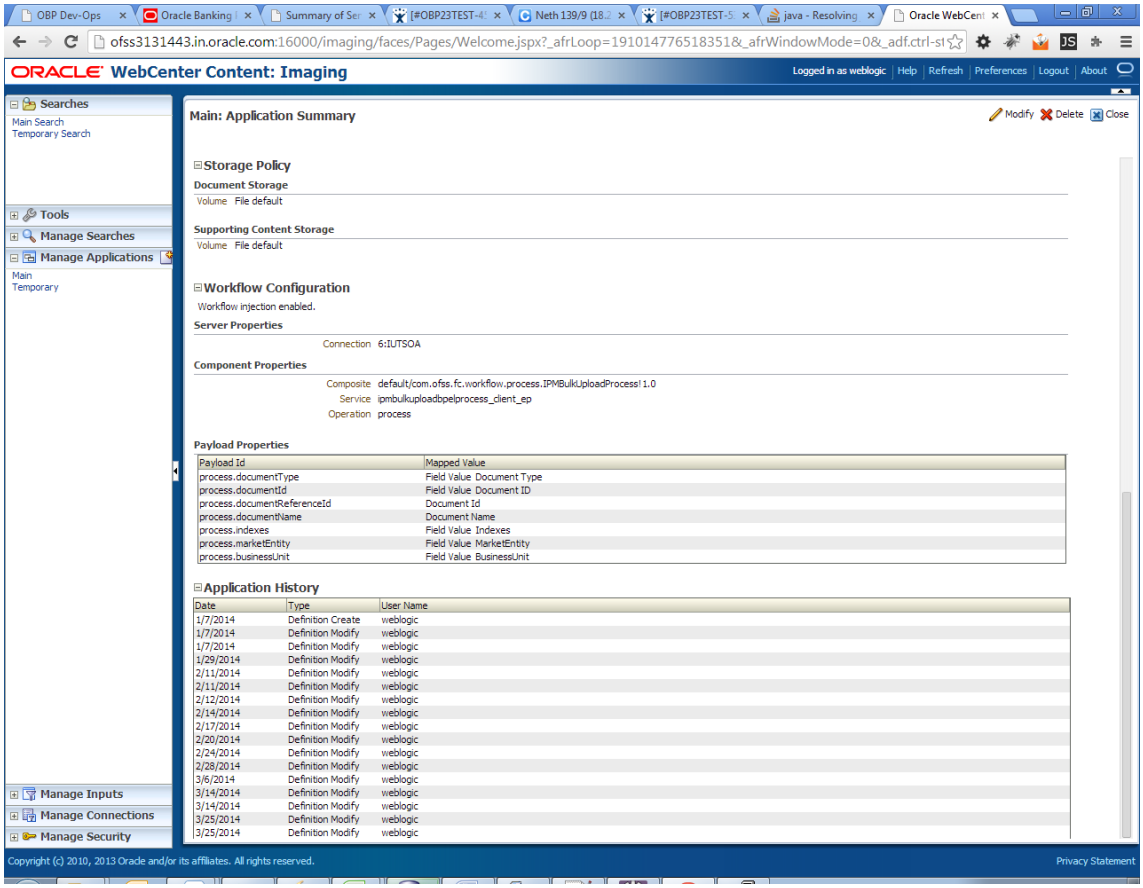
18. Add all those fields which are not present in the application as shown below.

Figure 8–53 Field Definitions



The Main Application Summary appears as shown Figure 8–54.

Figure 8–54 Main: Application Summary

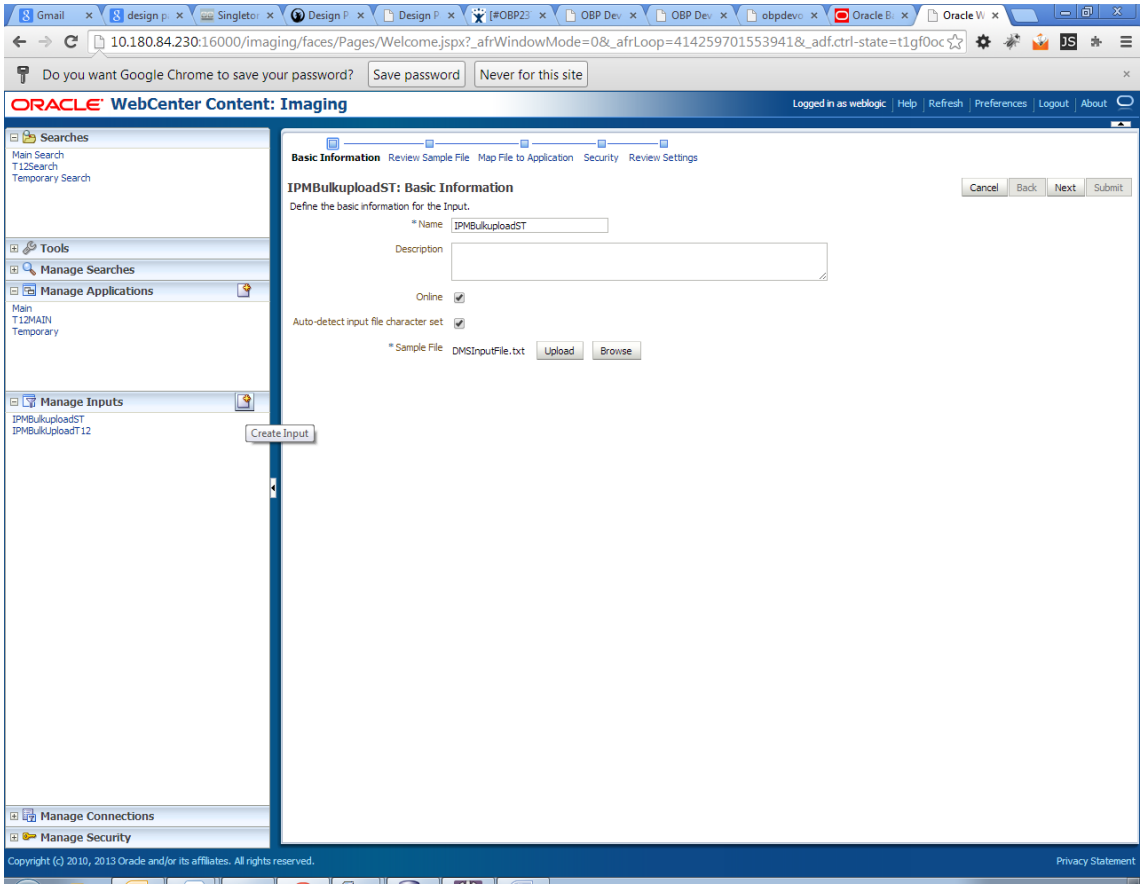


8.2.6 Manage Inputs for Input Agents

To manage workflow configuration:

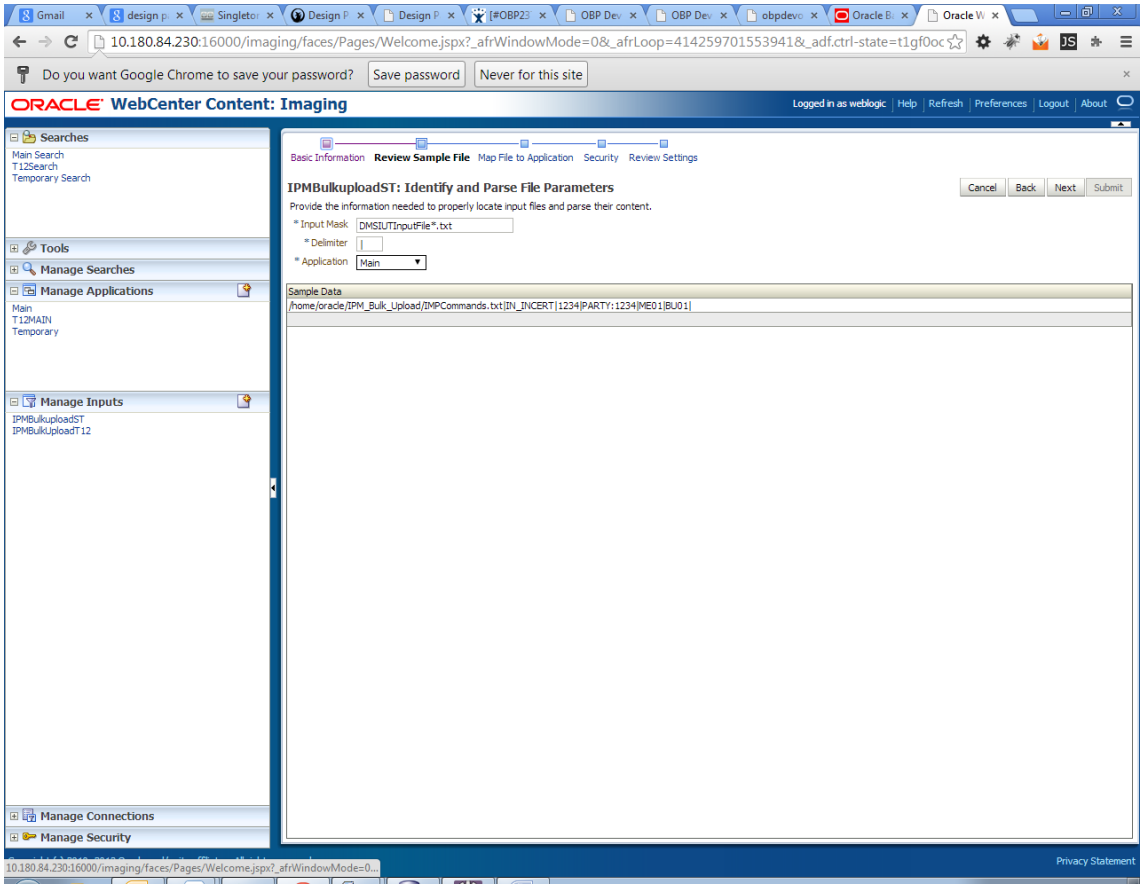
1. Log in to Image Processing Management (IPM).
2. Navigate to **Manage Inputs** section.

Figure 8–55 Input Agent: Basic Information



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

Figure 8–56 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';`

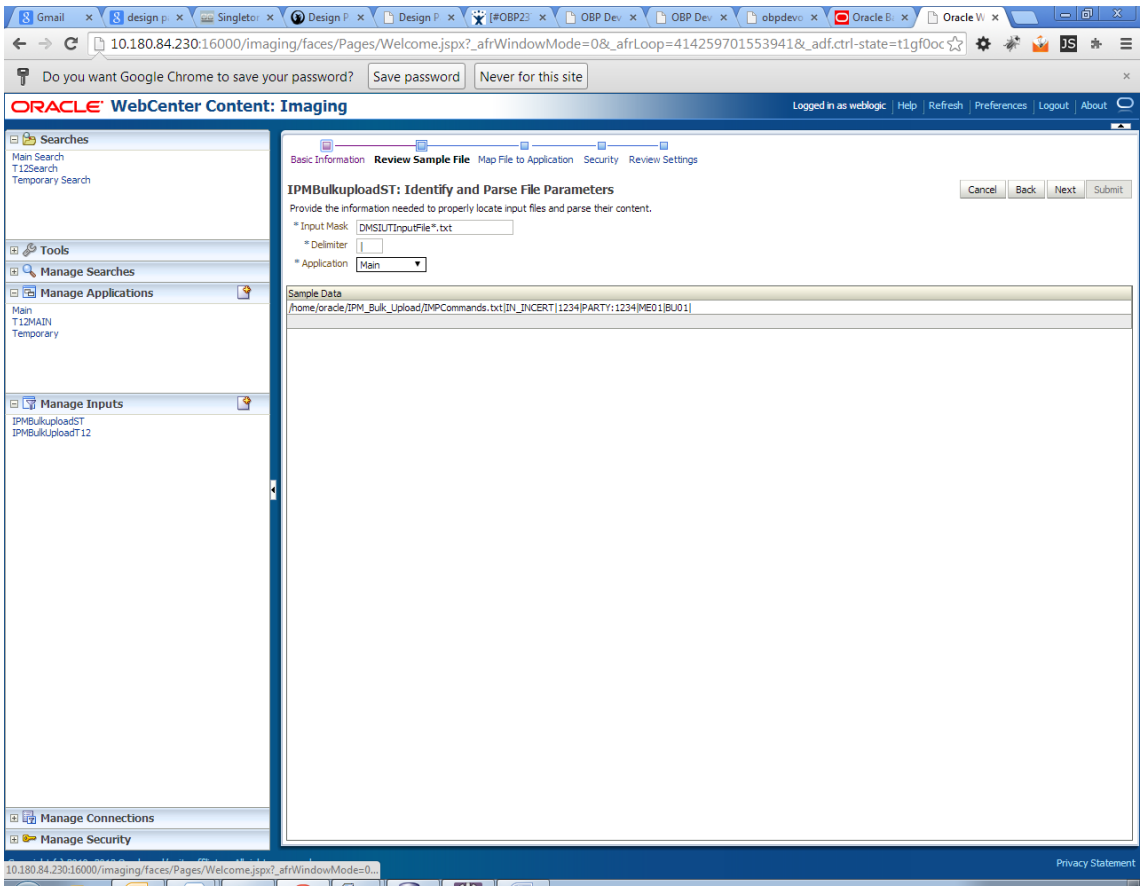
   Note

   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).

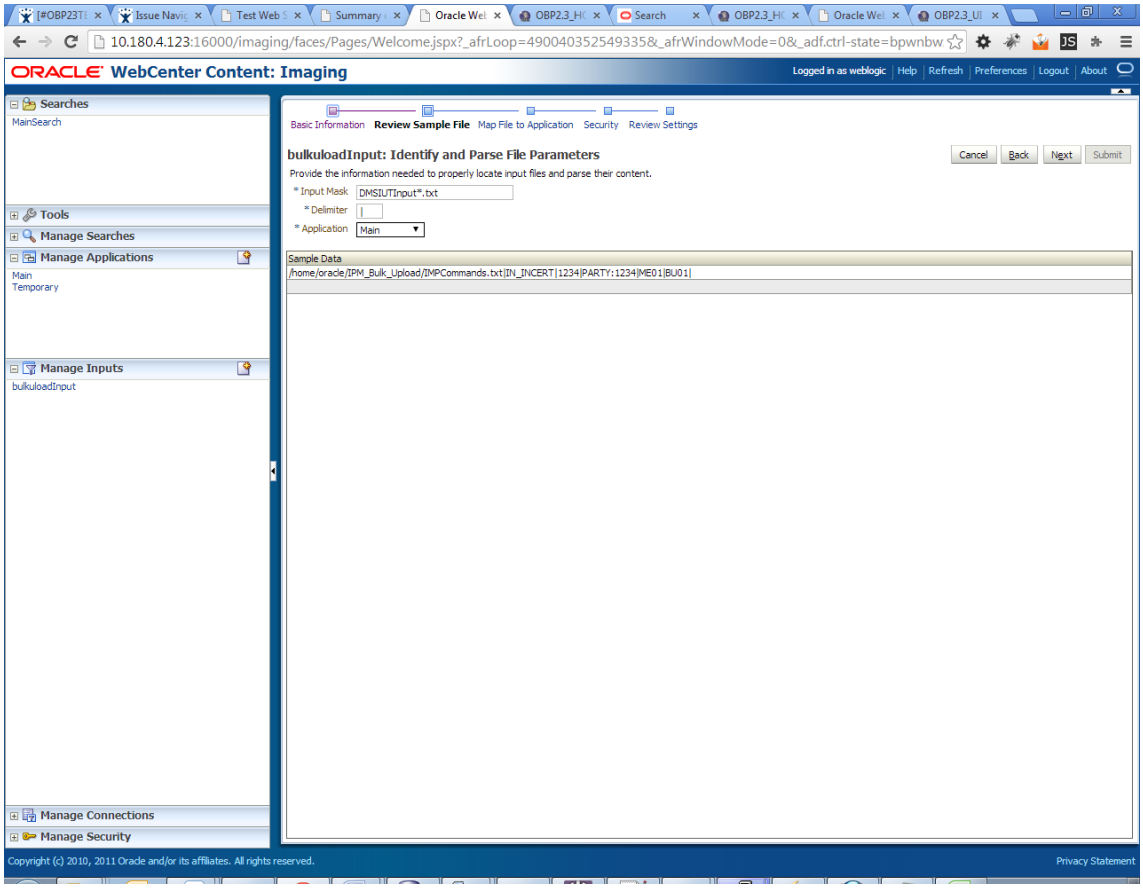
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 8–57 Input Agent: File Parameters



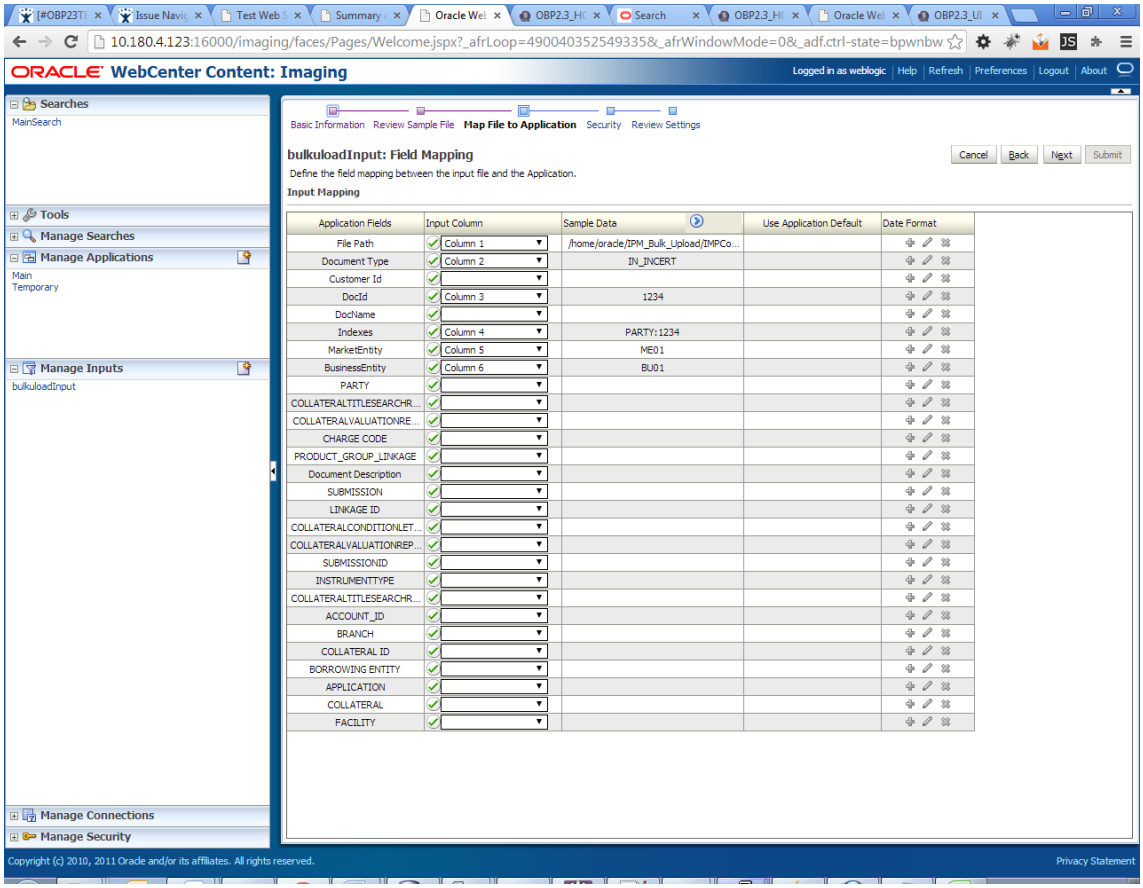
9. In the Field Mapping section, map the **Application Fields.**

Figure 8–58 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 8–59.

Figure 8–59 Input Agent: Summary



Note

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

8.2.7 Additional Steps

1. Update user and bankcode as follows:

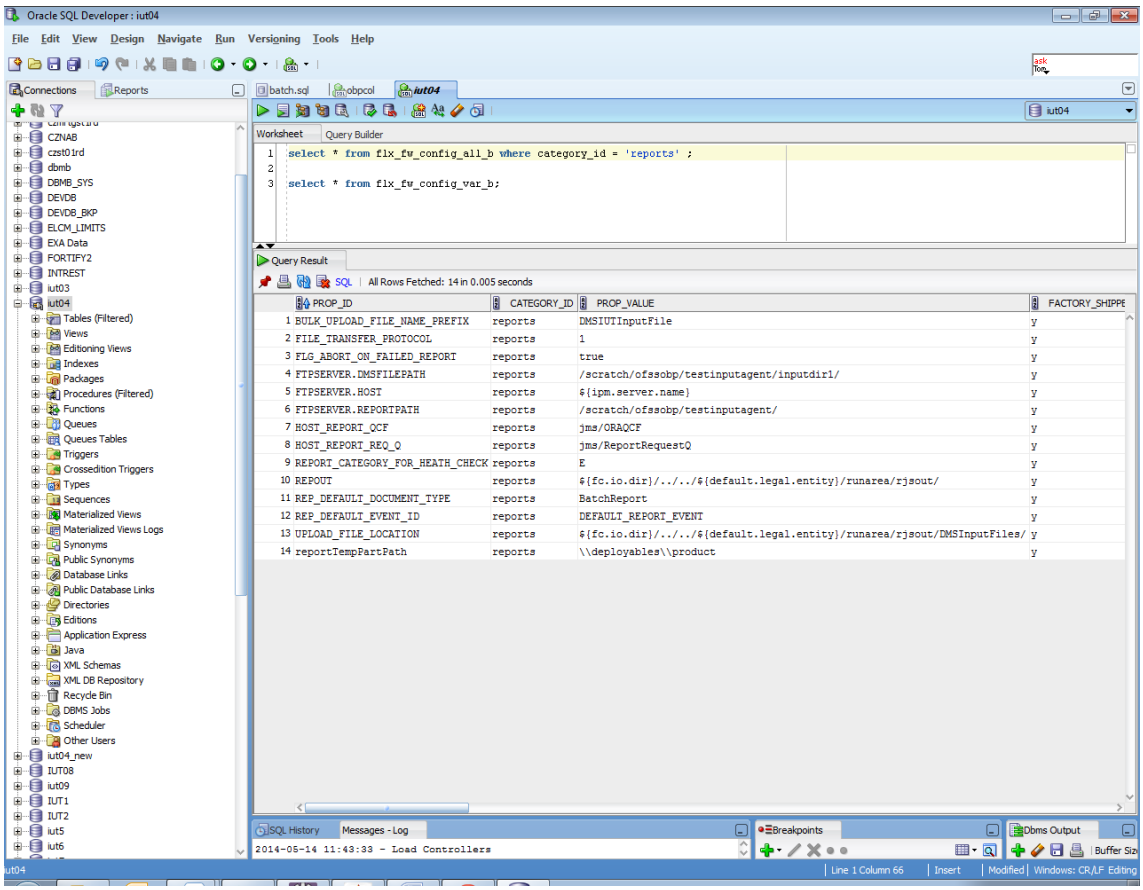
```
update flx_fw_config_all_b set prop_value='48' where prop_
value='335' and category_id like 'contentmanager%';
update flx_fw_config_all_b set prop_value='ofssuser' where
prop_id='userId' and category_id like 'contentmanager%';
```

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 8–1 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 8–60 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.

8.2.8 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.

