

**Oracle® Fusion Middleware**

Administrator's Guide for Imaging and Process Management

11g Release 1 (11.1.1)

**E12782-01**

January 2010

Oracle Fusion Middleware Administrator's Guide for Imaging and Process Management, 11g Release 1 (11.1.1)

E12782-01

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

Primary Author: Bruce Silver

Contributor: David Jones

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

---

---

# Contents

<b>Preface</b> .....	xi
Audience.....	xi
Documentation Accessibility .....	xi
Related Documents .....	xii
Conventions .....	xii
<b>1 Introduction</b>	
1.1 About This Guide.....	1-1
1.2 Getting Started.....	1-1
1.3 About This Product .....	1-2
1.4 About System Administration .....	1-3
1.4.1 Administrative Accounts.....	1-3
1.4.2 Administrative Tools.....	1-4
1.4.3 System Administration Tasks Not Covered in This Guide .....	1-4
1.5 Imaging and Process Management Architecture .....	1-4
1.5.1 Application Architecture Overview.....	1-5
1.5.2 Web Services and Java API .....	1-5
1.5.3 Business Logic and Agents.....	1-6
1.6 Integration with Key Oracle Technologies.....	1-7
1.6.1 Integration with Oracle Document Capture.....	1-7
1.6.2 Integration with an Oracle Document Repository.....	1-8
1.6.3 Integration with Oracle WebLogic Server.....	1-8
1.6.4 Integration with Oracle BPEL Server.....	1-8
<b>2 Managing Security</b>	
2.1 Security Model Overview .....	2-1
2.1.1 System Access.....	2-1
2.1.2 Installation Security Initialization .....	2-2
2.1.2.1 Migrating User Store from LDAP Server to Oracle Internet Directory .....	2-3
2.1.3 Integration with Single Sign-On.....	2-3
2.1.4 Definition Management Security Rights and Definition Security Rights .....	2-4
2.1.4.1 Definition Management Rights .....	2-4
2.1.4.2 Definition Rights.....	2-5
2.1.5 Users and Groups .....	2-5
2.2 Managing Definition and Definition Management Security .....	2-6

2.2.1	Working With Definition Management Security .....	2-6
2.2.2	Working with Definition Security .....	2-7
2.2.3	Working with Document Security .....	2-7
2.2.4	Working with Annotation Security .....	2-8
2.2.4.1	Annotation Permissions .....	2-8
2.2.5	Security Example .....	2-9
2.3	Managing System Level Security .....	2-11
2.3.1	Configuring a Fusion Middleware Application to use SSL.....	2-11
2.3.1.1	Configuring an SSL Content Server Repository Connection .....	2-11
2.3.2	Integrating with BPEL.....	2-11
2.3.2.1	Integration Points .....	2-12
2.3.2.2	BPEL Connection Configuration .....	2-12
2.3.2.3	SSL Configuration .....	2-13
2.3.3	Configuring a Fusion Middleware Application to Use Web Services .....	2-14
2.3.4	Web Services Security Configuration for I/PM .....	2-15
2.3.4.1	Working with Oracle Web Services Manager .....	2-15
2.3.4.2	Setting Policies on Services .....	2-15
2.3.4.3	API Usage .....	2-17
2.3.4.4	Examples.....	2-17
2.3.4.5	Working With Keystores .....	2-19
2.3.4.6	Working with the CSF through WLST .....	2-20

### 3 Changing Configuration Settings

3.1	Configuration Overview .....	3-1
3.2	Post-Installation Configuration.....	3-2
3.3	Configuration of Repository Options .....	3-2
3.3.1	Storage Management.....	3-2
3.3.2	Repository Capacity .....	3-2
3.3.3	Storage Media.....	3-3
3.3.4	Oracle Content Server File Store Provider Rules .....	3-3
3.3.4.1	Disabling the Repository Weblayout Directory .....	3-3
3.3.5	Additional Oracle Content Server Components .....	3-4
3.3.5.1	Required Components .....	3-4
3.3.5.2	Optional Components.....	3-4
3.3.6	Oracle Content Server Document Profiles .....	3-4
3.3.6.1	Global Profile Rules.....	3-4
3.3.6.2	Application Profile and Profile Rules .....	3-5
3.3.6.3	Working With Folders .....	3-5
3.3.6.4	Working With Universal Records Manager .....	3-6
3.3.6.5	Working With Information Rights Manager .....	3-7
3.3.6.6	Working With WebCenter Spaces.....	3-7
3.4	Exporting and Importing Definitions .....	3-8
3.4.1	Exporting Definitions .....	3-8
3.4.2	Importing Definitions.....	3-8
3.5	File Size Limits.....	3-9
3.6	Configuring MBeans.....	3-9
3.6.1	Oracle I/PM MBeans.....	3-9