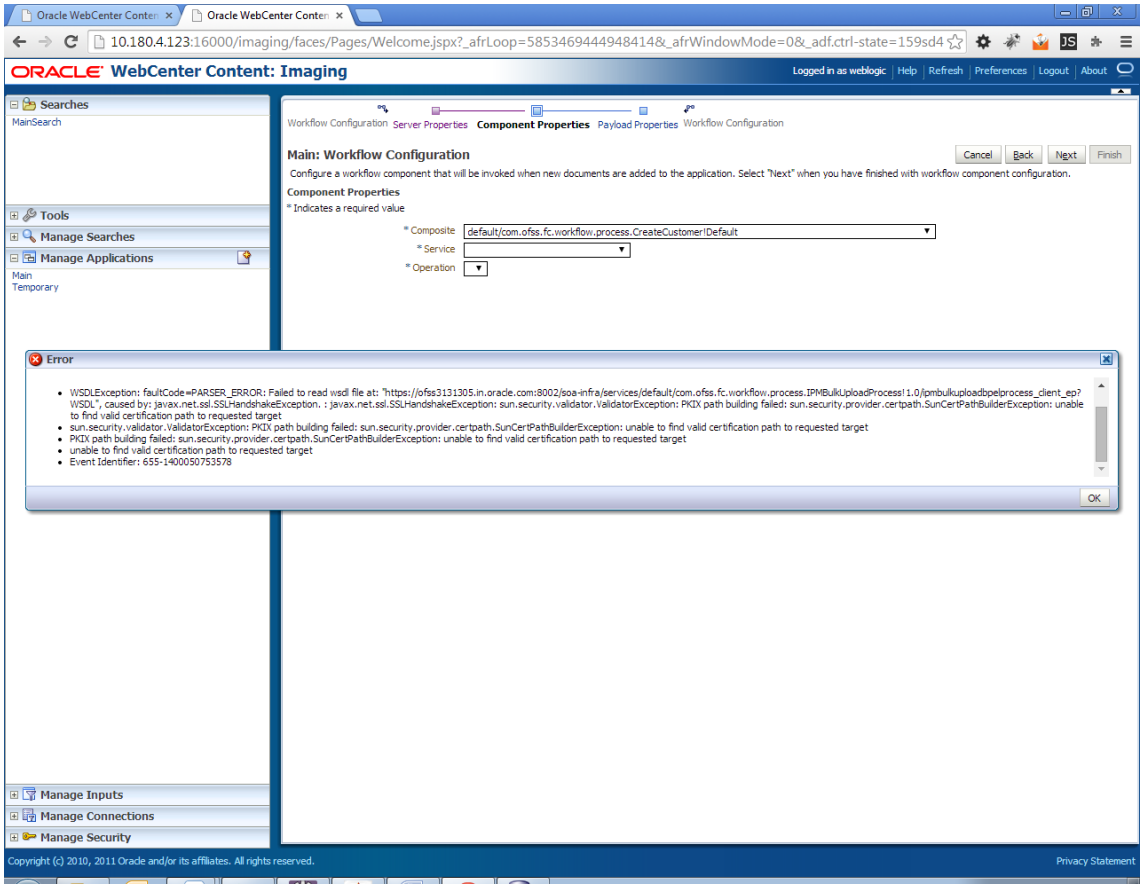
   Copy certificate at following path on IPM server.

   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 8–61 SSL Handshake Resolution



8.3 IPM Report Upload Setup

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

8.3.1 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.

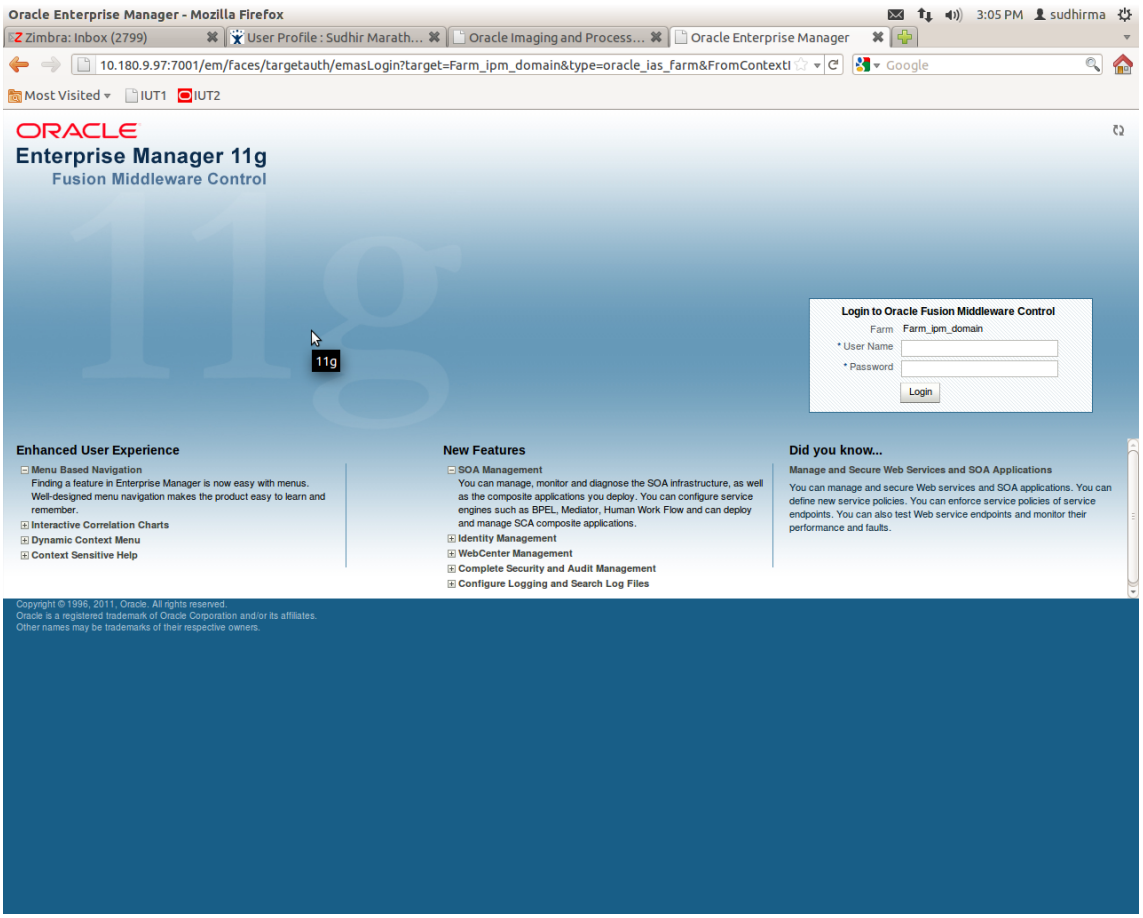
8.3.2 Setting up the Connection Name

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:

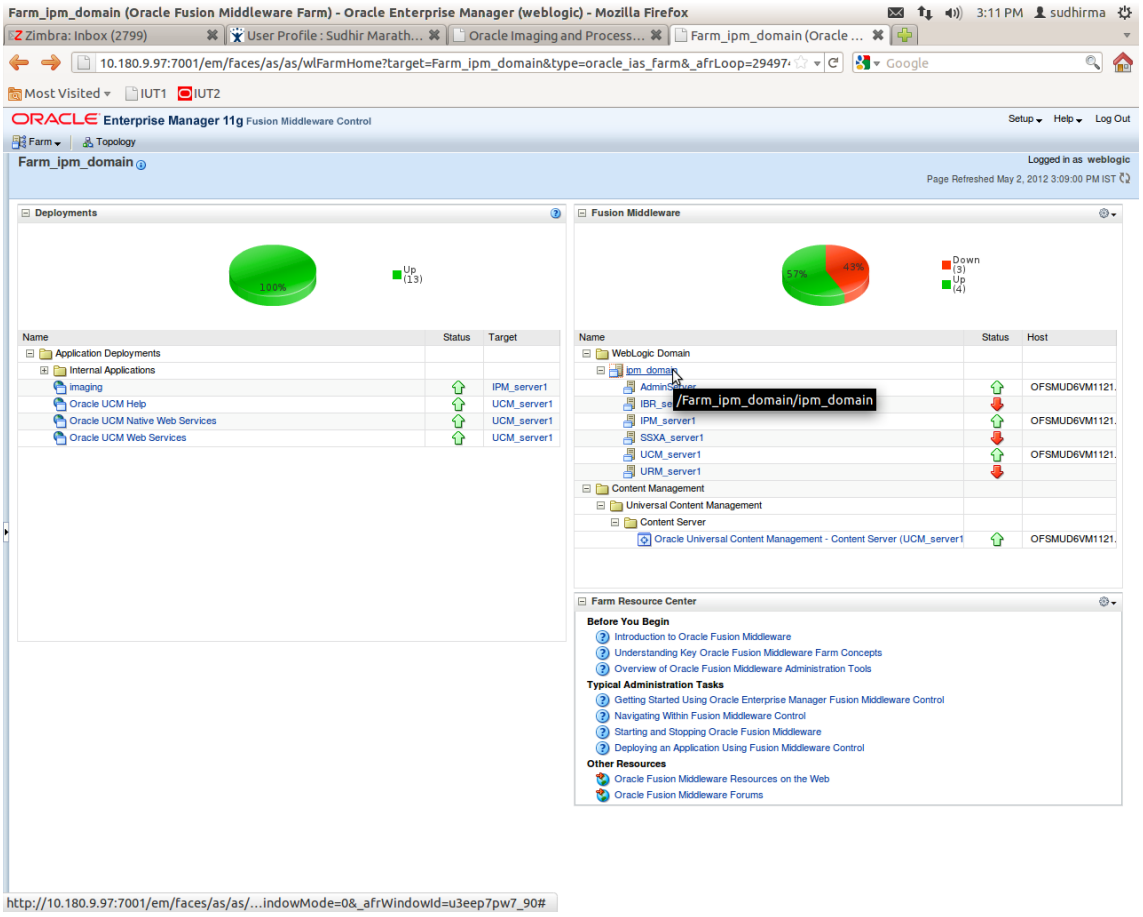
1. Log in to Enterprise Manager (EM) console.

Figure 8–62 Log in to Enterprise Manager (EM) console



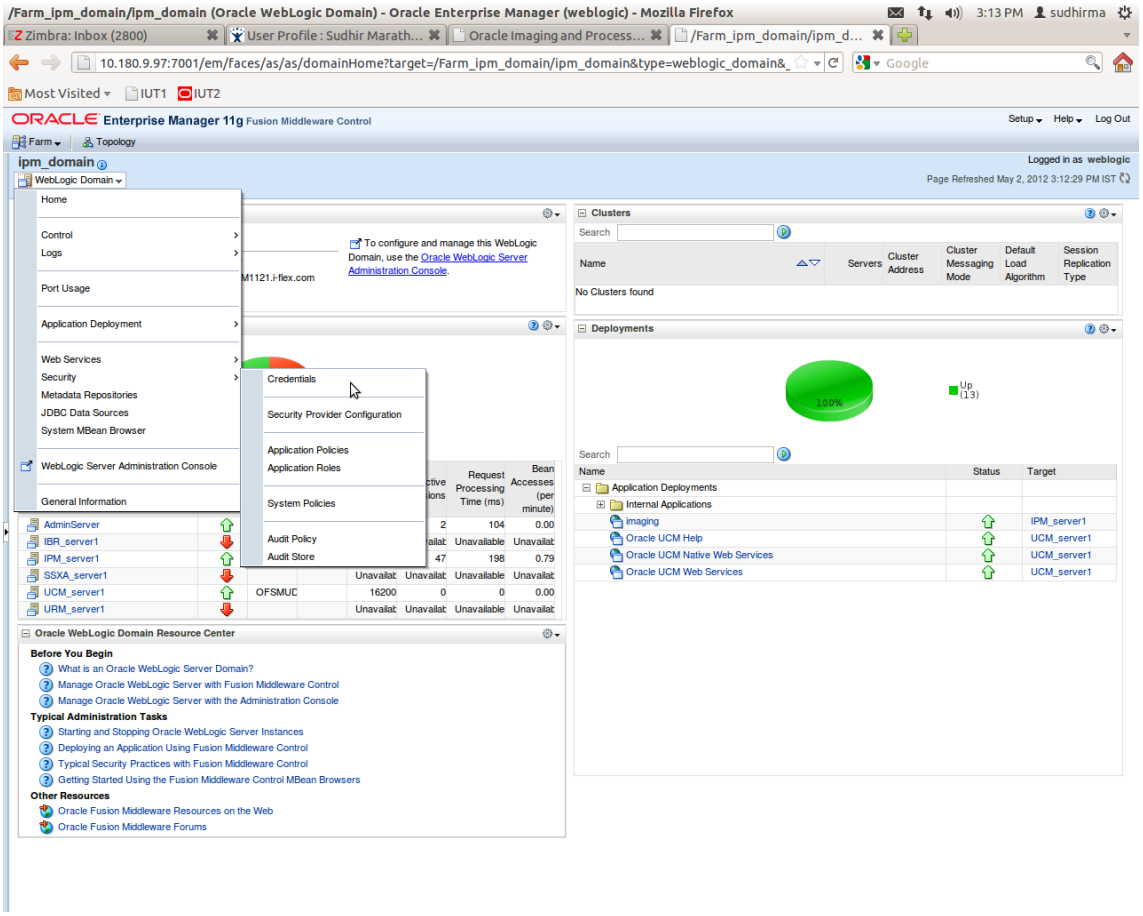
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain** (or base domain where ipm server is installed).

Figure 8–63 Click Weblogic Domain: ipm domain



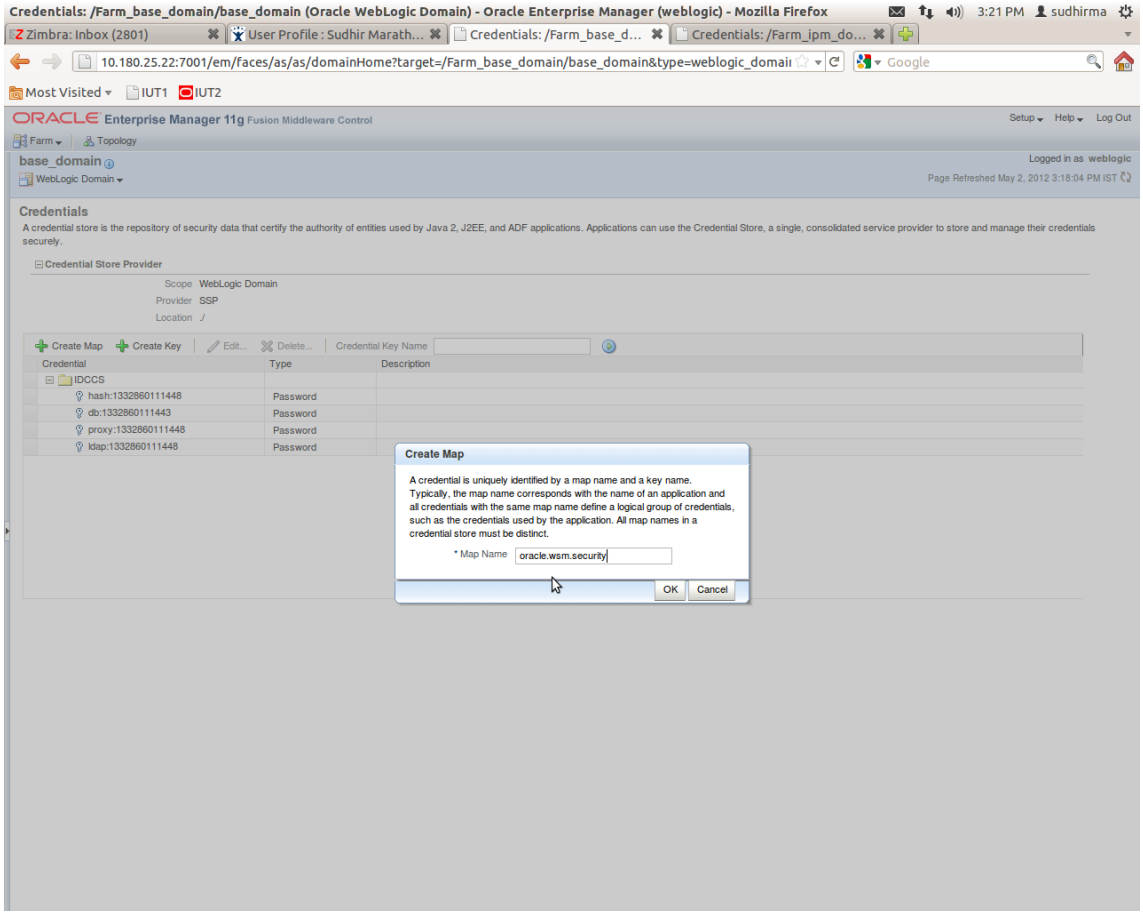
3. In the top menu, click **Weblogic Domain.** The corresponding menu appears.
4. Navigate to **Security > Credentials.** The Credentials page appears.

Figure 8–64 Navigate to Weblogic Domain --> Security --> Credentials



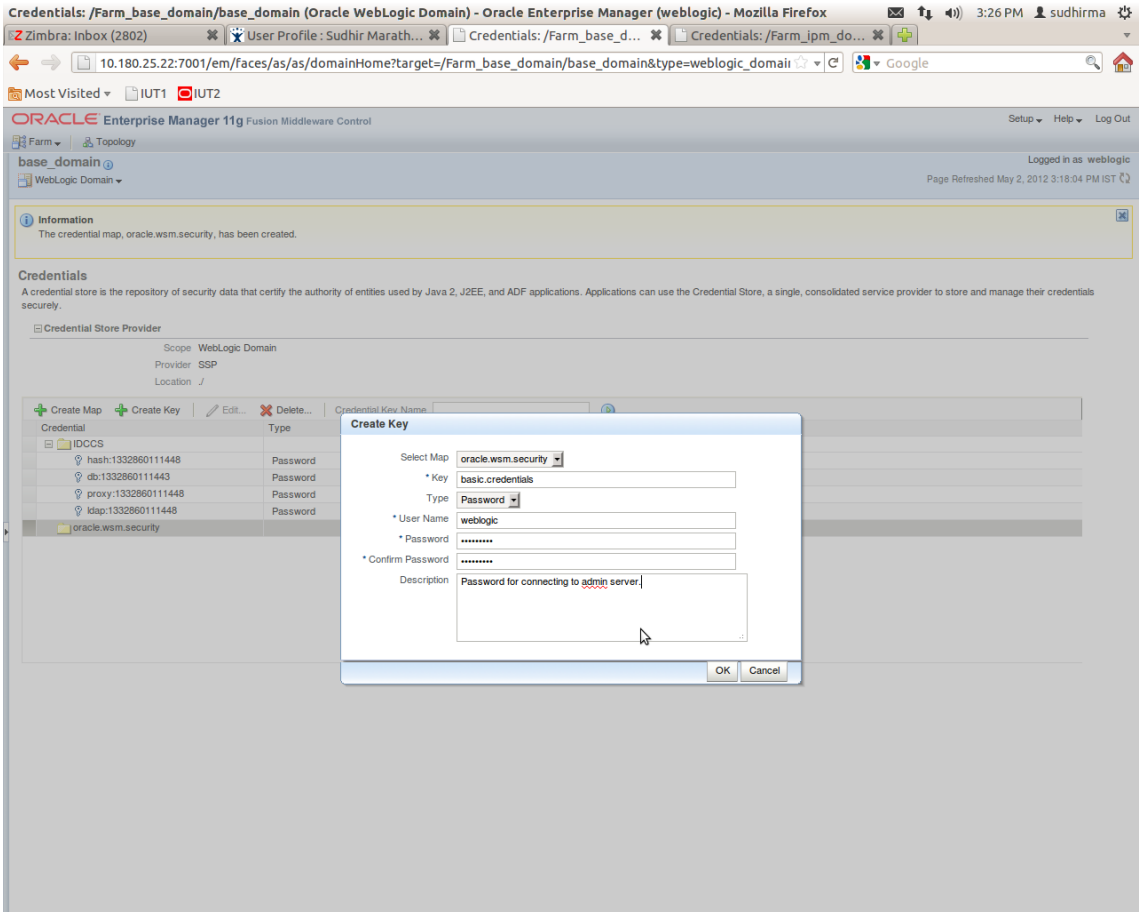
5. Click **Create Map** to create a map with the **Map Name** as **oracle.wsm.security.**

Figure 8–65 Create Map oracle.wsm.security



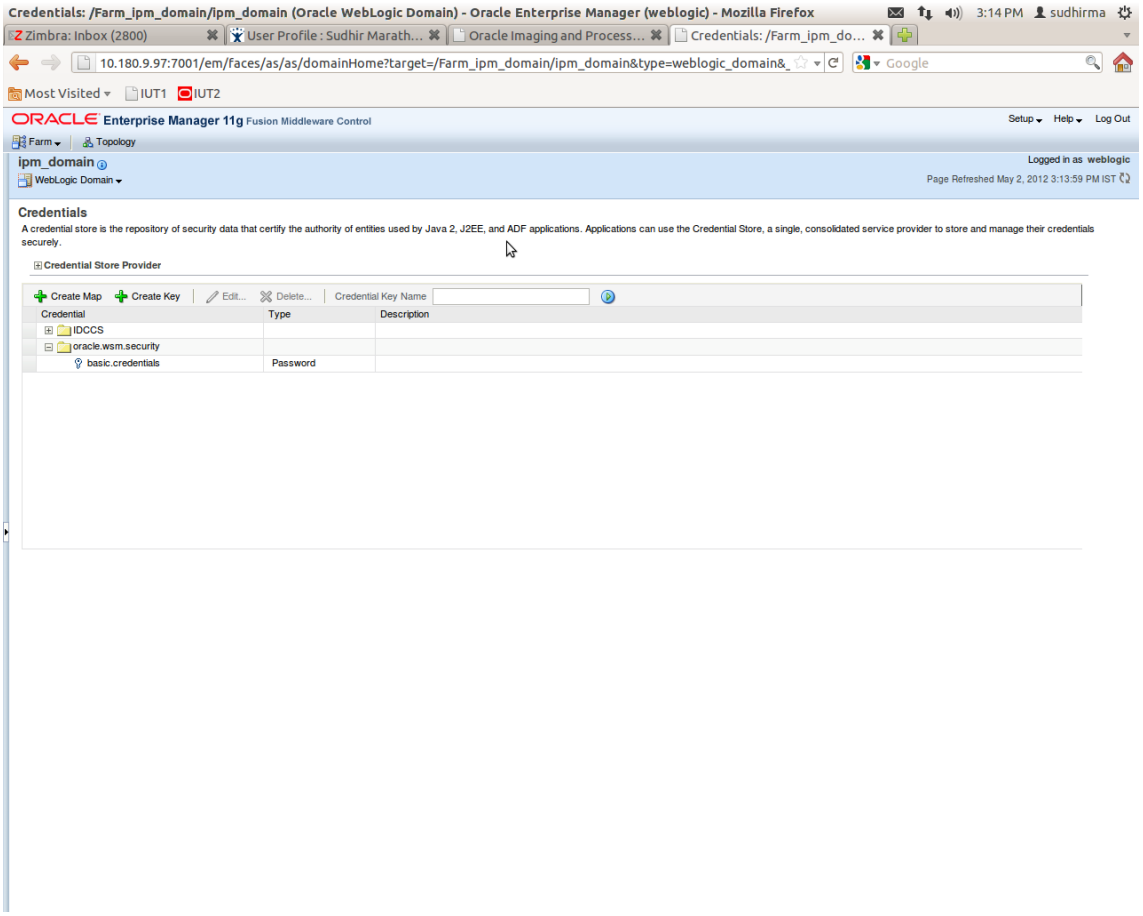
6. Click **Create Key** to create a key under the map **oracle.wsm.security.**

Figure 8–66 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 8–67 ipm_domain: Credentials Created

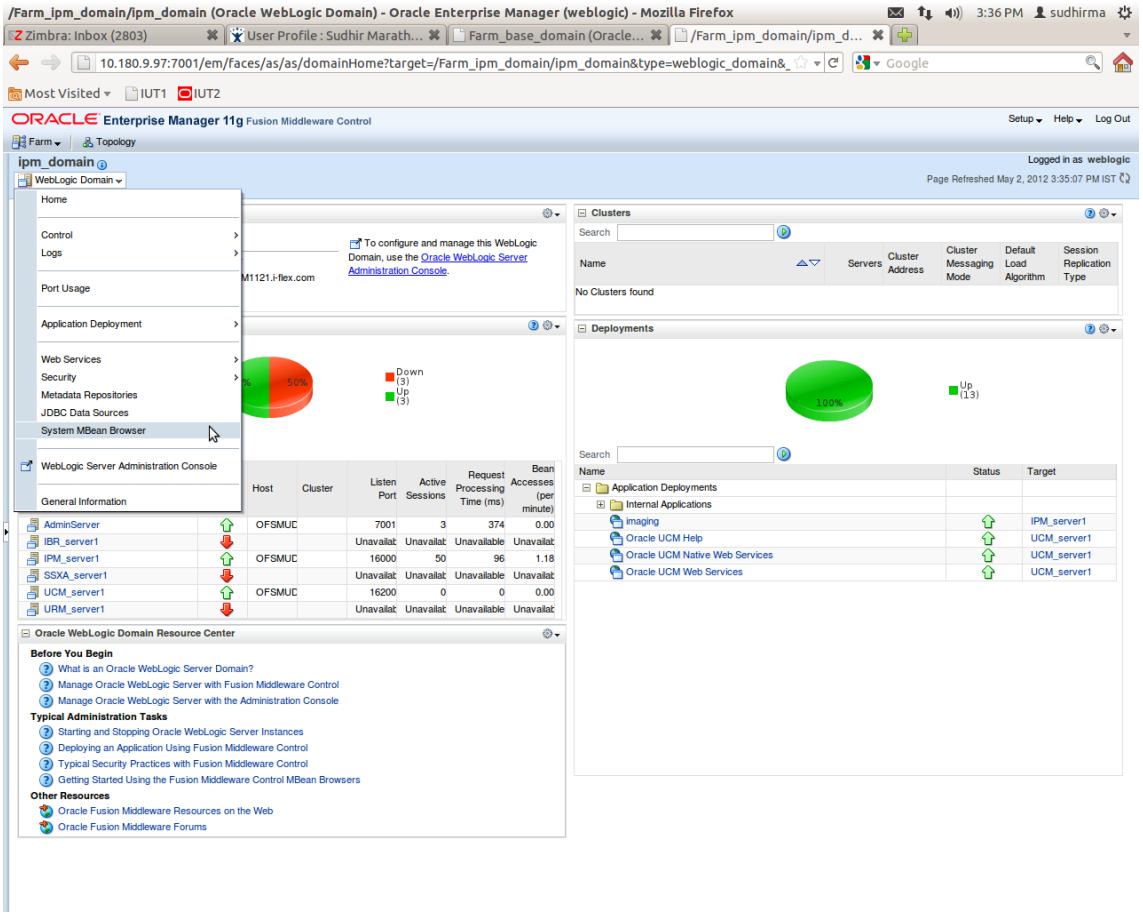


8.3.3 Setting up Input Agent Path

To set up input agent path:

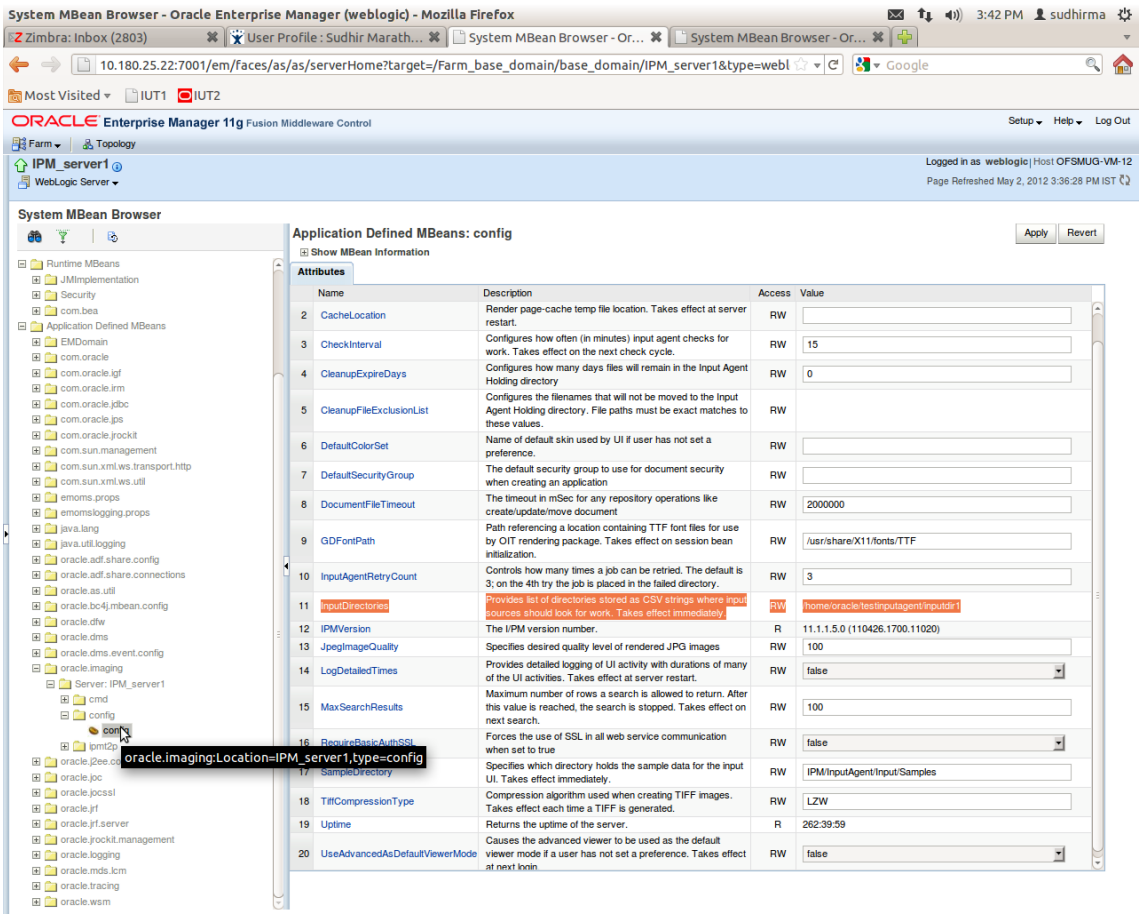
1. Log in to Enterprise Manager (EM) console.
2. In the Fusion Middleware section, under Weblogic domain, click **ipm domain**.
3. In the top menu, click Weblogic Domain. The corresponding menu appears.
4. Navigate to the domain System MBean Browser. The System MBean Browser page appears.

Figure 8–68 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 8–69 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

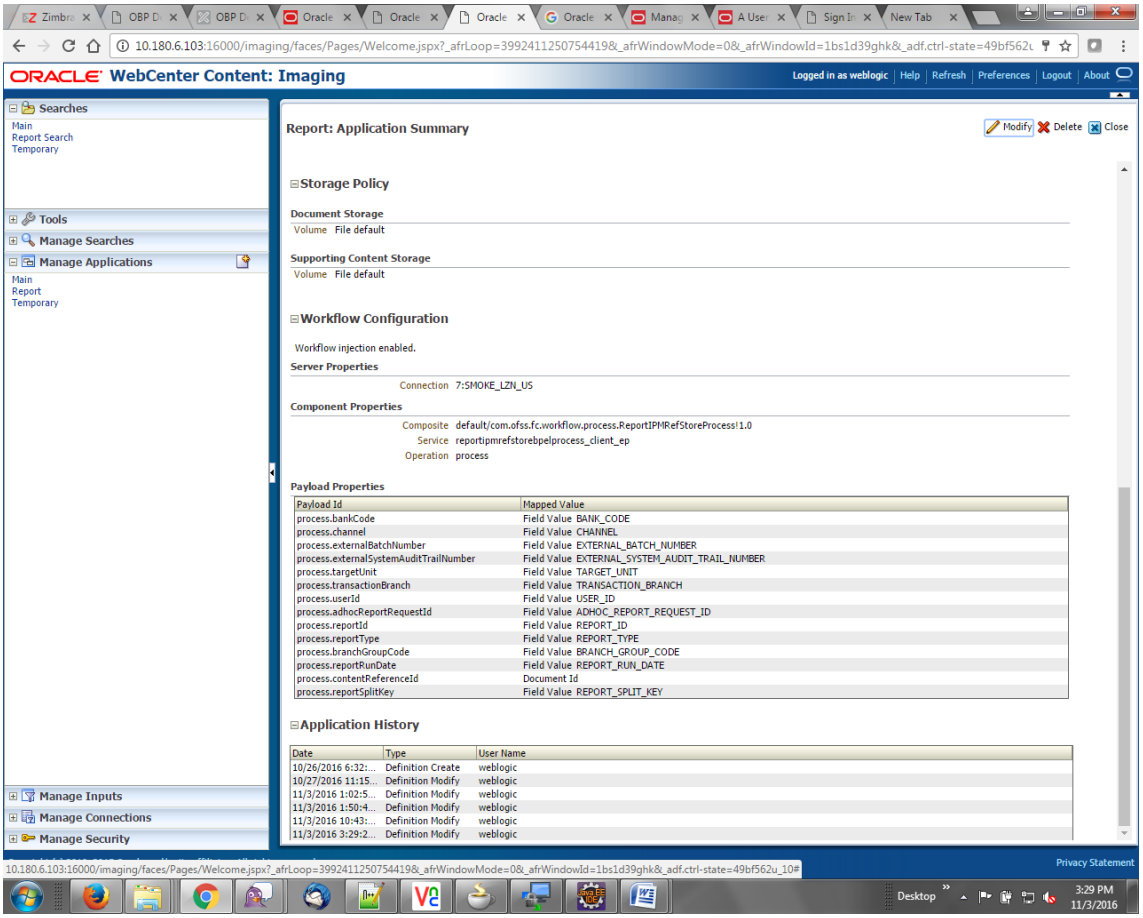
8. Restart IPM server.

8.3.4 Create SOA Connection

To create a SOA Connection:

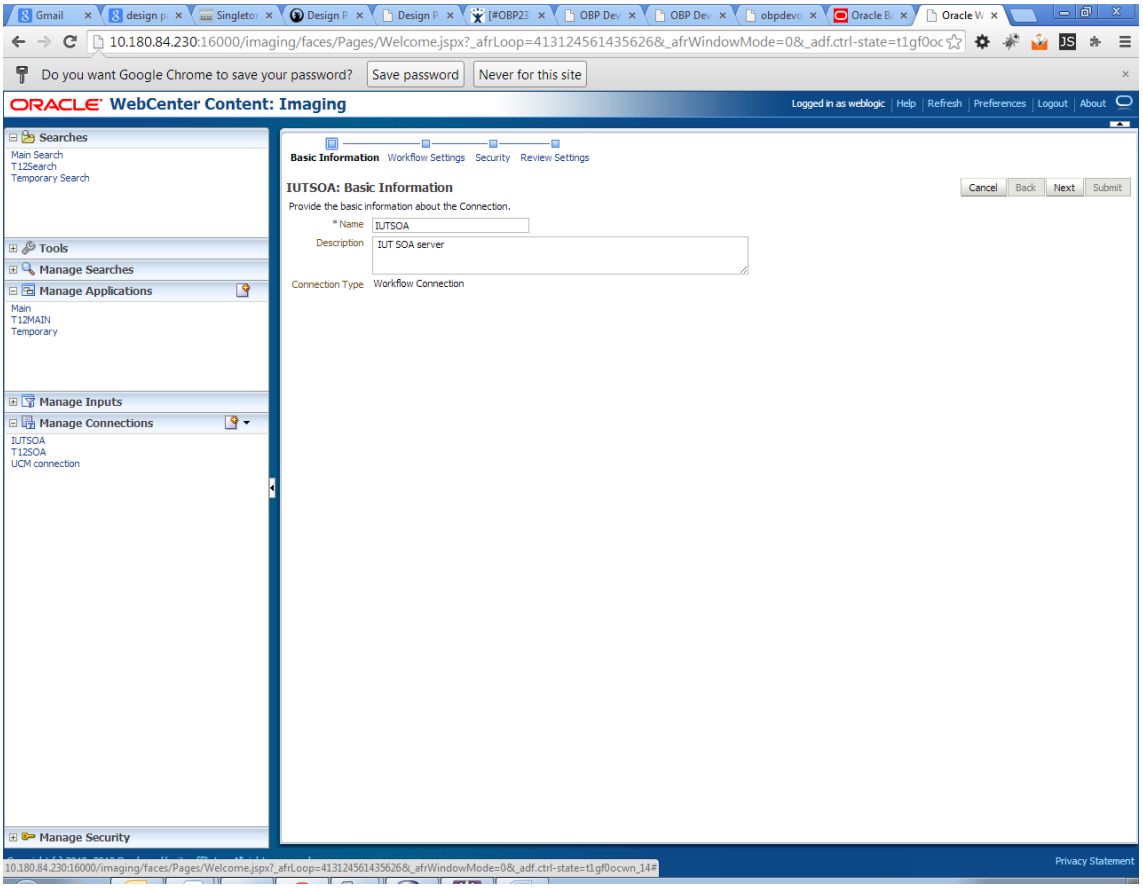
1. Log in to Image Processing Management (IPM).
2. Navigate to the Manage Connections section.

Figure 8–70 Manage Connections: Create Workflow Connection



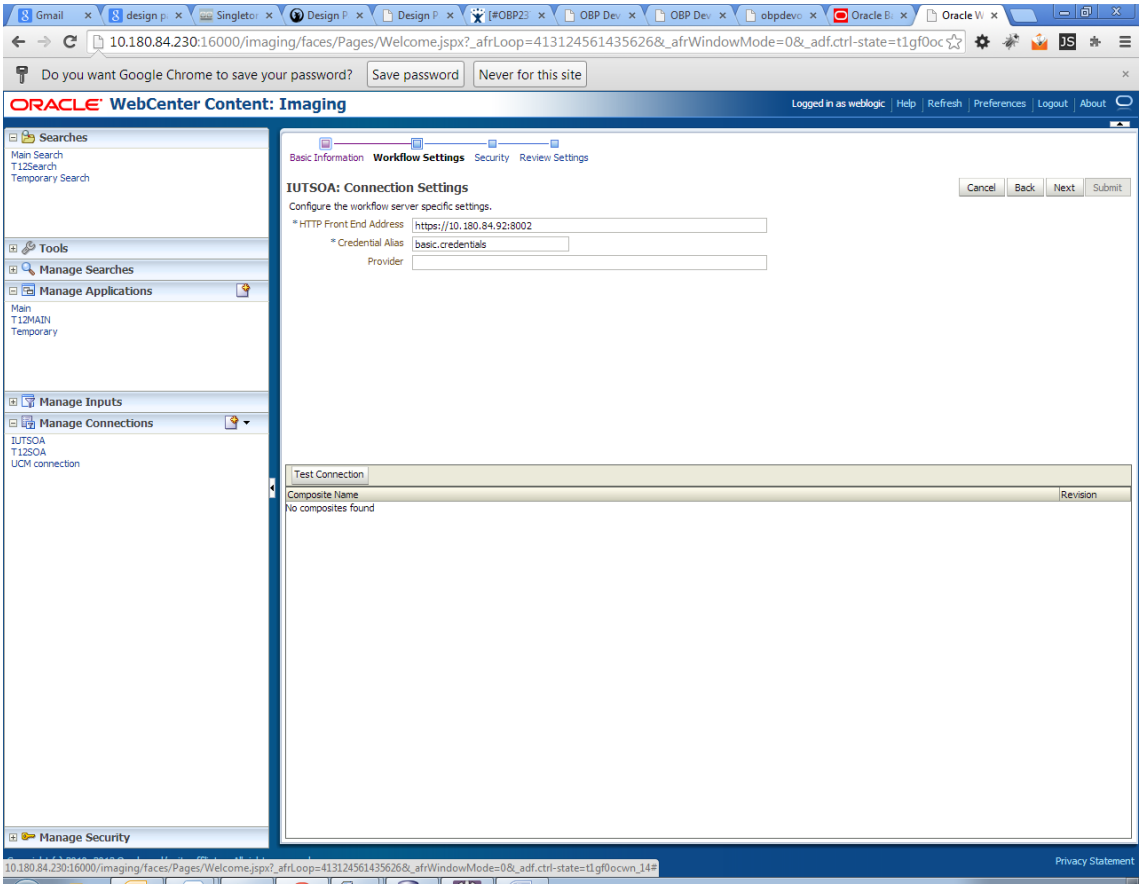
3. Click **Create Workflow Connection.**
4. In the **Name** field, enter the name for SOA Connection as IUTSOA.

Figure 8–71 IUTSOA: Basic Information



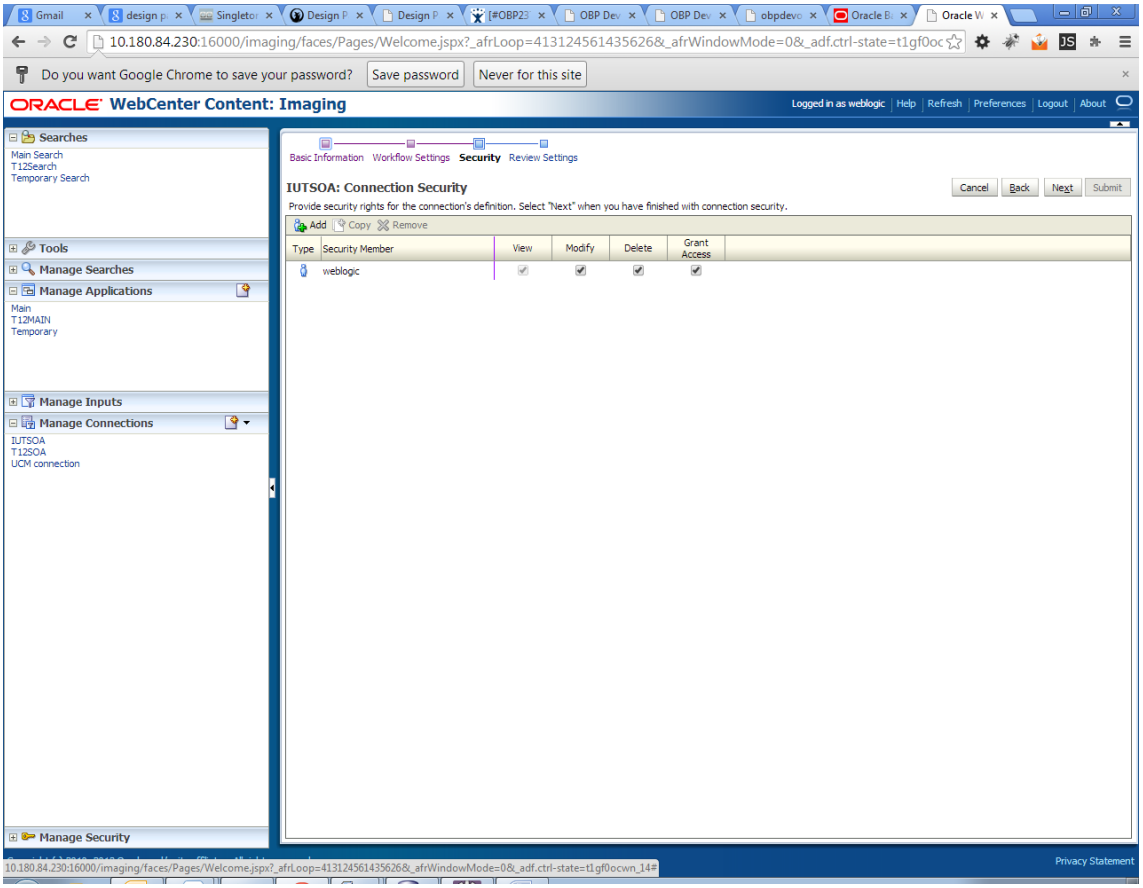
5. In the **HTTP Front End Address** field, enter the value for SOA server.

Figure 8–72 IUTSOA: Workflow Settings



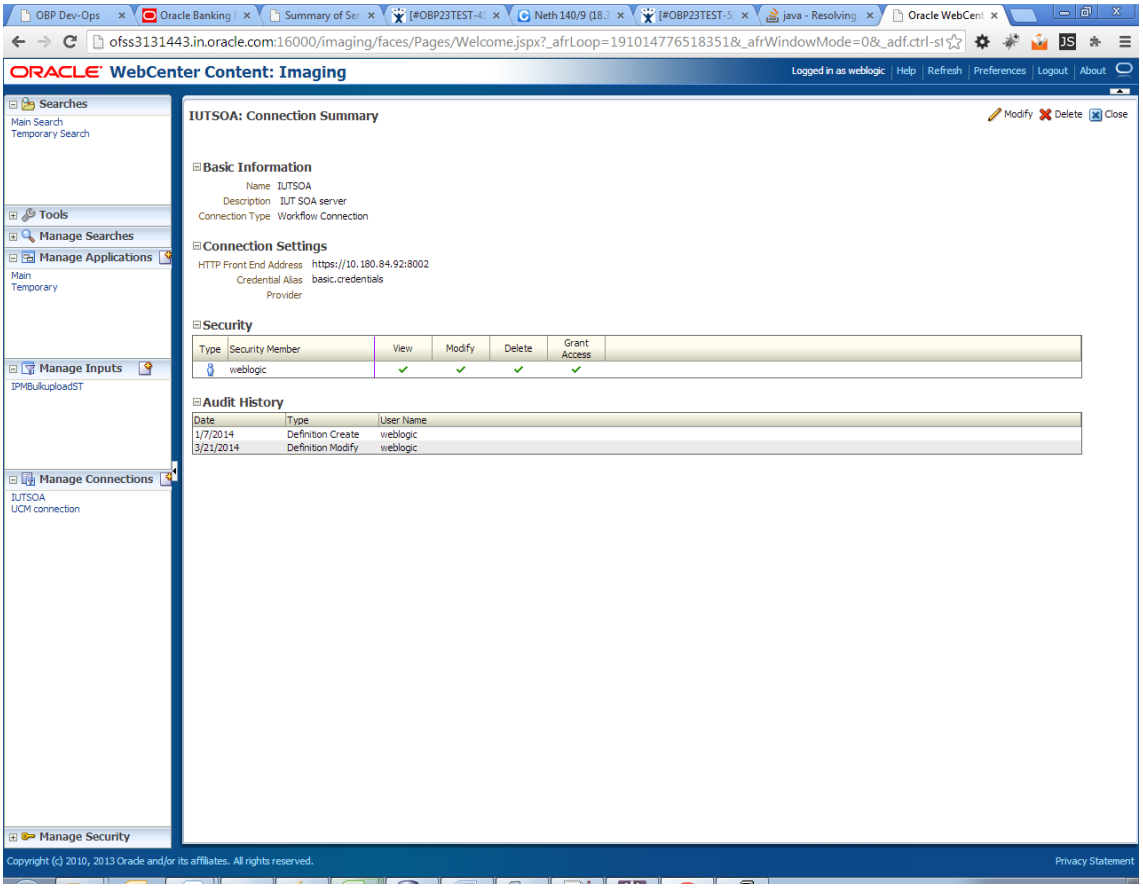
6. In the **Credential Alias** field, enter the value as basic.credentials.
7. Click **Next** to proceed. The Connection Security page appears.

Figure 8–73 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.

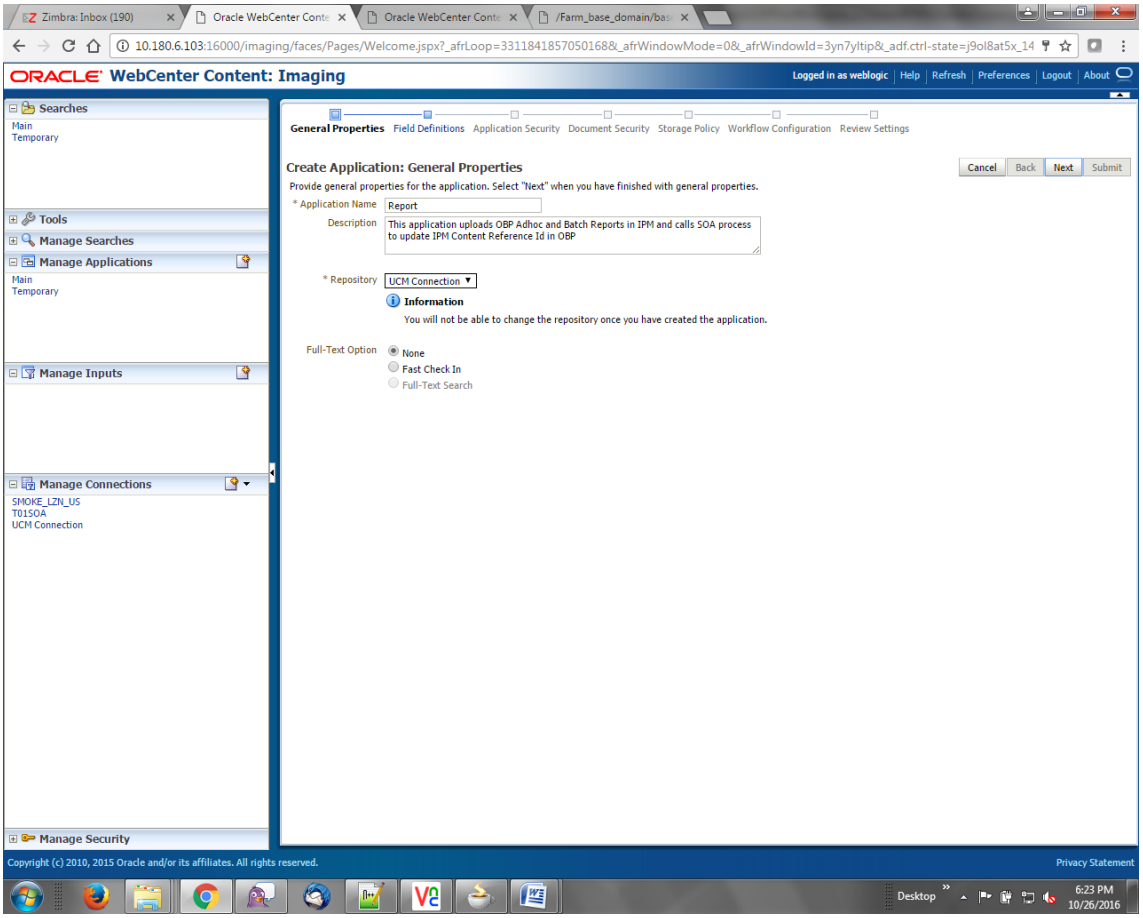
Figure 8–74 IUTSOA: Review Settings



8.3.5 Manage Application Configuration

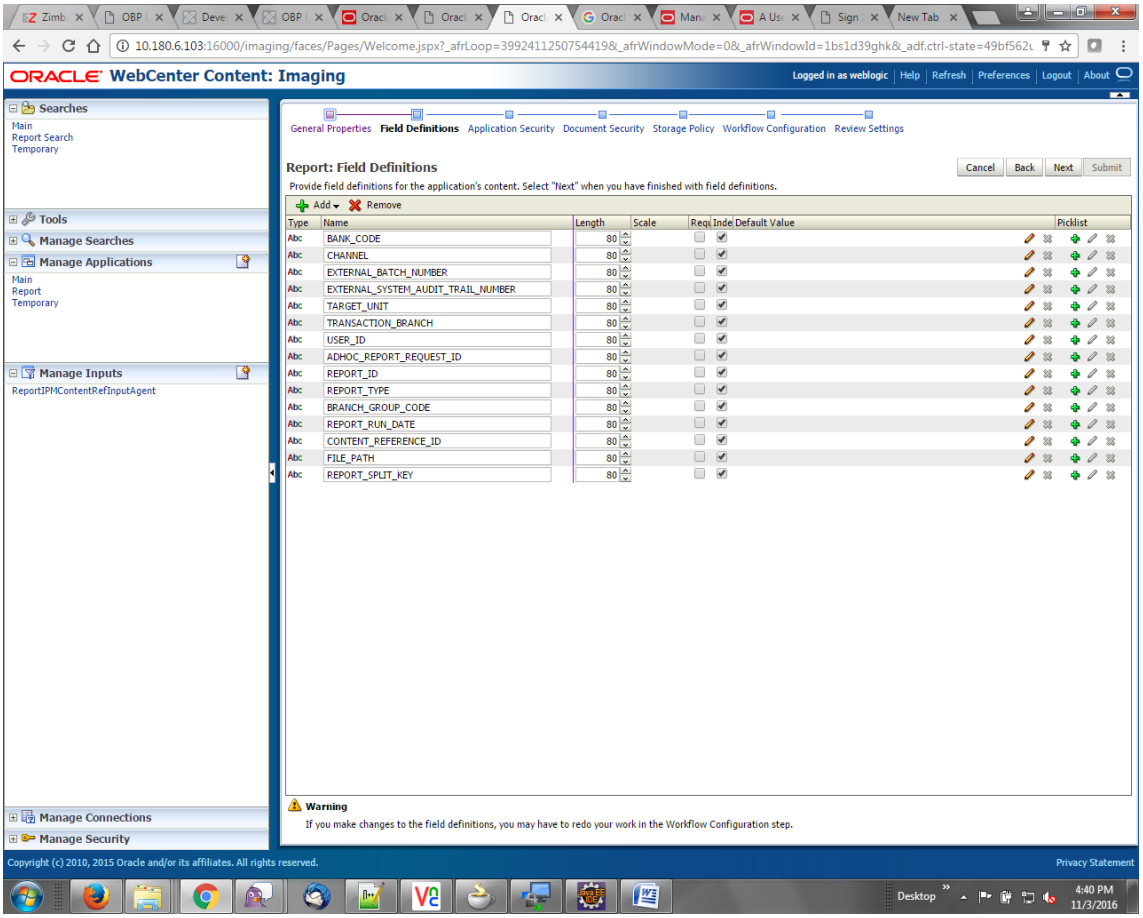
1. Navigate to the Manage Applications section.
2. Select Create New Application option. The Create Application: General Properties page appears.

Figure 8–75 Create Application: General Properties



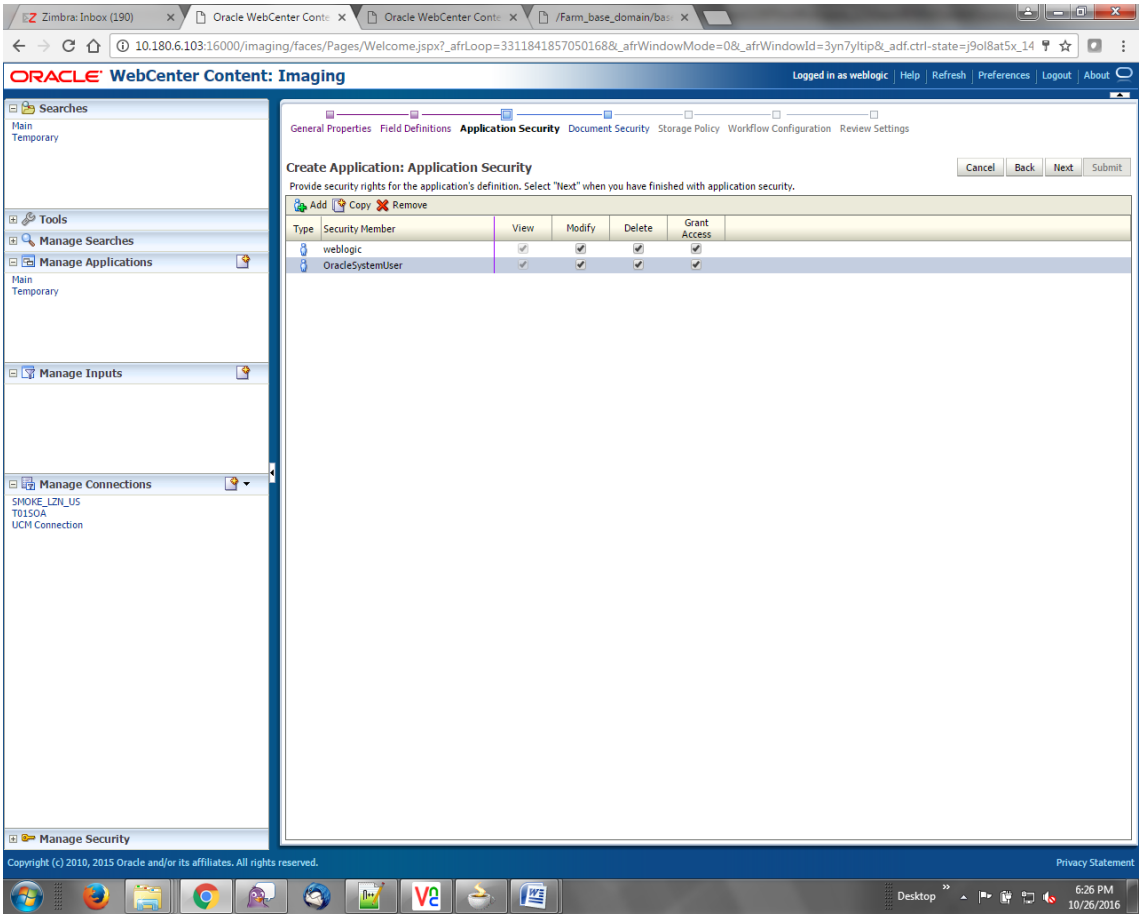
3. Enter the general properties for the application and click **Next.** The Report: Field Definitions page appears.

Figure 8–76 Report: Field Definitions



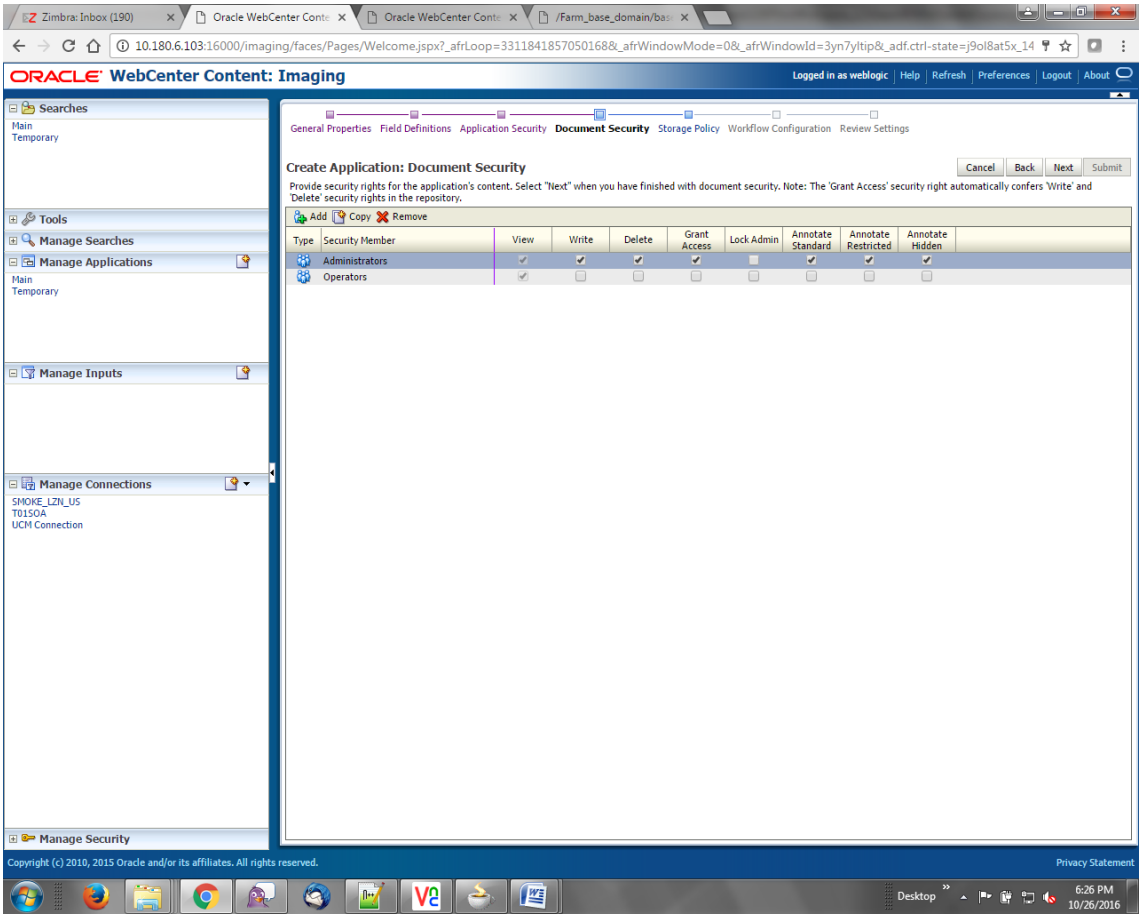
4. Enter the field definition details and click **Next.** The Create Application: Applications Security page appears.

Figure 8–77 Create Application: Applications Security



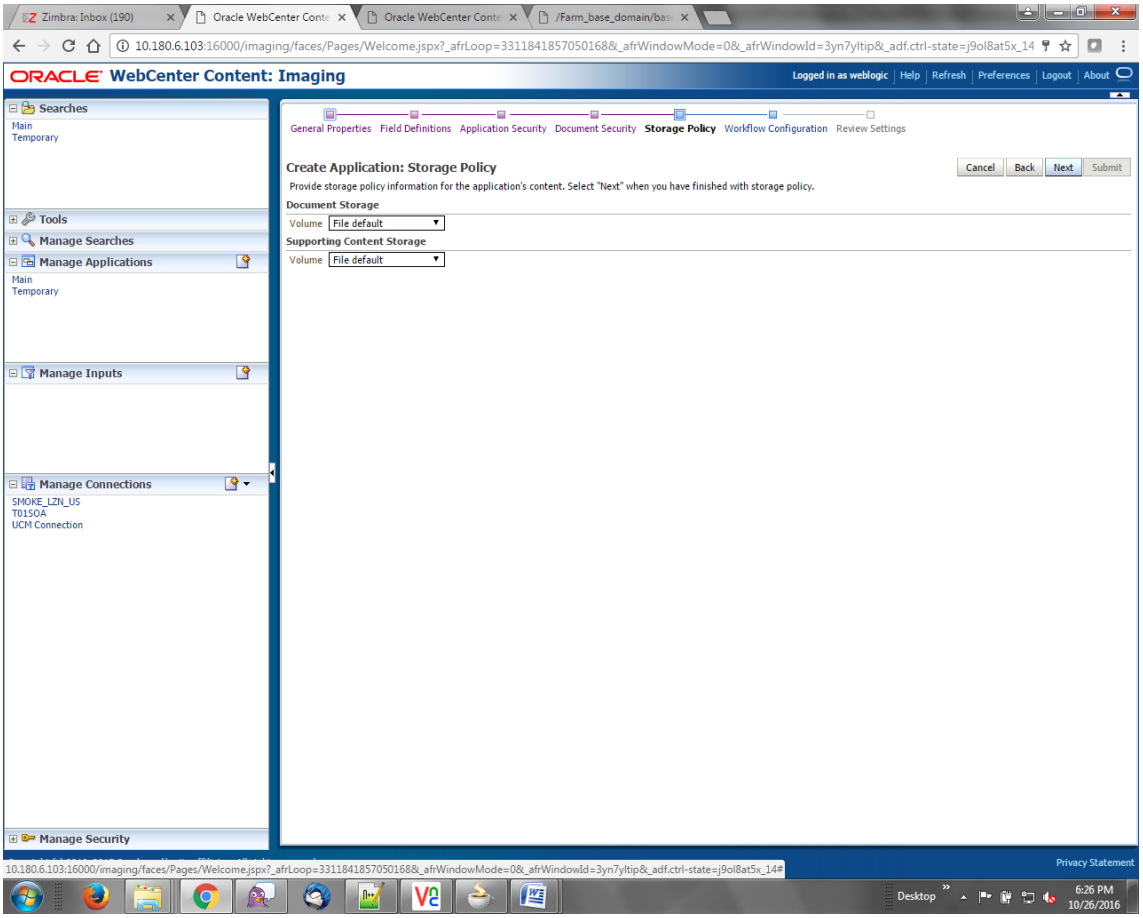
5. In the Application Security section, select the access rights for users and click **Next.** The Create Application: Document Security page appears.

Figure 8–78 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 8–79 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 8–80 Report: Workflow Configuration - Server Properties

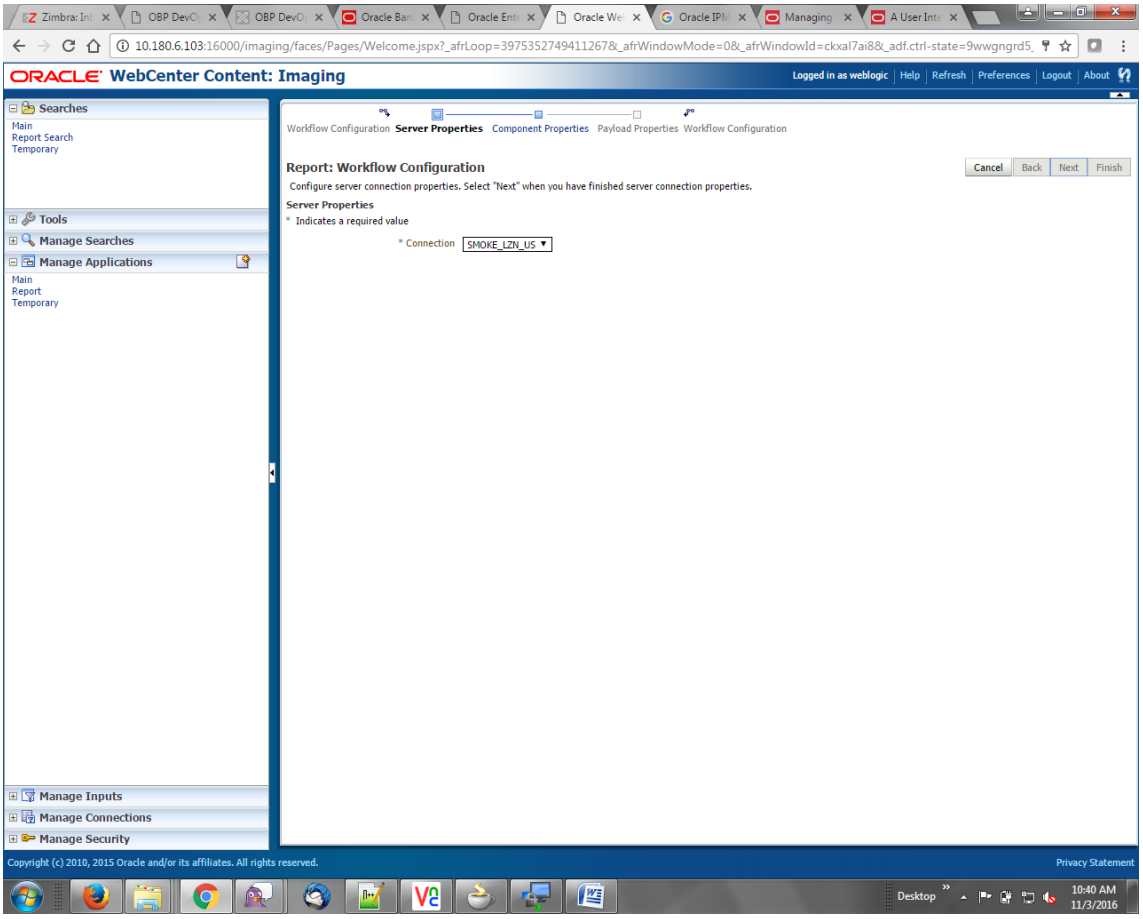


Figure 8–81 Report: Workflow Configuration - Component Properties

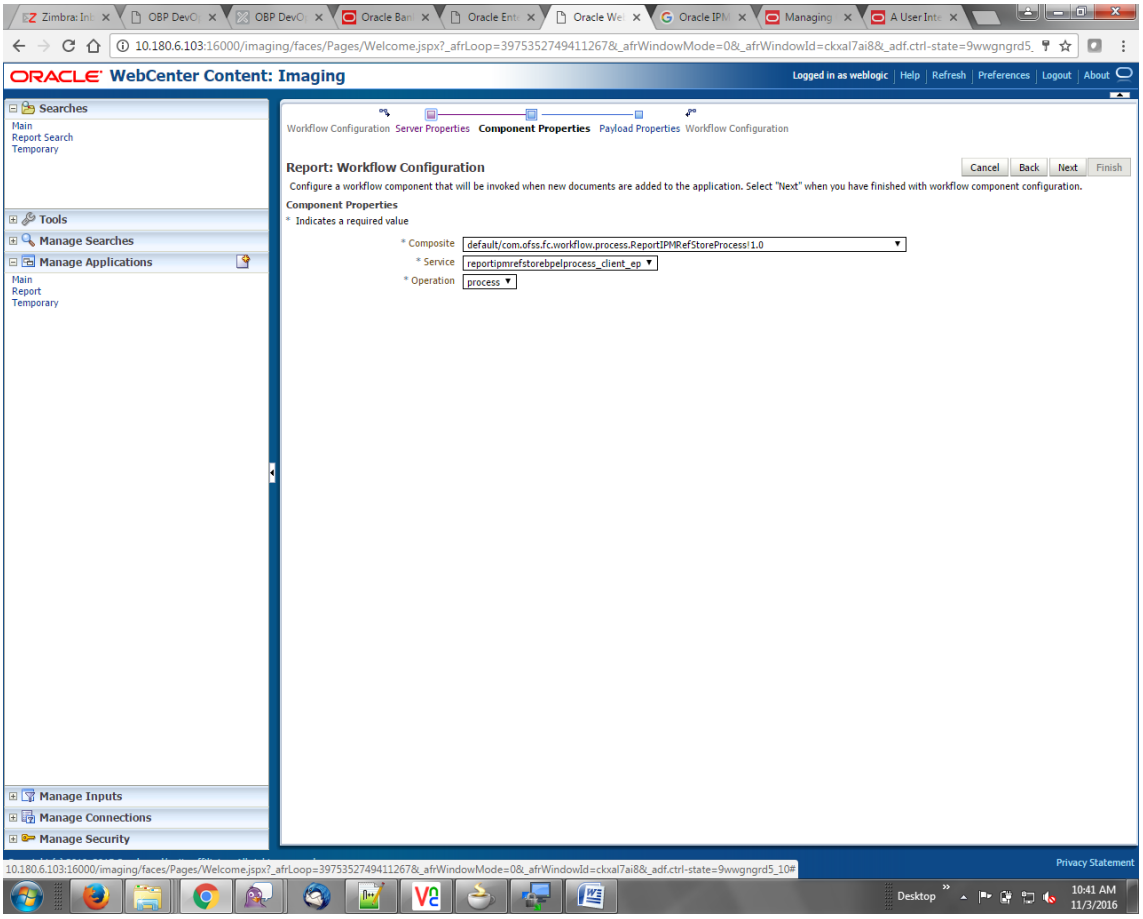
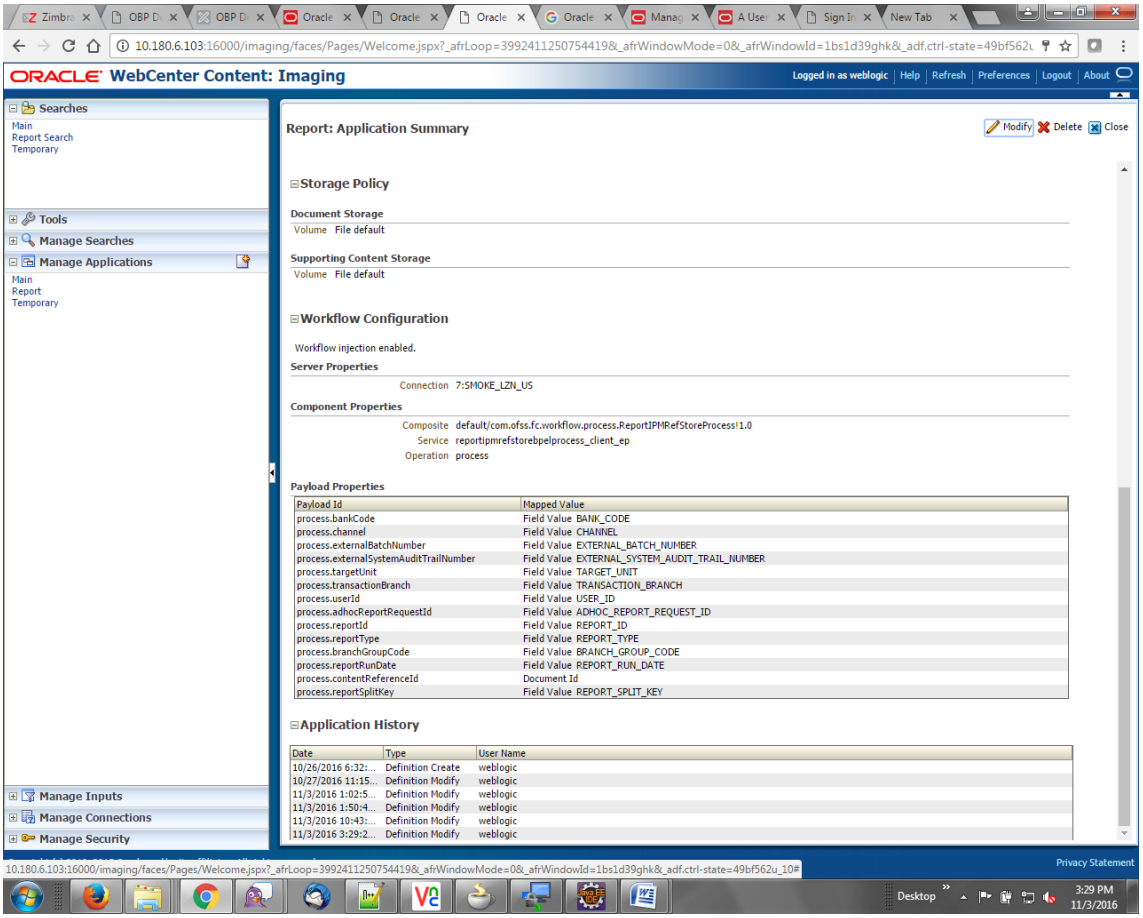
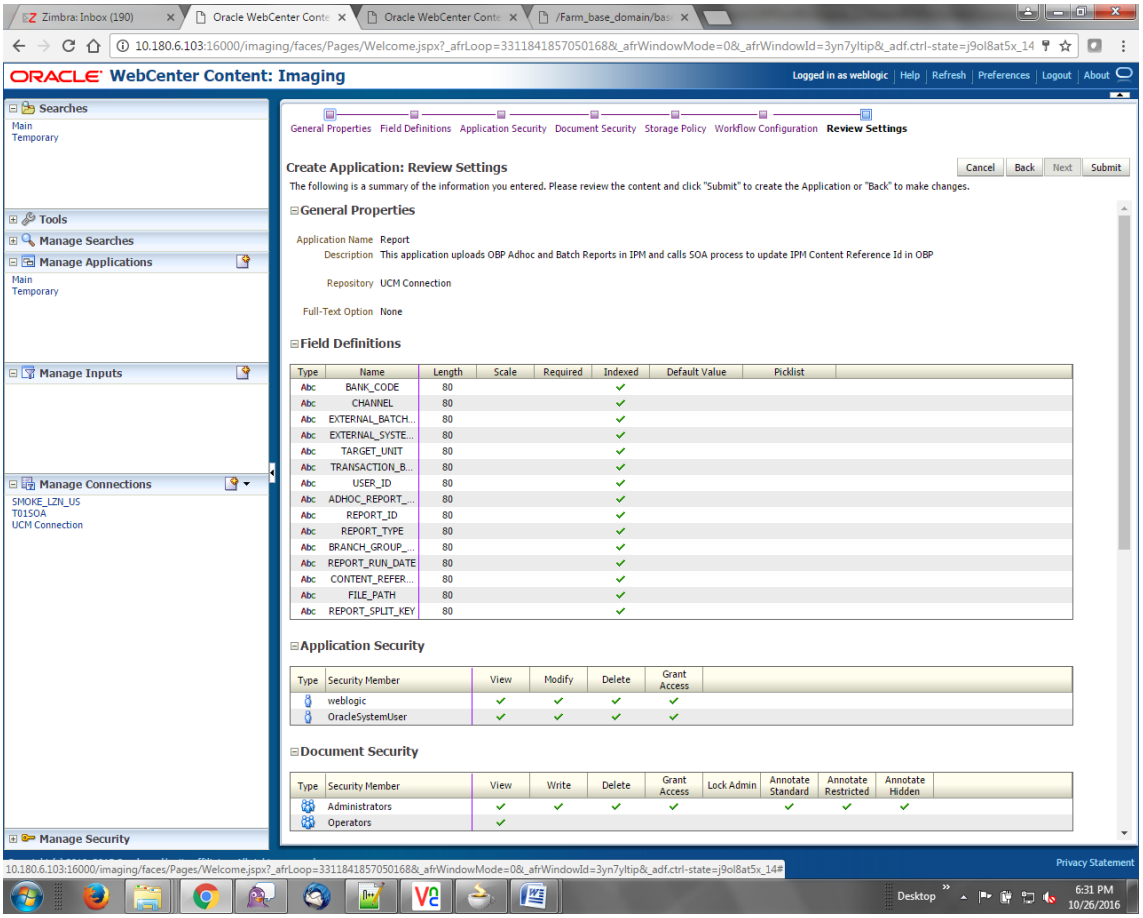


Figure 8–82 Report: Application Summary



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

Figure 8–83 Create Application: Review Settings

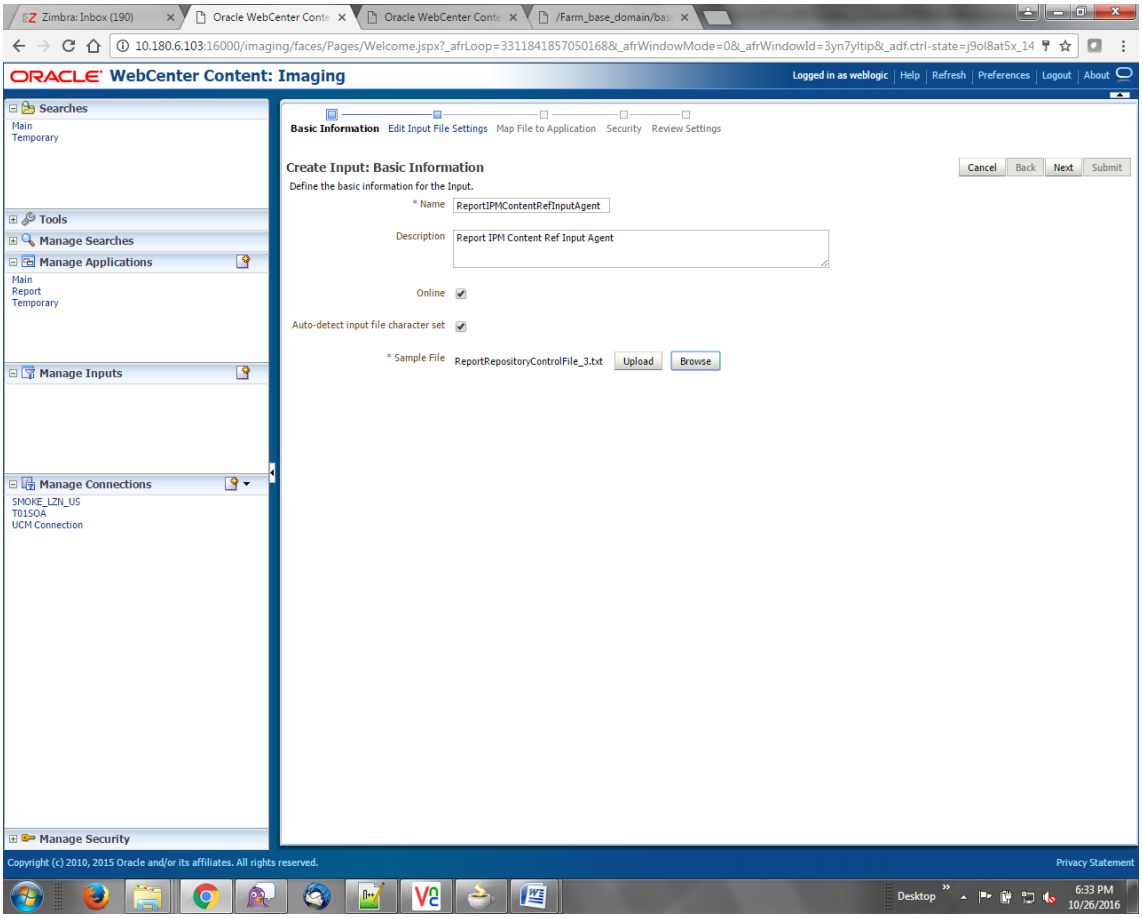


8.3.6 Manage Inputs for Input Agents

To manage workflow configuration:

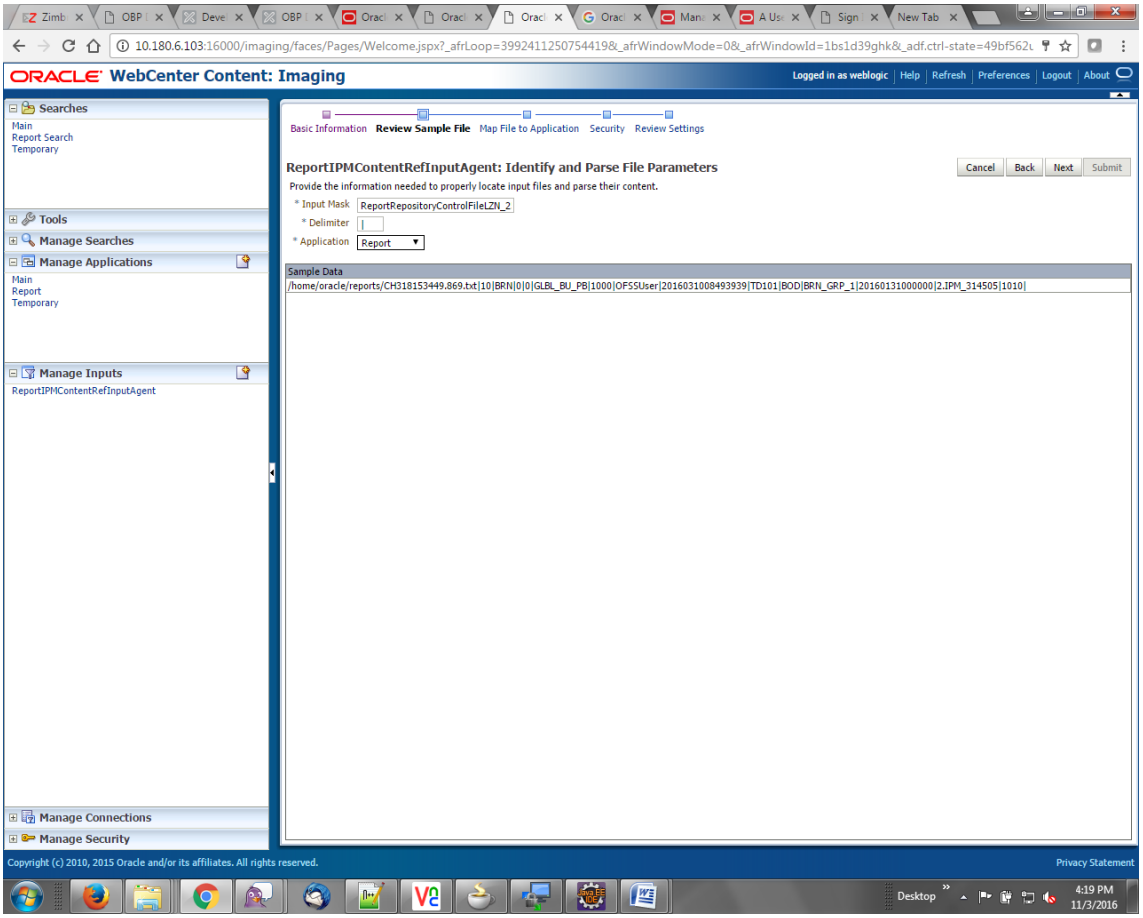
1. Log in to Image Processing Management (IPM).
2. Navigate to Manage Inputs section.

Figure 8–84 Manage Inputs



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

Figure 8–85 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

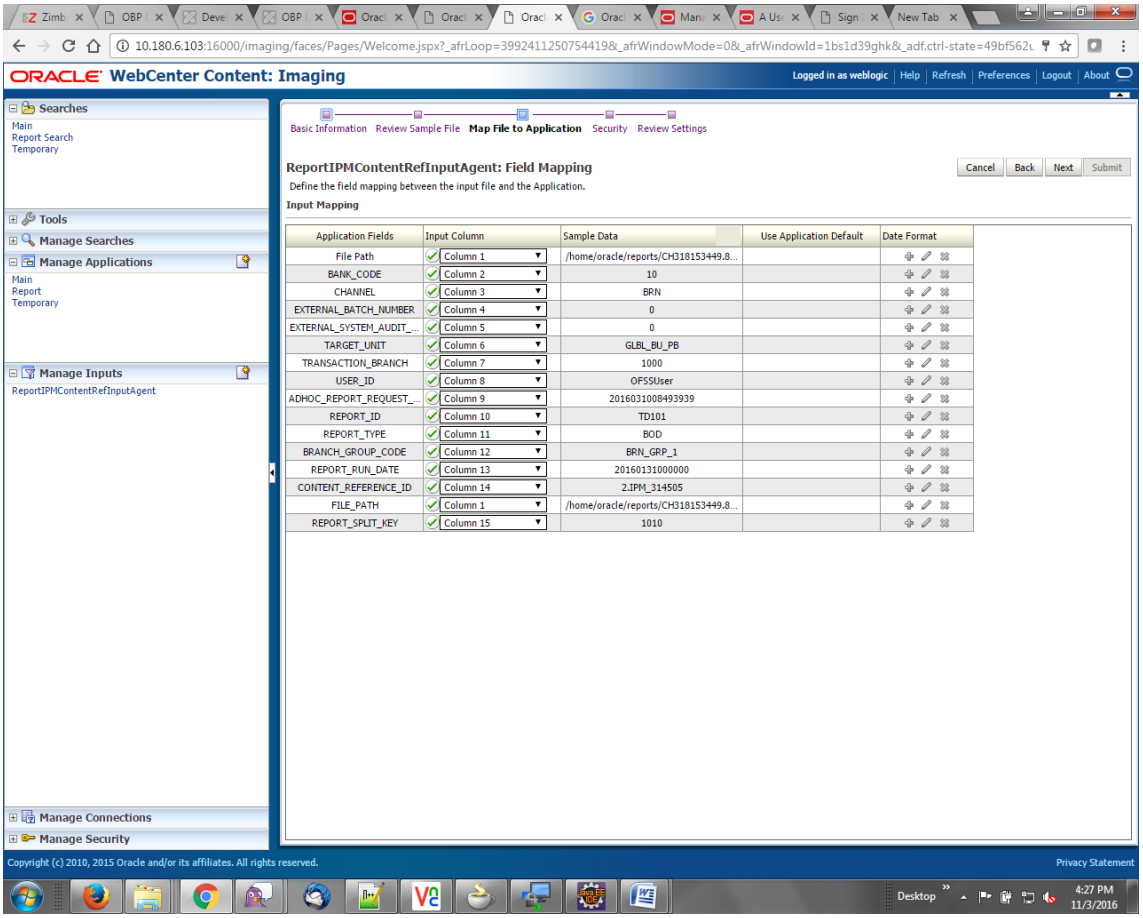
   select prop_value from flx_fw_config_var_b where prop_id = env.name;

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.

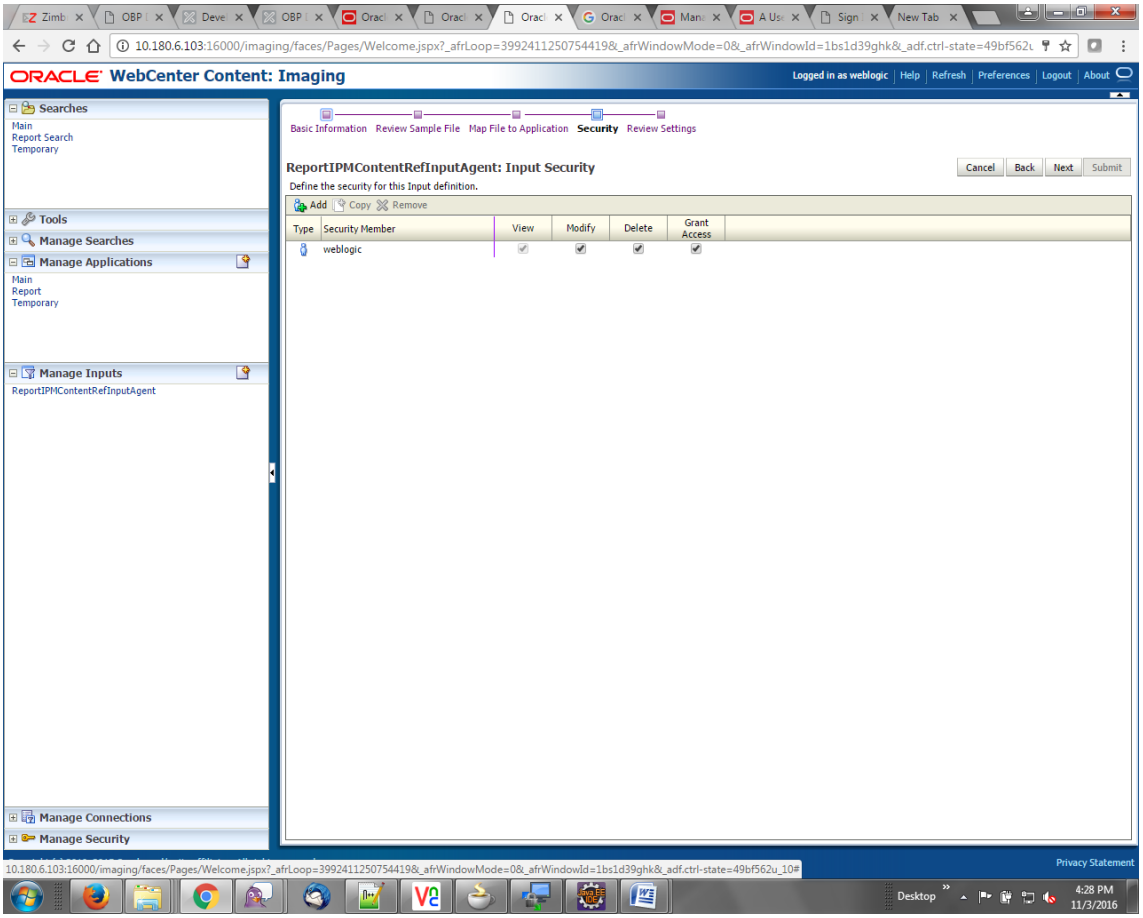
7. In the **Delimeter** field, enter the delimiter value as | (vertical bar character).
8. From the **Application** field, select the application to which the input agent will be applied.

Figure 8–86 Input Agent Details: Field Mapping



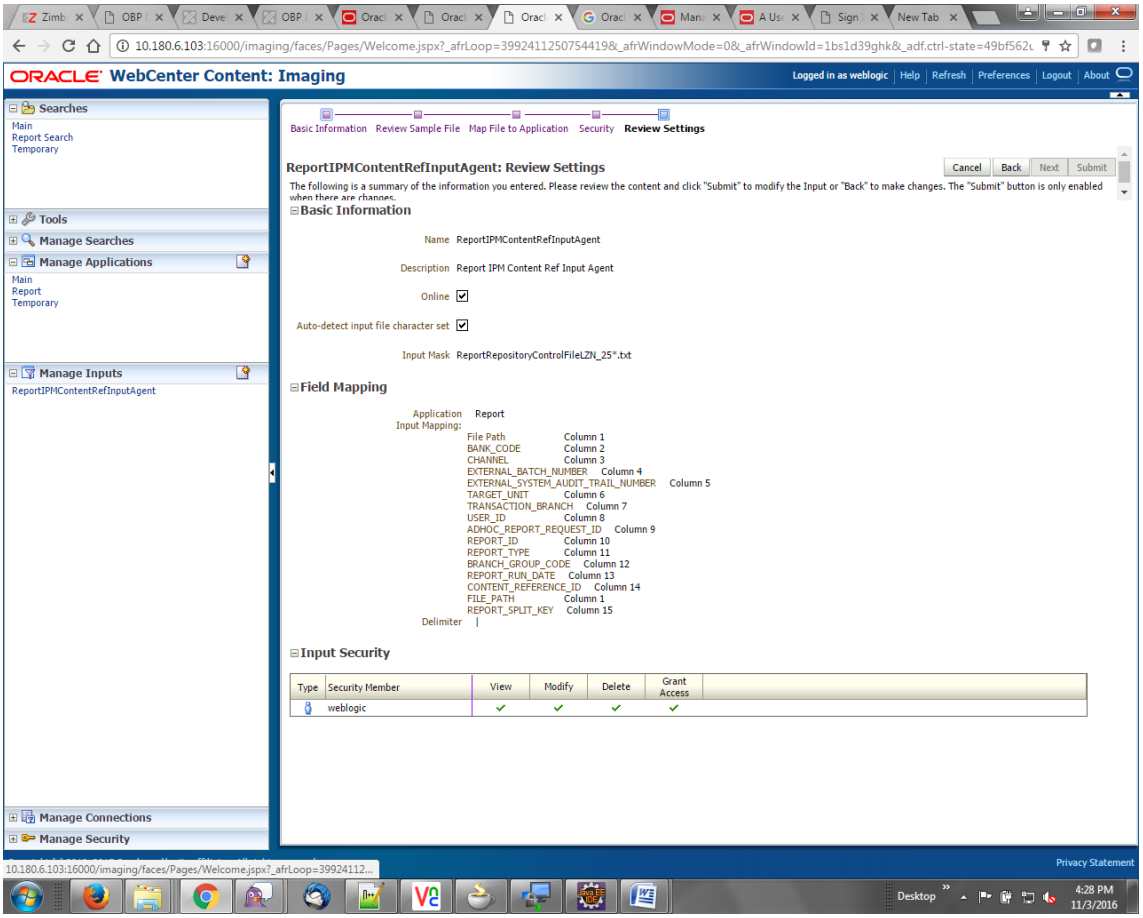
9. Select the access rights for user in the Security section and click **Next.**

Figure 8–87 Input Agent Details: Security



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

Figure 8–88 Input Agent Details: Review Settings



Note

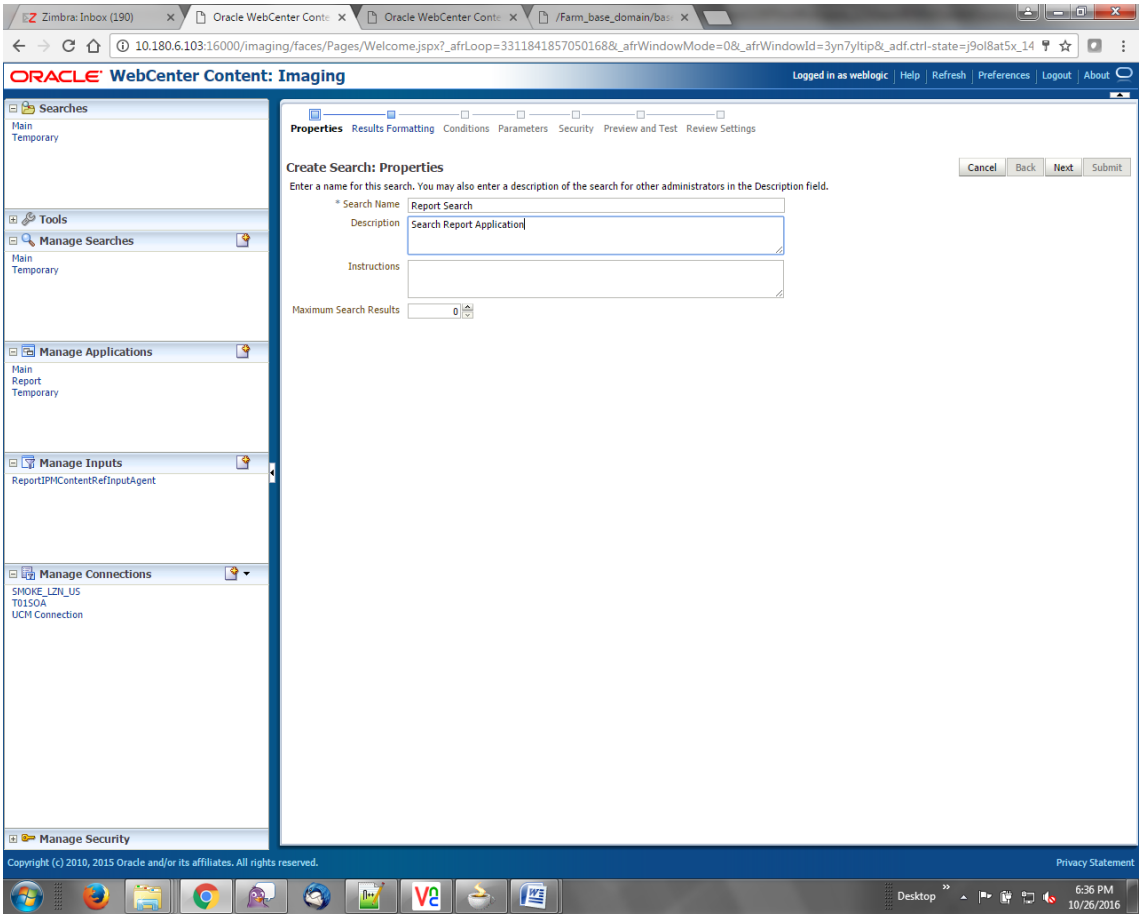
Do not forget to toggle online, else the input agent will not pick up any file for processing.

8.3.7 Manage Searches

To manage searches:

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

Figure 8–89 Create Search: Properties



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

Figure 8–90 Create Search: Results Formatting

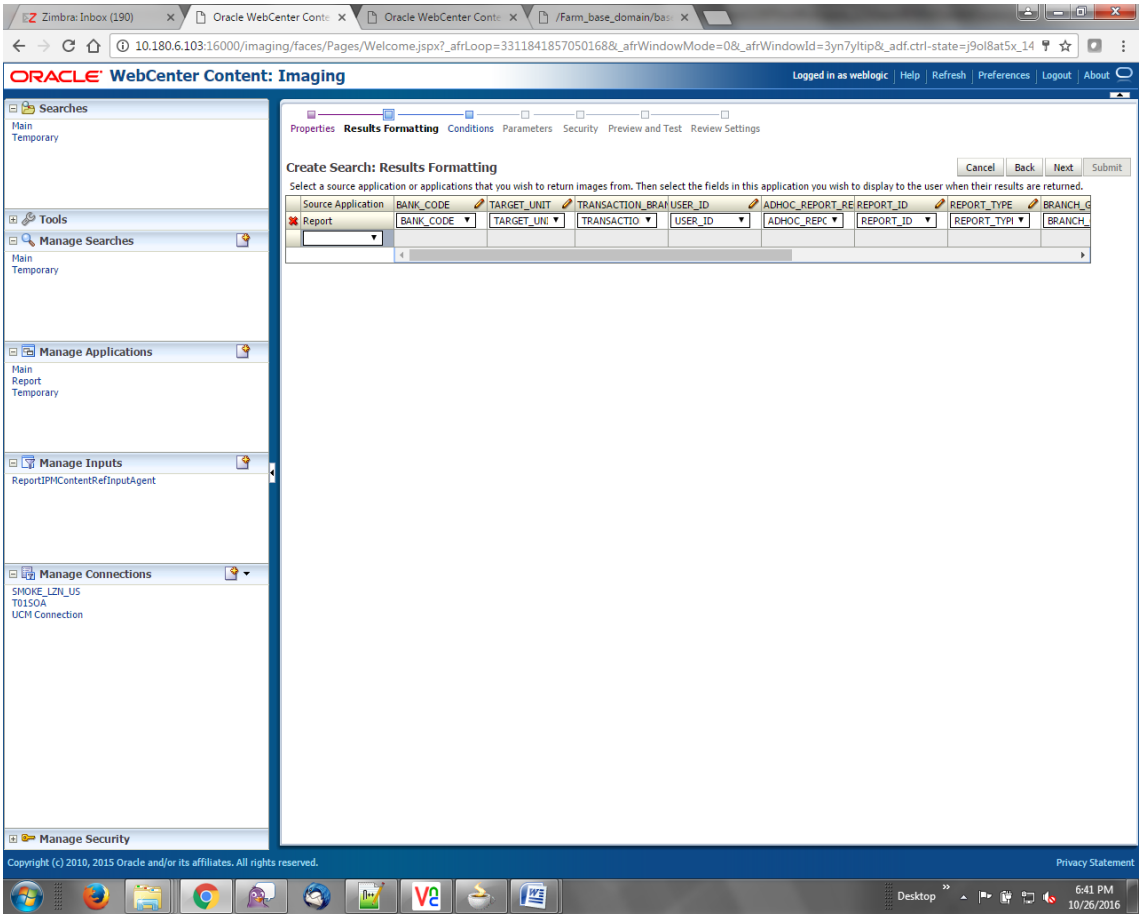


Figure 8–91 Create Search: Conditions

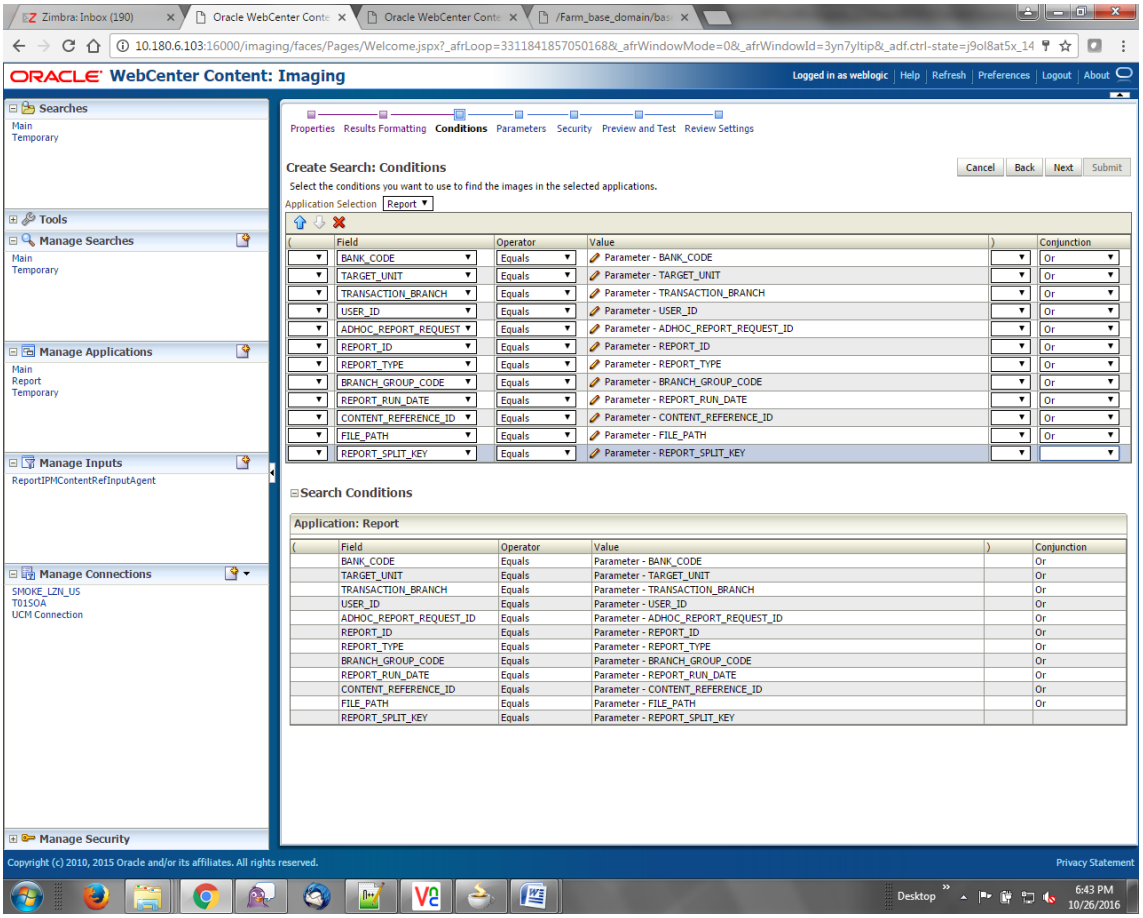
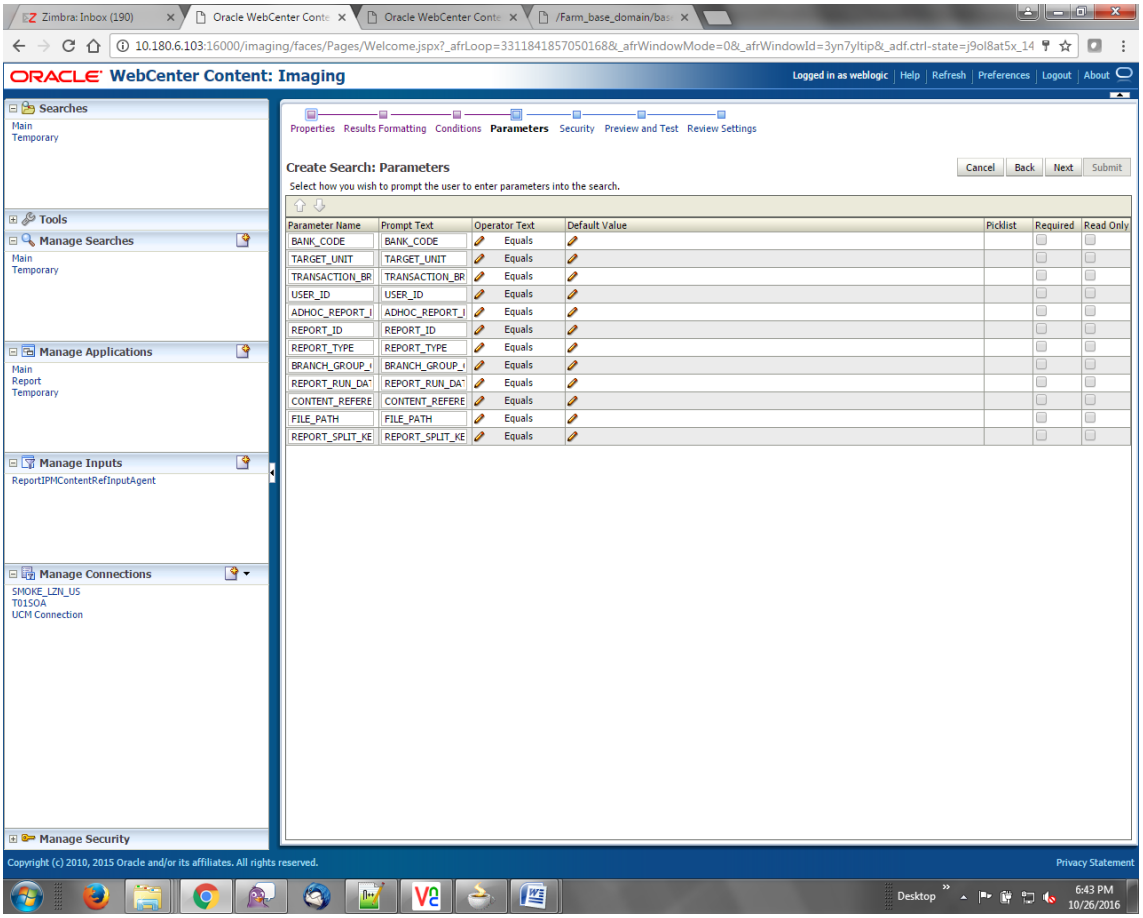
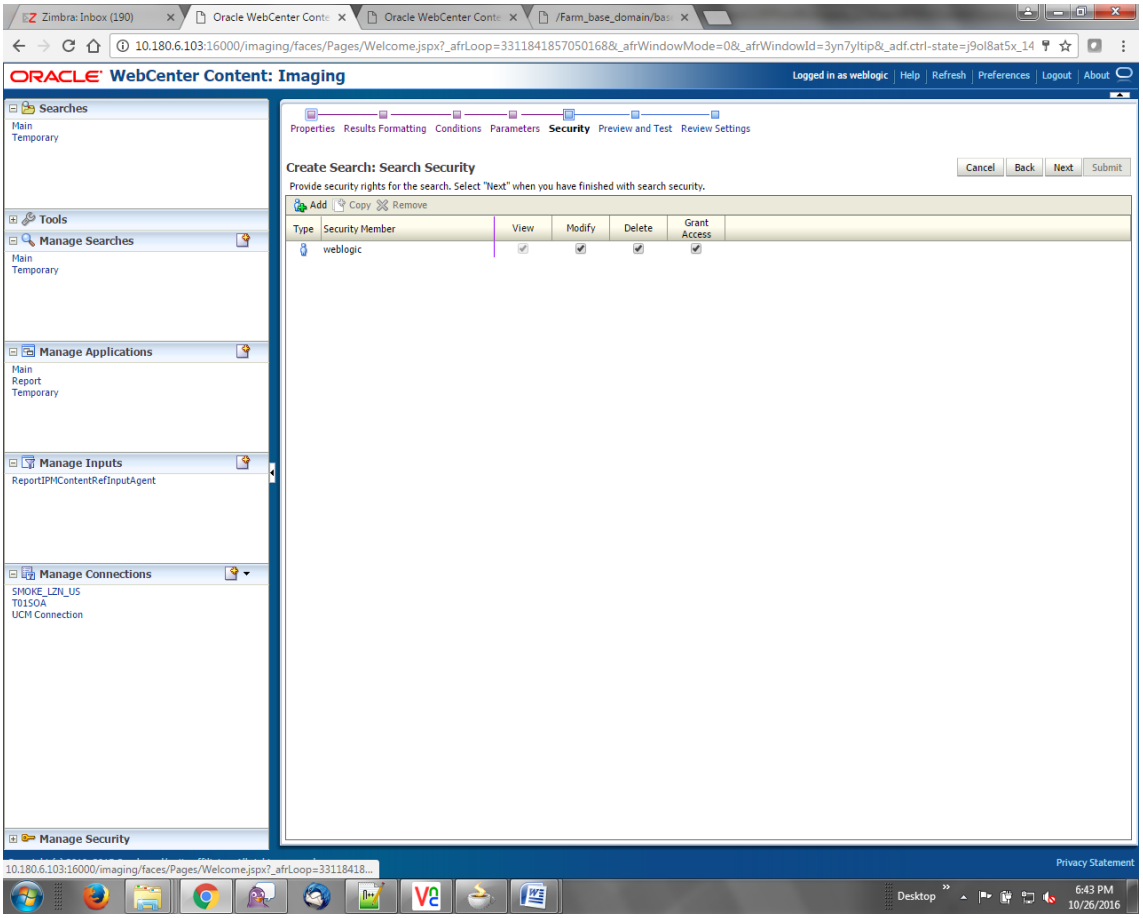


Figure 8–92 Create Search: Parameters



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

Figure 8–93 Create Search: Security



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

Figure 8–94 Create Search: Preview and Test

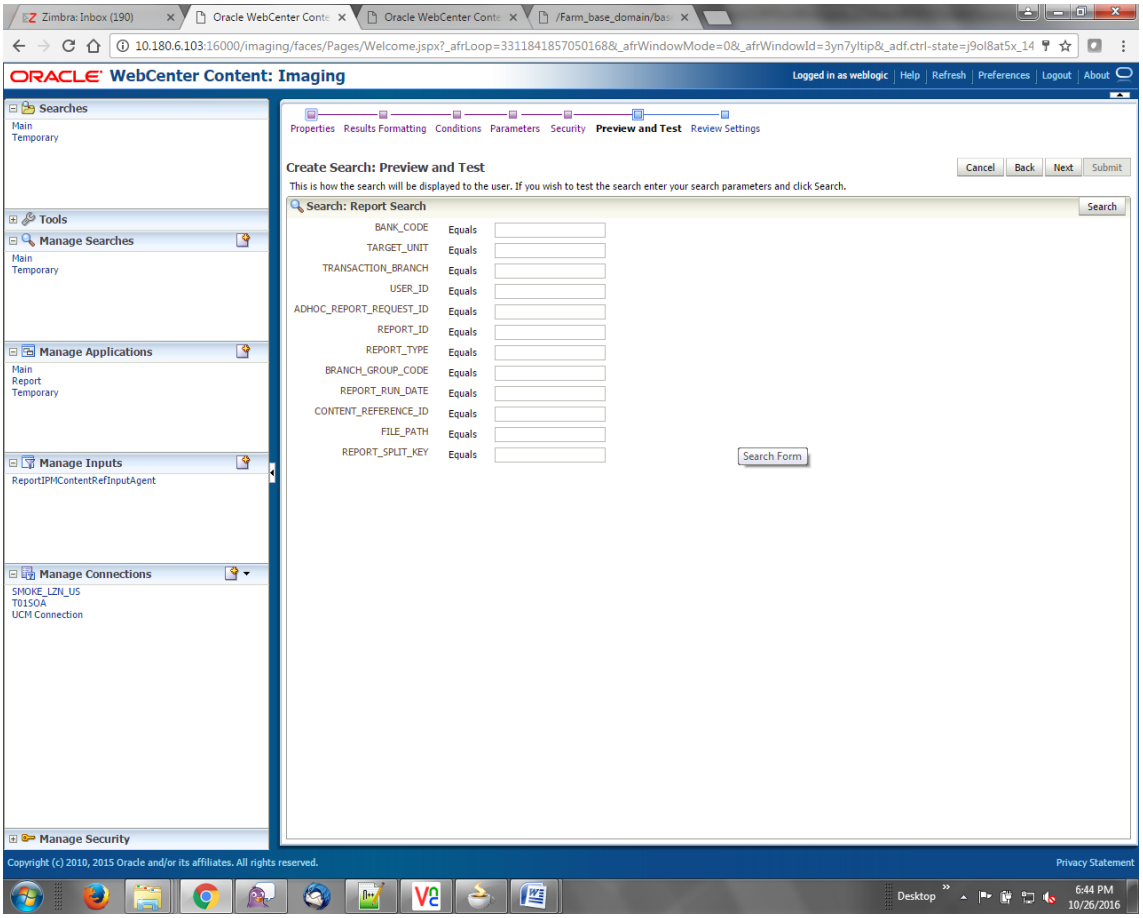
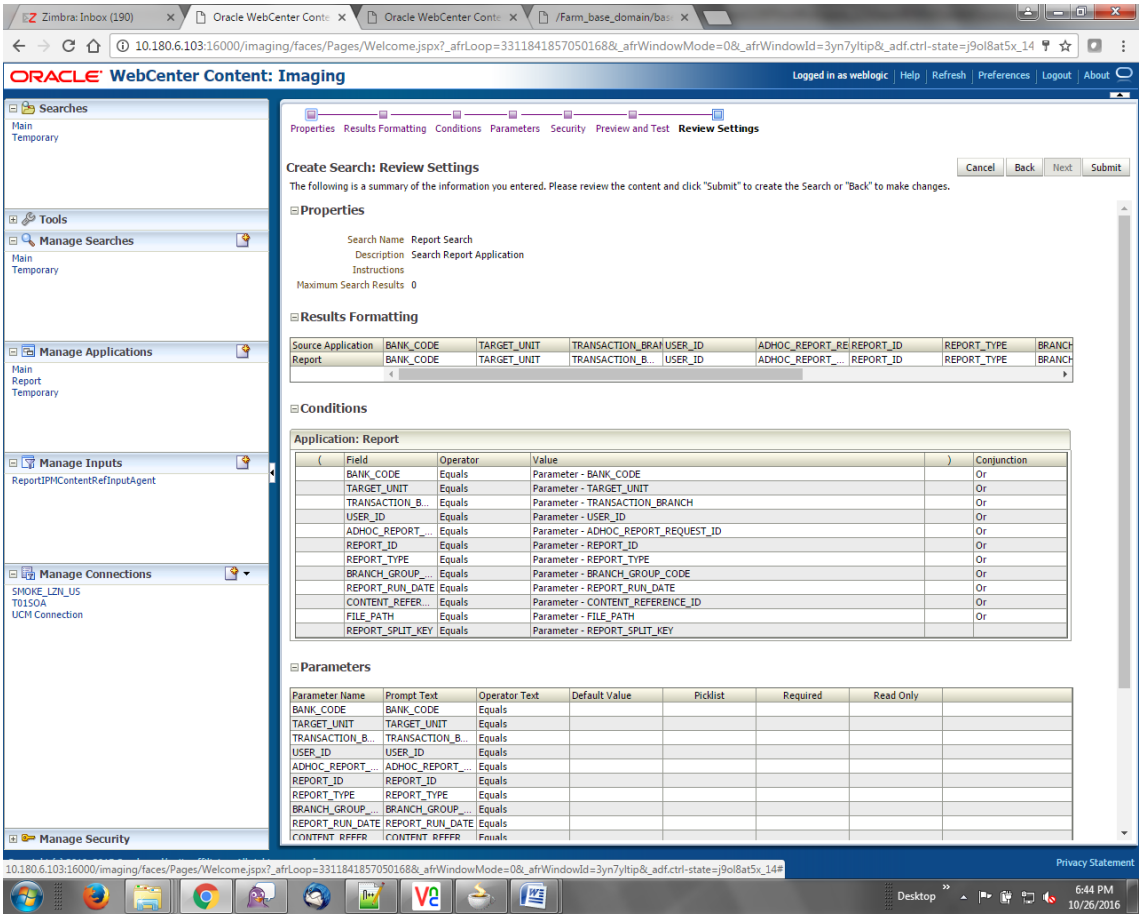


Figure 8–95 Create Search: Review Settings



8.3.8 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 8–2 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

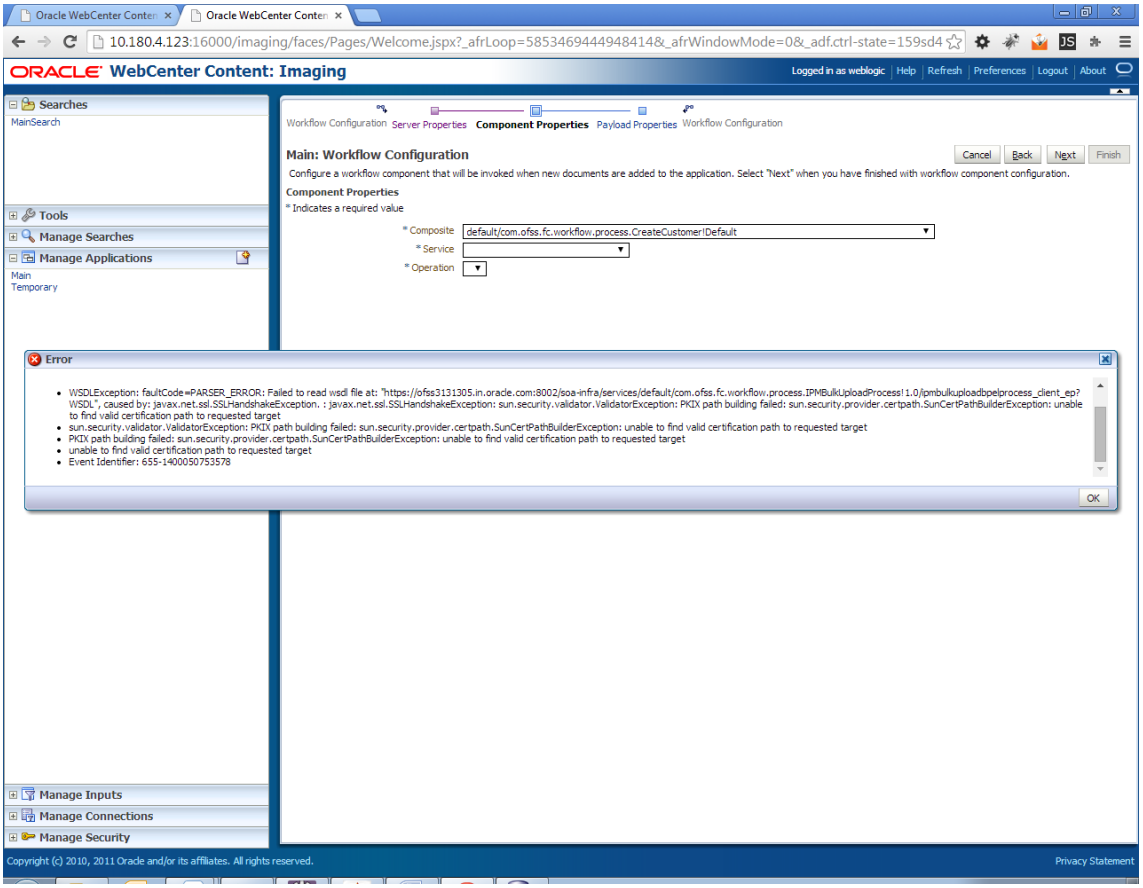
    c. Security policy for ReportIPMRefStoreProcess can been removed (if required).

        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 8–96 Component Properties



9 OAS (BIP) Datasource Creation

This chapter explains the steps required for Oracle Analytics Server (OAS) (formerly known as BIP or Business Intelligence Publisher) datasource creation.

9.1 OAS (BIP) Datasource Creation

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

Follow the below mentioned steps to create the datasource:

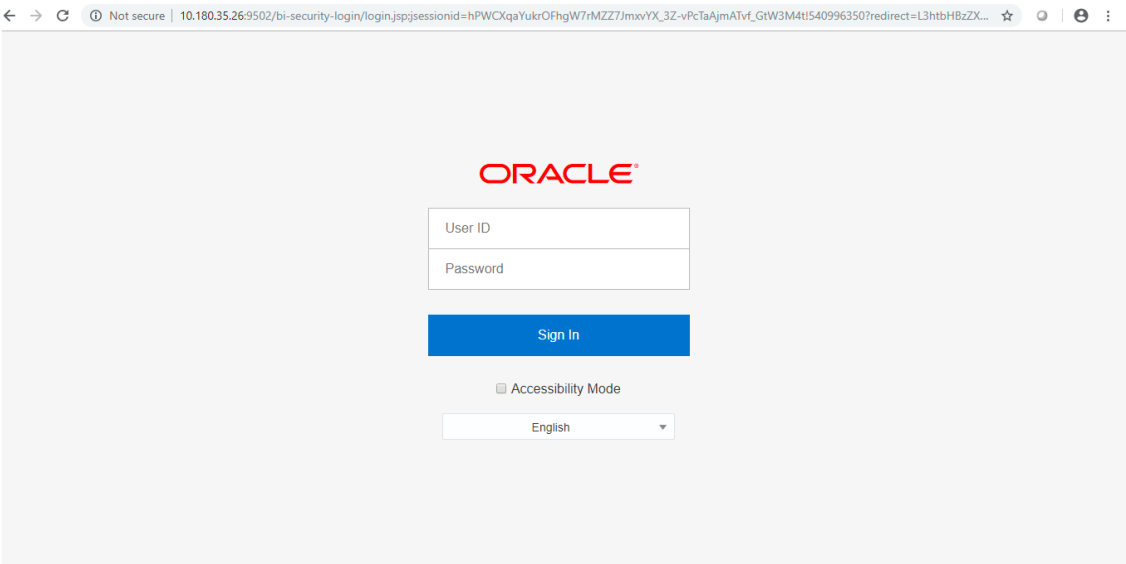
1. Open a browser and navigate to:

   <BIP_SERVER_IP>:<BIP_SERVER_PORT>/xmlpserver

2. Log in using the following credentials:

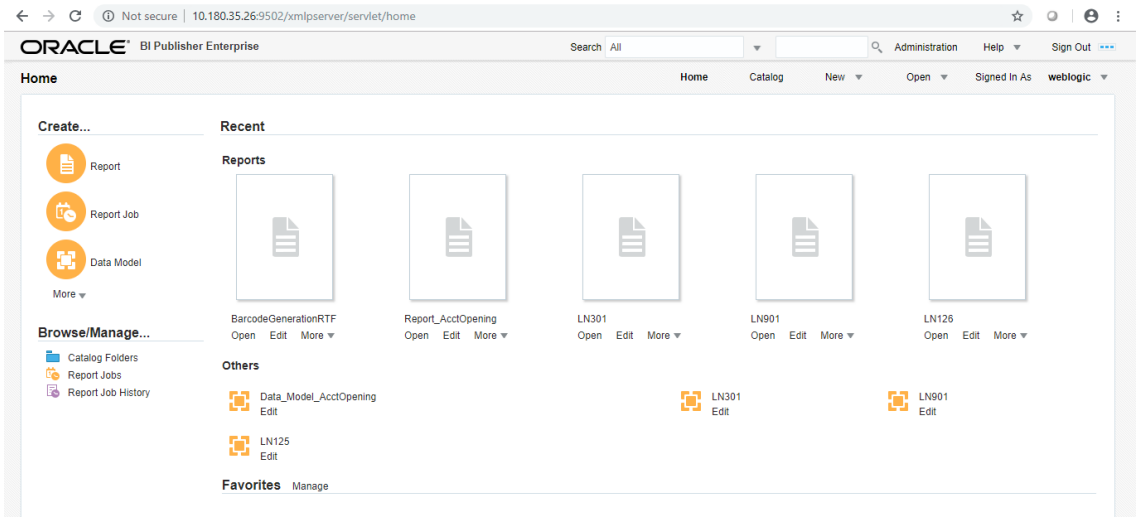
   - Username: <BIP_SERVER_USER>
   - Passowrd: <BIP_SERVER_PSWD>

Figure 9–1 OAS (BIP) Server Console Login



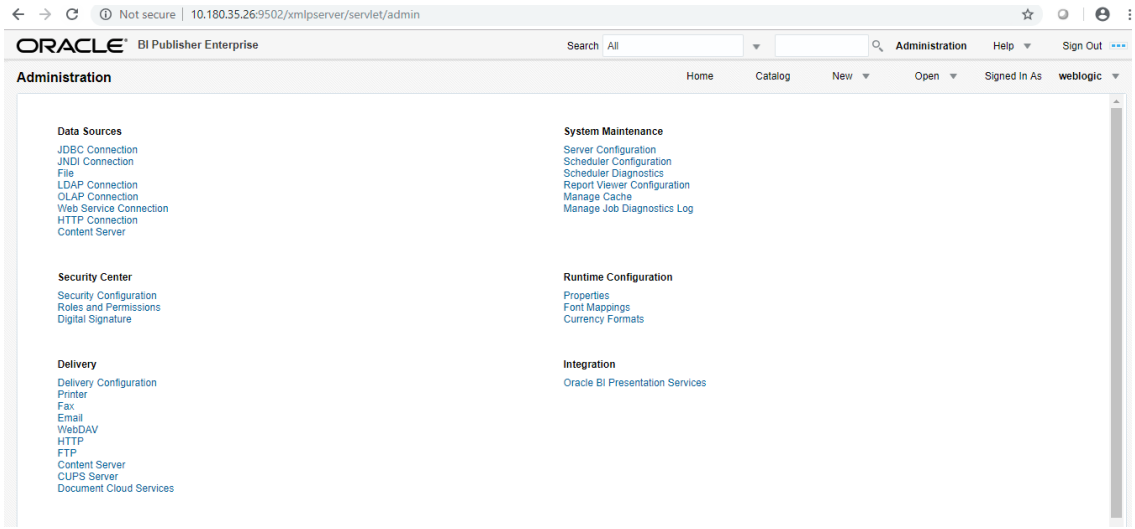
3. After logging in, click **Administration**.

Figure 9–2 OAS (BIP) Administration



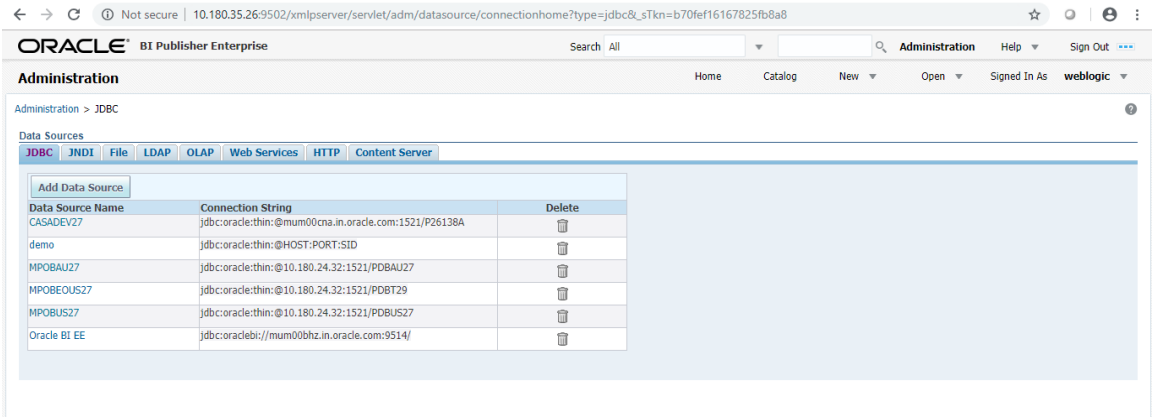
4. Click **JDBC Connection** under **Data Sources**.

Figure 9–3 OAS (BIP) JDBC Connection



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

Figure 9–4 OAS (BIP) - Add Data Source



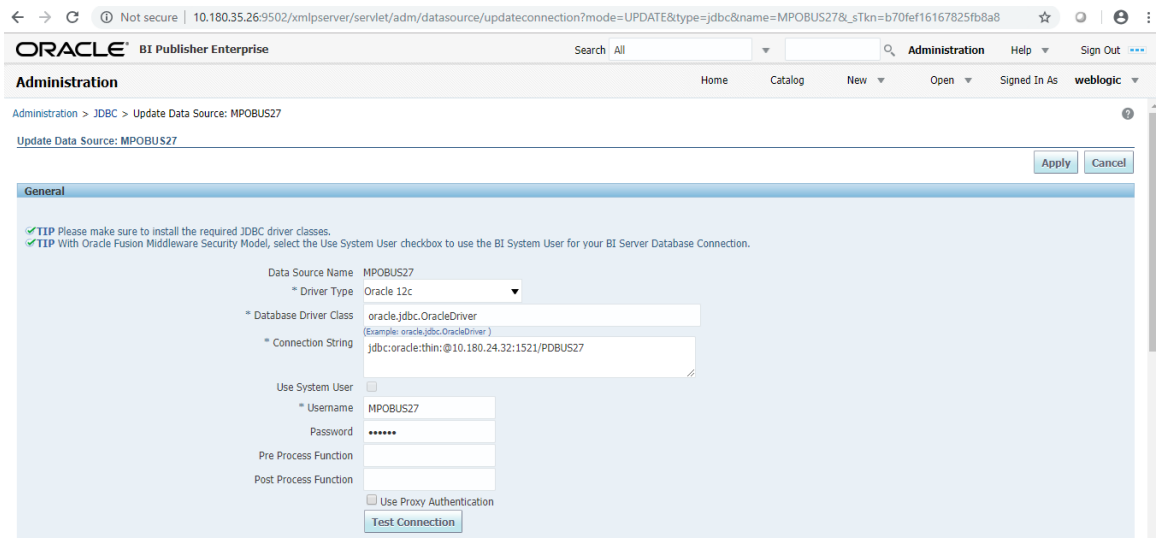
6. Fill up the following fields:

Table 9–1 Data Source Details

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

7. Click **OK**.

Figure 9–5 OAS (BIP) Data Source Created



10 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.

10.1 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

11 Monitoring Servers Using Oracle Enterprise Manager

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

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

12 Post Installation Verification

This chapter lists the steps required to verify the Oracle Banking Enterprise Originations solution installation.

12.1 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 OBEO libraries and applications is *Active*.
    - Shared Libraries
        - ob.app.client.coll
        - ob.app.client.communications
        - ob.app.client.cz
        - ob.app.client.deposit
        - ob.app.client.fw
        - ob.app.client.broker
        - 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.broker
        - ob.ui.lending
        - ob.ui.or

- ob.ui.party
- ob.ui.pm
- ob.ui.pricing
- ob.ui.sh
- ob.ui.tp
- ob.ui.tp.cz

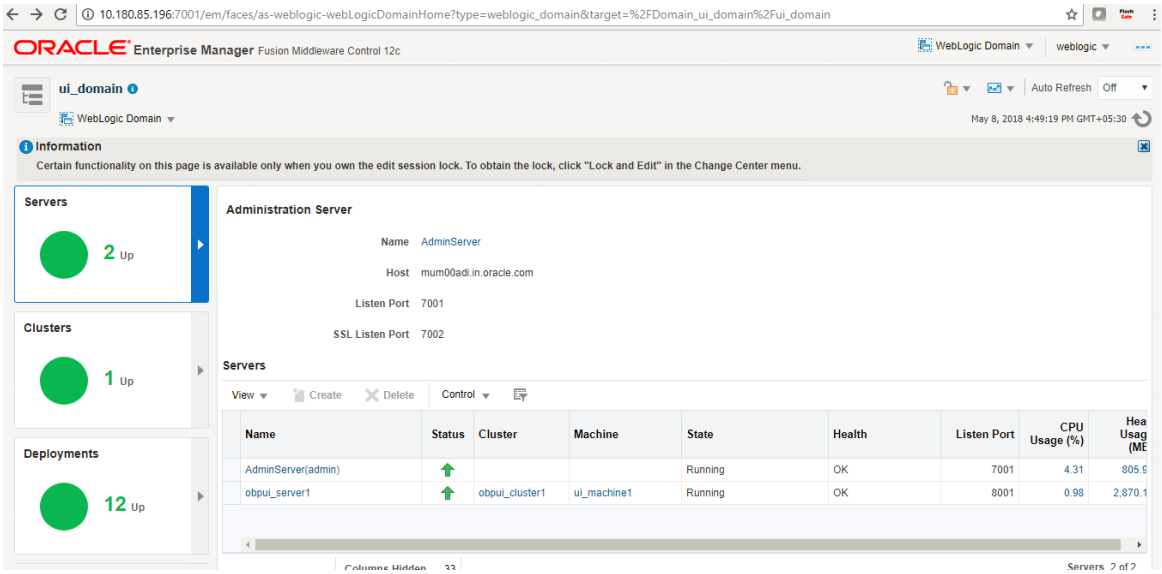
- Ears
  - com.ofss.fc.app.monitoring
  - com.ofss.fc.app.ui.connector
  - com.ofss.fc.ui.view.obcm
  - com.ofss.fc.ui.view.admin
  - com.ofss.fc.ui.view.admin.dashboard
  - com.ofss.fc.ui.view.developer
  - com.ofss.fc.ui.view.mds
  - com.ofss.fc.ui.view.obeo
  - com.ofss.fc.ui.view.obepm
  - com.ofss.fc.ui.view.qa
  - com.ofss.fc.ui.view.taskqueue

Note

Broker shared libraries will be a part of only AU localization.

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

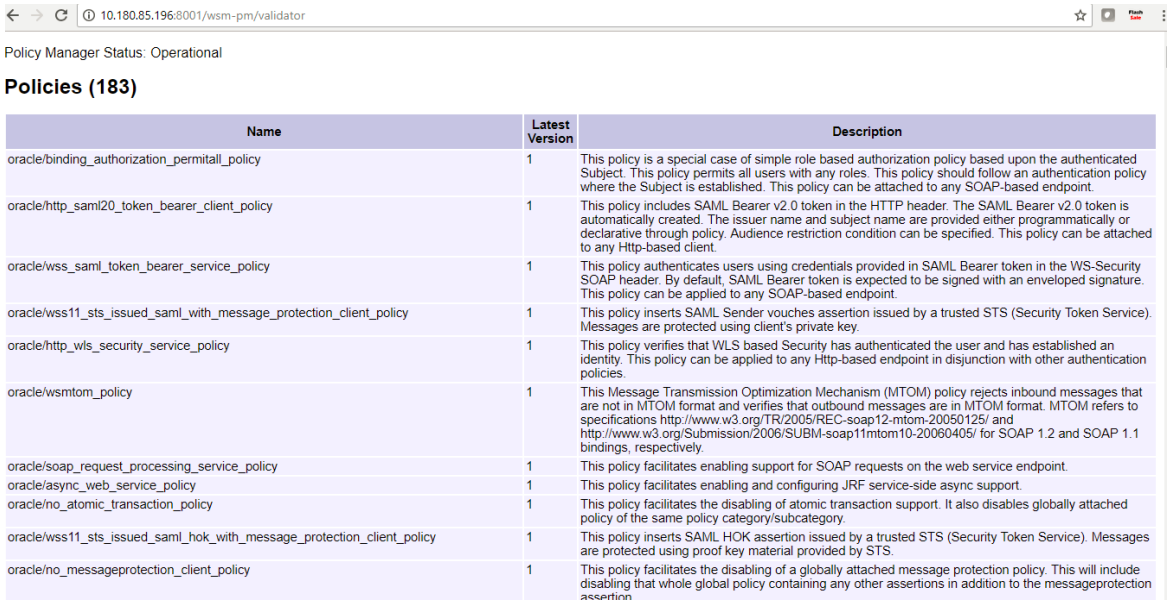
Figure 12–1 UI EM Console Status Check



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

Figure 12–2 UI Admin wsm-pm Validator

Figure 12–3 UI managed wsm-pm validator



10.180.85.196:8001/wsm-pm/validator

Policy Manager Status: Operational

Policies (183)

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 include disabling that whole global policy containing any other assertions in addition to the messageprotection assertion

12.2 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 OBEO libraries and applications is *Active*. Following are the details of all XD components libraries and ears:

   batchhost Server deployments

   - Shared libraries
     - ob.app.client.coll
     - ob.app.client.communications
     - ob.app.client.cz
     - ob.app.client.deposit
     - ob.app.client.fw
     - ob.app.client.broker
     - ob.app.client.lcm
     - ob.app.client.lending
     - ob.app.client.or
     - ob.app.client.party
     - ob.app.client.pm

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

■ Ears

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

OBPR Server deployments

■ Shared libraries

- ob.app.client.coll
- ob.app.client.communications
- ob.app.client.cz
- ob.app.client.deposit
- ob.app.client.fw
- ob.app.client.lcm
- ob.app.client.lending

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

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

OBEPM Server deployments

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

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

OBEO Server deployments

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

- com.ofss.fc.middleware.or
- com.ofss.fc.webservices.or

OBPM Server deployments

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

OBShared Server deployments

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

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

OBCCM Server deployments

- Shared libraries
    - ob.app.client.coll
    - ob.app.client.communications
    - ob.app.client.cz
    - ob.app.client.deposit
    - ob.app.client.fw
    - ob.app.client.lcm
    - ob.app.client.lending
    - ob.app.client.or
    - ob.app.client.party
    - ob.app.client.pm

- ob.app.client.pricing
- ob.app.host.cz
- ob.app.host.fw
- ob.app.host.lcm
- ob.app.host.sh
- ob.app.host.tp
- ob.app.host.tp.cz

■ Ears

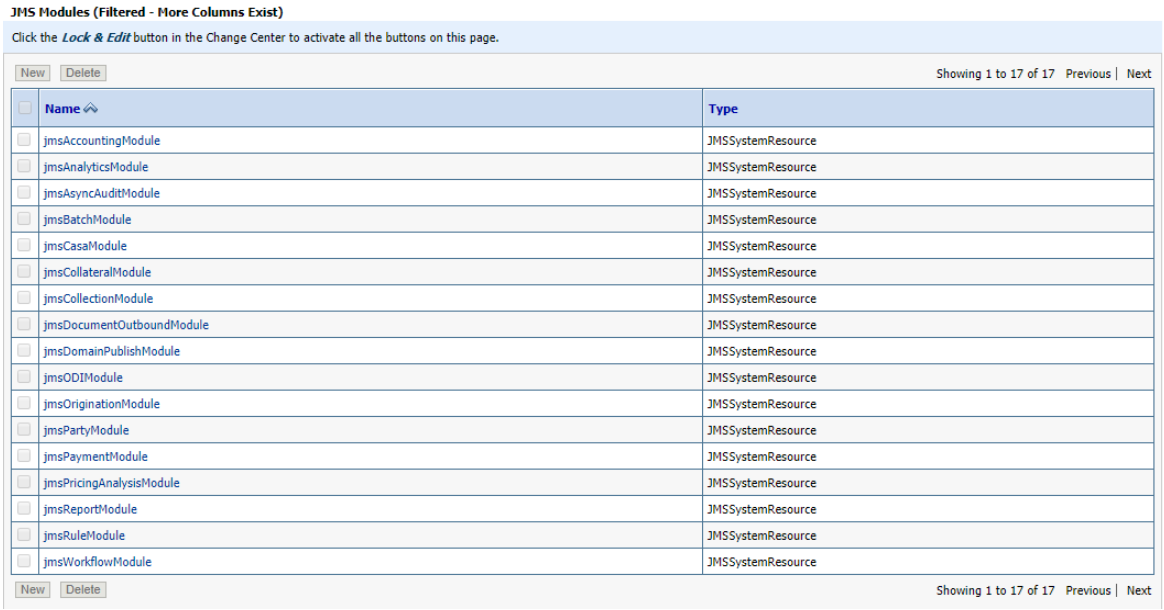
- com.ofss.fc.app.connector
- com.ofss.fc.app.monitoring
- com.ofss.fc.messaging.lcm
- com.ofss.fc.middleware.lcm
- com.ofss.fc.webservices.lcm

Note

Broker shared libraries will be a part of only AU localization.

JMS Modules

JMS Modules for all XD host servers.



JMS Modules (Filtered - More Columns Exist)

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

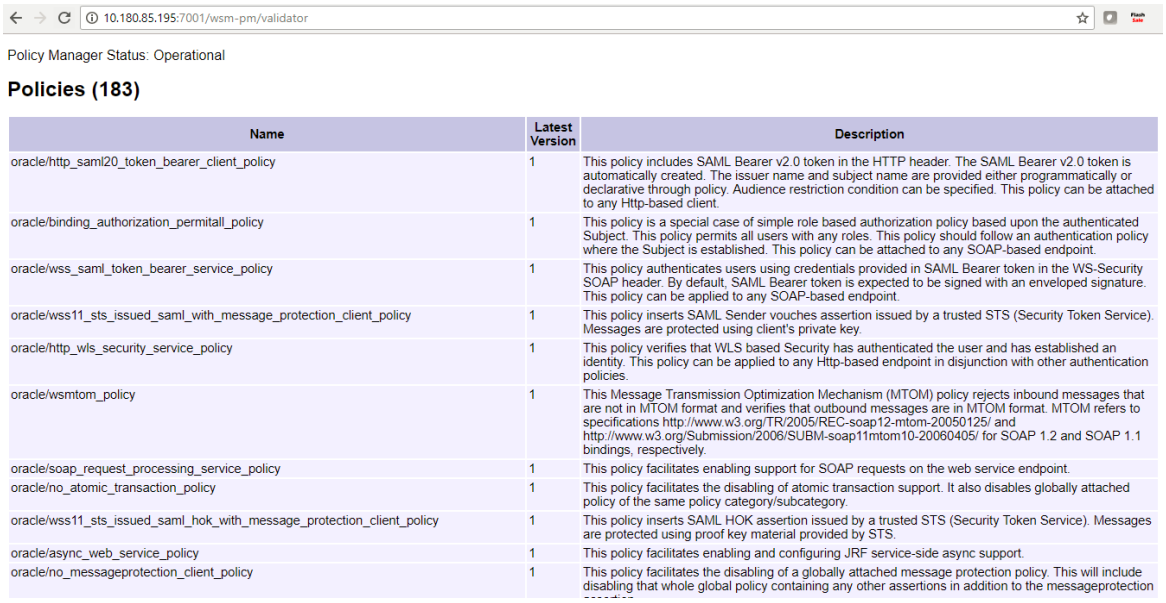
New Delete — Showing 1 to 17 of 17 Previous | Next

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

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

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

Figure 12–4 HOST admin wsm-pm validator



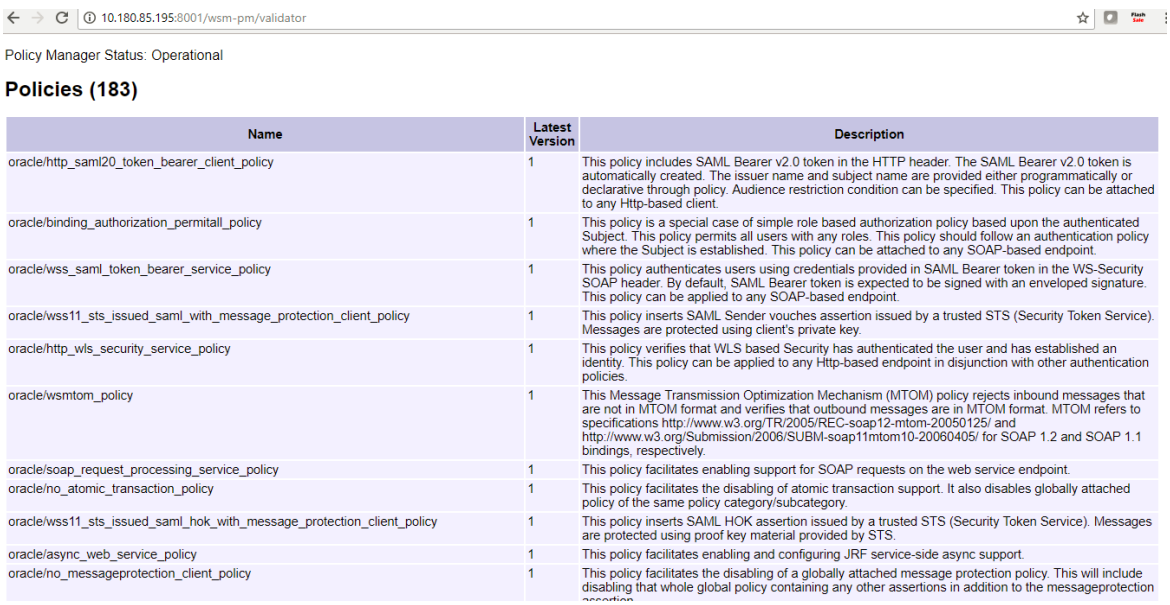
10.180.85.195:7001/wsm-pm/validator

Policy Manager Status: Operational

Policies (183)

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

Figure 12–5 HOST managed wsm-pm validator



10.180.85.195:8001/wsm-pm/validator

Policy Manager Status: Operational

Policies (183)

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

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.

12.3 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 OBEO libraries and human task files with .ear extension is *Active*.
   - Shared Libraries
     - ob.app.client.coll
     - ob.app.client.broker
     - 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.broker
     - ob.ui.communications
     - ob.ui.cz
     - ob.ui.deposit
     - ob.ui.fusion
     - ob.ui.lcm

- ob.ui.lending
- ob.ui.or
- ob.ui.party
- ob.ui.pm
- ob.ui.pricing
- ob.ui.sh
- ob.ui.tp
- ob.ui.tp.cz

- Ears
  - com.ofss.fc.app.ui.connector
  - com.ofss.fc.ui.view.mds
  - com.ofss.fc.workflow.ui.batchexceptionrecovery
  - com.ofss.fc.workflow.ui.brop
  - com.ofss.fc.workflow.ui.CapturePartyFinancialsHumanTask
  - com.ofss.fc.workflow.ui.common.approval
  - com.ofss.fc.workflow.ui.FeeNegotiationApprovalTask
  - com.ofss.fc.workflow.ui.hardshiprelief
  - com.ofss.fc.workflow.ui.lcm.PerformManualAllocationUITask
  - com.ofss.fc.workflow.ui.lcm.valuation
  - com.ofss.fc.workflow.ui.origination
  - com.ofss.fc.workflow.ui.PartyMerge
  - com.ofss.fc.workflow.ui.ProcessLoanRolloverHumanTask

Note

Broker shared libraries will be a part of only AU localization.

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

12.4 BAM Installation Verification

To verify the BAM installation:

1. Bring up the Admin and Managed servers (bam_server1).
2. Go to the BAM Login Page Link: http: //<BAM_IP>:9003/bam/composer/faces/designer

Figure 12–6 BAM Composer

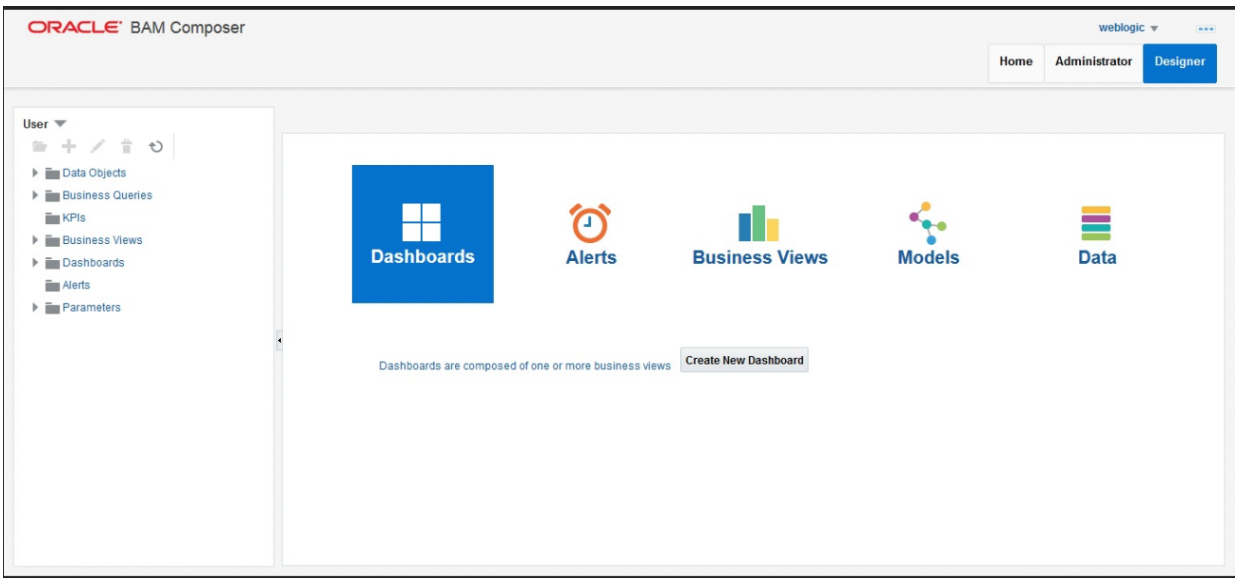


Figure 12–7 BAM Composer

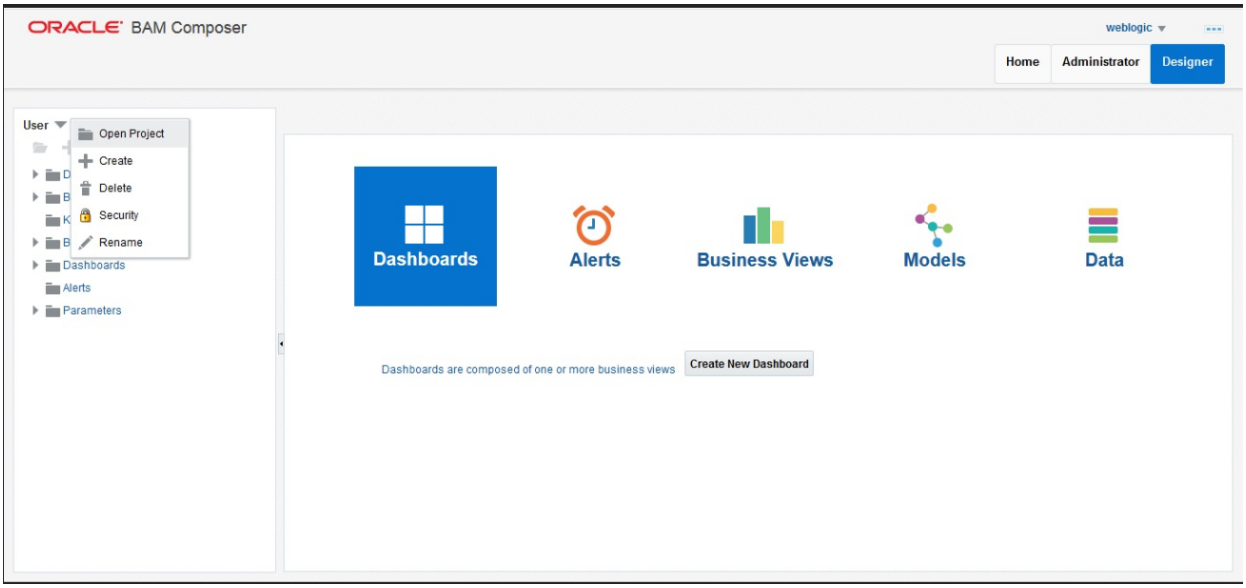
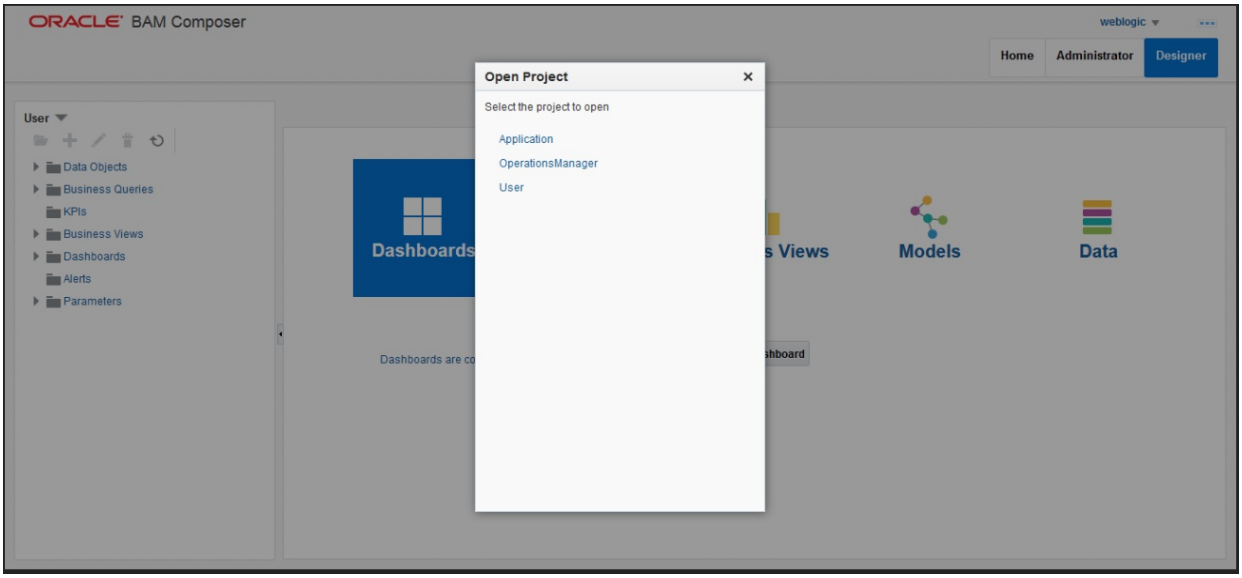


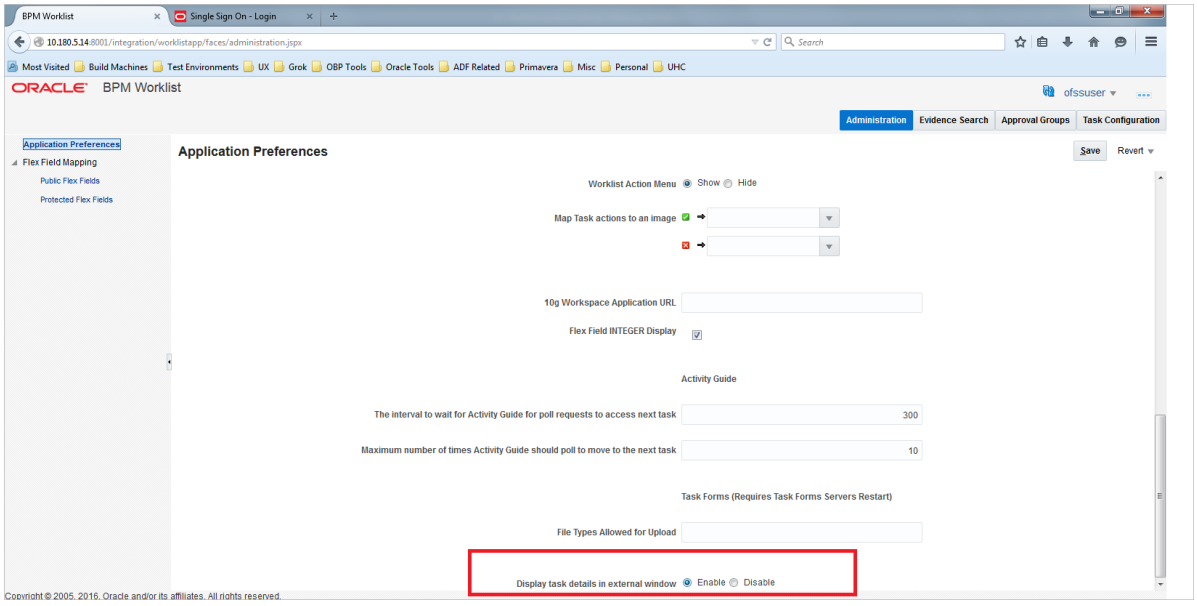
Figure 12–8 BAM Composer



12.5 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 12–9.

Figure 12–9 BPM Worklist Window Settings



13 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 Originations.

13.1 OBEO 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 OBEO 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 13–1 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.

13.2 OBEO Security Policy Seeding

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

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

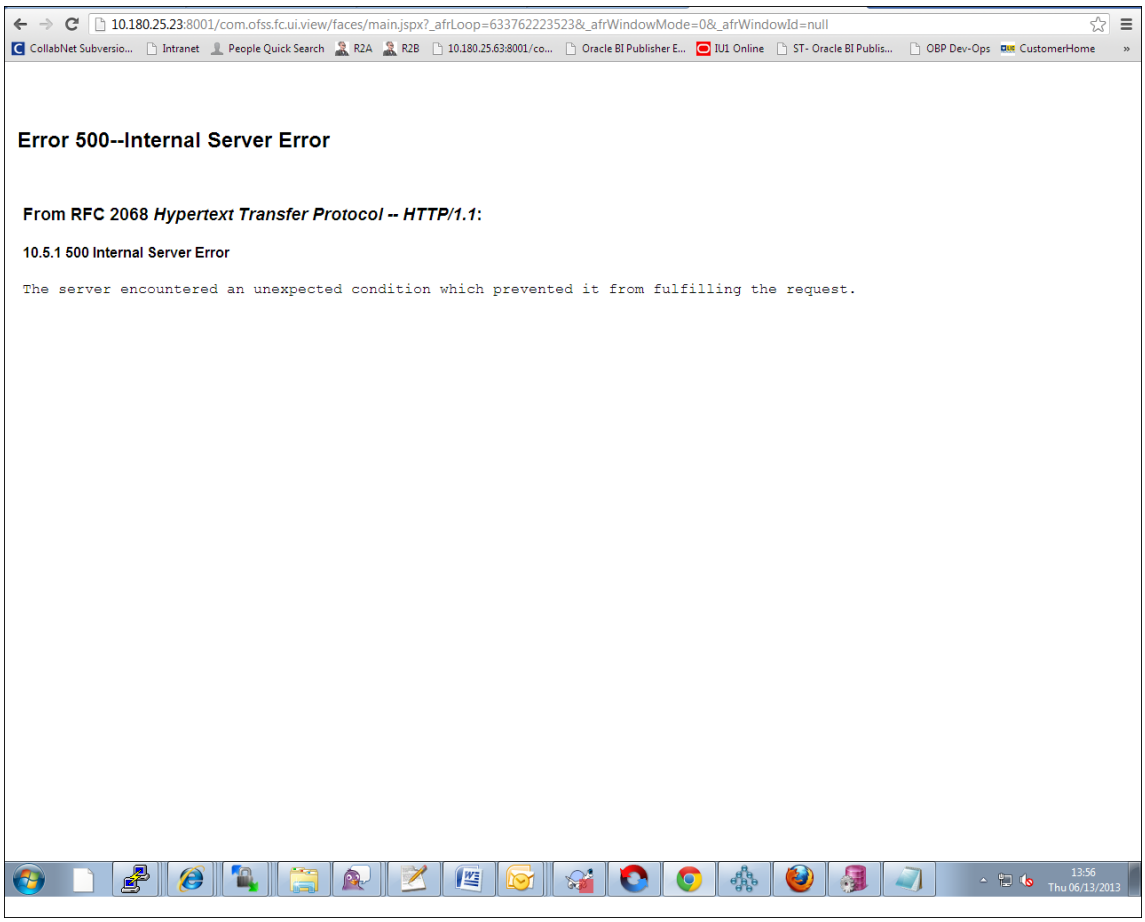
Once the post install script is completed successfully, you can start the domain servers and enter a dummy transaction to check the system correctness. If you face an error you can inspect the stderr log, the WebLogic domain managed server logs as well as the ofss logs under domain directory.

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.

13.4 Error on First Log in

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

Figure 13–2 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.

13.5 Log in Issues

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

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

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

13.6 SOA Setup in Cluster

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

13.6.1 "COMPONENTTYPE": invalid identifier error

Due to one of the one-off patches for SOA applied during the OBEO 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**.

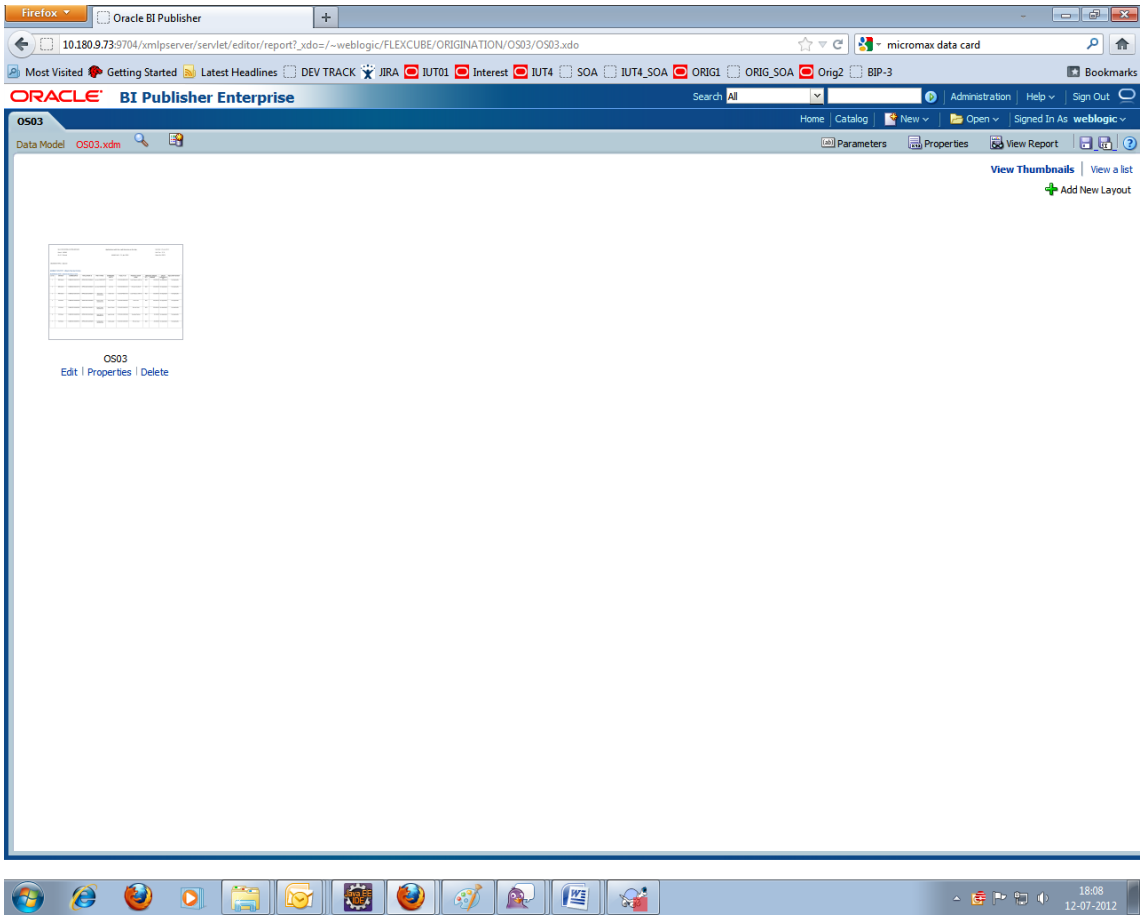
For example on Oracle database user needs to run the following command on soainfra schema:

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

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

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

Figure 13–3 Selecting the Data model



Note

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

13.8 Oracle BAM Command Utility Issue

This is not an issue. This occurs if Oracle BAM is installed for the second time on the same machine.

The following message appears:

Oracle BAM Command Utility [Build 19427, BAM Repository Version 2025] Copyright © 2002, 2015.

Oracle and/or its affiliates. All rights reserved.

java.lang.SecurityException: User: weblogic, failed to be authenticated.

[ErrorSource="javax.security.auth.login.LoginException: java.lang.SecurityException: User: weblogic, failed to be authenticated."]

The solution or pre-requisite before a second installation is to alter the following file:

<MIDDLEWARE_HOME>/soa/bam/config/BAMICommandConfig.xml

In this file, remove the following tags:

```
<ICommand_Default_User_Name>weblogic</ICommand_Default_User_Name>
<ICommand_Default_
Password>HkFBFDf0t65Kuw9/I70cnwXPYIXKz/OElhl0ID+qjdw=</ICommand_
Default_Password>
```

13.9 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

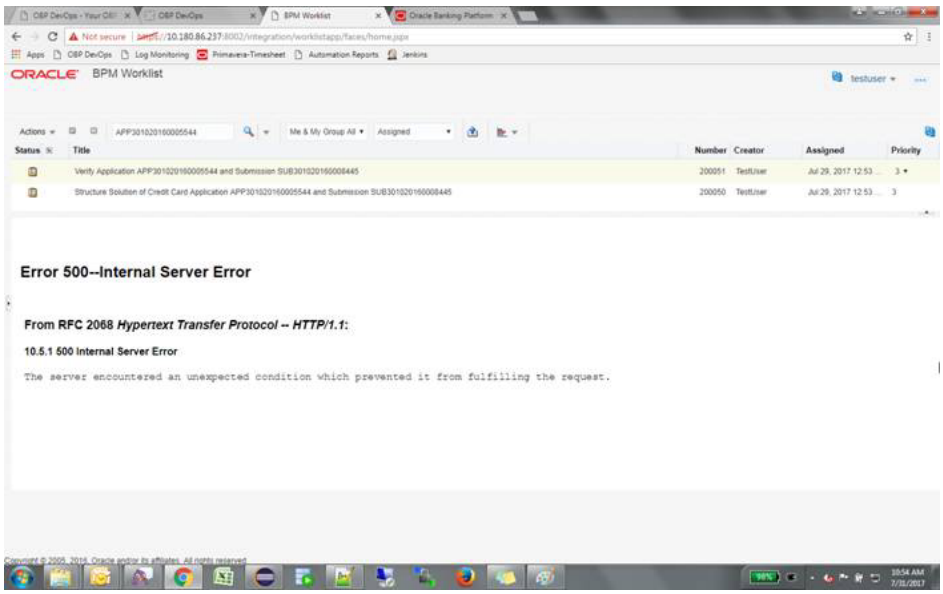
   <property name="trust.keystoreType" value="KSS"/>

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

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

2. Restart it.

Figure 13–4 BPM Worklist Task issue



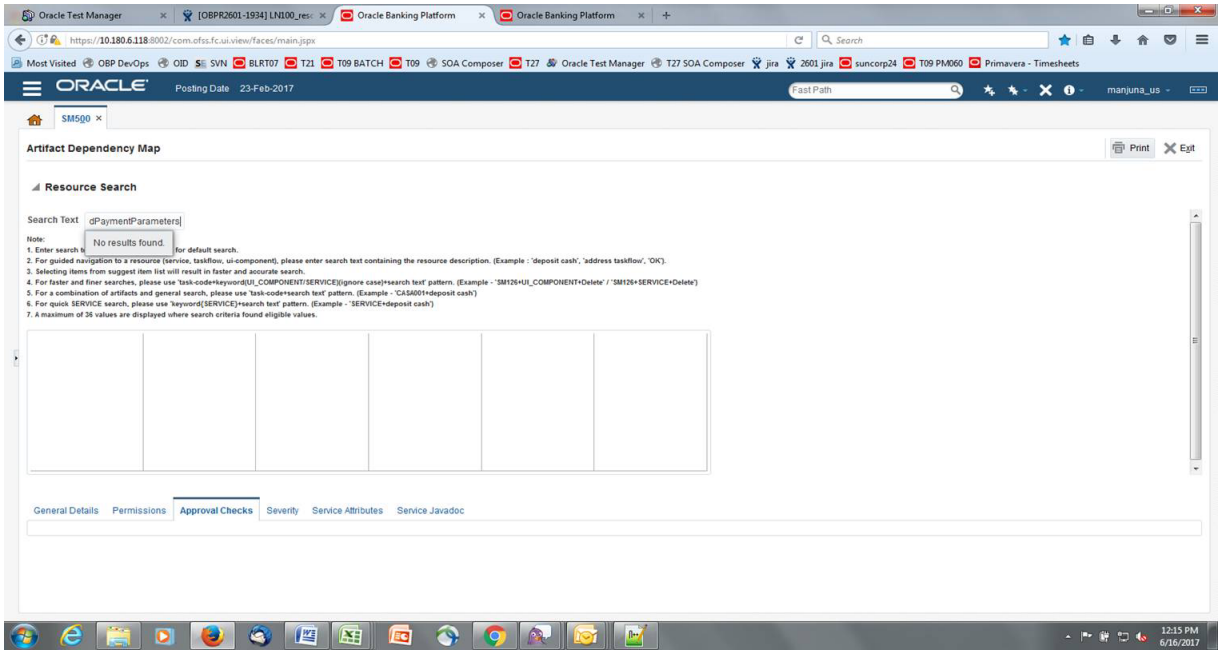
13.10 Artifacts Issue for SM500 page

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 13–5 Artifacts Issue for SM500 page



13.11 ra/FCRJConnectorSOA connector issue

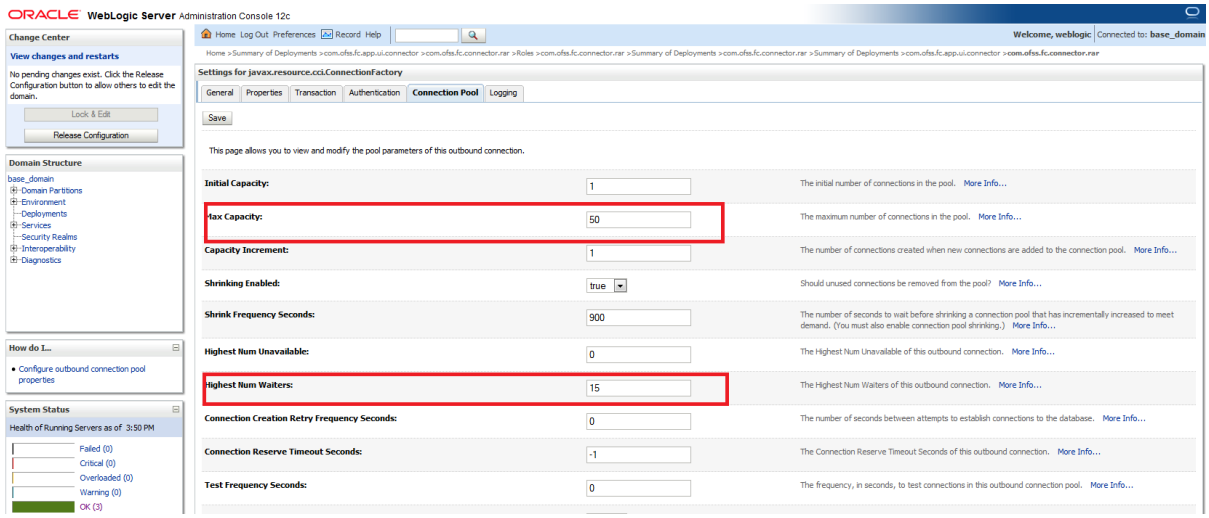
If below mentioned error is faced on Humantask server, configuration shown in the below figure has to be done to resolve issue.

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 13–6 Settings for javax.resource.cci.ConnectionFactory page



13.12 Humantask Startup Issue

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

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

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

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

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

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

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

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

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

Truncated. see log file for complete stacktrace

>

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

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

export EXTRA_JAVA_PROPERTIES

13.13 Collection Mocking

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

1. Execute the following SQL queries in application database:

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

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

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

   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -

   DAdapterFactories:INS_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:PARTY_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:LN_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:LCM_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:ACCOUNT_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:DDA_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:AC_COLLECTION_ADAPTER_MOCKED=true -

   DAdapterFactories:CS_COLLECTION_ADAPTER_MOCKED=true"

   export EXTRA_JAVA_PROPERTIES

3. Restart the HOST managed server.

13.14 DDA, Party and LOAN Mocking for OBEO installer

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

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

   EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -

   DAdapterFactories:ACCOUNT_DDA_MOCKED=true -

   DAdapterFactories:ACCOUNT_LOAN_MOCKED=true -

   DAdapterFactories:PARTY_ENTITLEMENT_ADPT_MOCKED=true "

export EXTRA_JAVA_PROPERTIES

2. Restart the HOST managed server.
3. Please add following argument in setDomainEnv.sh file of PRICING server. Please make sure to add the space at the end of line

   -DPricingConfiguration:MockedDomainCategories=LN,CS,TD

4. Restart Pricing Server managed server.
5. Please add following argument in setDomainEnv.sh file of shared server. Please make sure to add the space at the end of line

   -DAdapterFactories:ACCOUNT_DDA_MOCKED=true

   -DAdapterFactories:ACCOUNT_TD_MOCKED=true

   -DAdapterFactories:ACCOUNT_LOAN_MOCKED=true

6. Restart shared managed server.

Note

From point 3, steps are applicable only for OBEO US setup

14 Uninstalling the Application

This chapter explains the process of uninstalling the Oracle Banking Enterprise Originations.

14.1 Manual Uninstall

Currently an installed OBEO 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 Originations related database schemas run the RCU utility and choose the **Drop** option.