3.6.2	Using WLST to Change MBeans .....	3-12
3.6.3	Using Enterprise Manager to Set an MBean Value.....	3-14
3.7	Setting Font Variables .....	3-14
3.7.1	Configuring the AgentUser and GDFontPath MBeans.....	3-15
3.8	Configuring Display of Seconds in Search Results.....	3-15
3.9	Configuring I/PM Logging.....	3-16

## 4 Managing Applications

4.1	Application Overview .....	4-1
4.1.1	Document Overview .....	4-1
4.1.2	Uploading Documents.....	4-2
4.2	Creating An Application.....	4-2
4.2.1	Specifying General Properties.....	4-3
4.2.2	Defining Application Fields.....	4-4
4.2.3	Assigning Application Security.....	4-5
4.2.3.1	Copying Permissions From One User to Another User.....	4-5
4.2.4	Assigning Document Security .....	4-5
4.2.5	Assigning a Storage Policy .....	4-6
4.2.6	Configuring BPEL Integration.....	4-6
4.2.7	Reviewing Application Settings .....	4-7
4.3	Modifying an Existing Application.....	4-7

## 5 Managing Inputs

5.1	Enabling Input Agent.....	5-1
5.2	Understanding Input Files.....	5-2
5.3	Using Input Filing Commands .....	5-3
5.3.1	Locale.....	5-3
5.3.2	New.....	5-4
5.4	Creating Input Definitions.....	5-4
5.5	Input Agent Processing.....	5-6
5.5.1	Input Directory Structure .....	5-6
5.5.2	Input Agent Processing Order .....	5-7
5.5.2.1	Polling .....	5-7
5.5.2.2	Processing .....	5-7
5.5.3	Changing WLS Work Manager Settings .....	5-7
5.6	Checking Results and Error Files.....	5-8

## 6 Managing Searches

6.1	Search Overview .....	6-1
6.2	Creating a Search .....	6-1
6.3	Modifying an Existing Search .....	6-3

## 7 Managing Connections

7.1	Creating a Content Server Connection .....	7-1
7.1.1	Configuring SSL Connection to Content Server Repository .....	7-2

7.2	Creating a BPEL Connection .....	7-2
7.2.1	Configuring SSL for the BPEL Server .....	7-3
7.2.2	Configuring a BPEL Connection CSF Credential.....	7-4

## 8 Working with BPEL

8.1	Business Process Management.....	8-1
8.2	Business Process Execution Language (BPEL) .....	8-1
8.2.1	Configuring BPEL Properties.....	8-2
8.2.1.1	BPEL Payload Mapping Functions .....	8-2
8.2.1.2	Required Payload Element (MinOccurs) Handling .....	8-4
8.2.1.3	Date Field Format .....	8-4
8.2.1.4	Doc Property Functions .....	8-4
8.2.1.5	Field Value Functions .....	8-4
8.2.1.6	Format Value Function .....	8-5
8.2.2	Payload Limitations.....	8-5
8.2.3	Mapping Secure BPEL Services .....	8-5
8.2.4	Changing WebLogic Server Work Manager Settings.....	8-6
8.2.5	Using a BPEL Connection CSF Credential.....	8-6
8.2.6	BPEL Agent Retry Sequence .....	8-6
8.2.7	Configuring the BPEL Faults Table.....	8-7
8.2.8	Initiating a BPEL Process Instance .....	8-7

## 9 Document Storage

9.1	Document Storage Overview .....	9-1
9.1.1	Oracle Content Server Document Properties .....	9-1

## 10 Troubleshooting

10.1	Contacting Support.....	10-1
10.2	UI Slowdown .....	10-2
10.3	Decimal Field Error.....	10-2
10.4	I/PM and Windows Server Prerequisites .....	10-3
10.5	Search Results Not Displaying Seconds When Displaying Time .....	10-3
10.6	NULL Number Fields.....	10-3
10.7	Full-Text Search Fails On Large Documents.....	10-3
10.8	Repository Capacity Errors .....	10-3
10.9	Problems Connecting Multiple I/PM Systems to Single Repository .....	10-4
10.10	Font Errors .....	10-4
10.11	Input Agent and Input File Issues .....	10-5
10.11.1	Input Agent Will Not Detect and Process Input Files .....	10-5
10.11.2	Auto-detect Not Determining Character Set .....	10-5
10.11.3	Input File Entries Have Errors .....	10-5
10.11.4	Dates and Times Shifting on Content Ingested Using Input Agent.....	10-6
10.12	Advanced Viewer Transformation Errors.....	10-6
10.13	Problems with TIFF Display in Viewer .....	10-6
10.14	Shared Temp Directory in Linux Causes Display Failure .....	10-6
10.15	Shifting Redaction and Other Annotations.....	10-6

10.16	Logging of ImagingException.....	10-7
10.17	Reviewing Audit History of Deleted Documents.....	10-7
10.18	Deciphering Nested Stack Errors.....	10-7
10.19	500 Internal Server Error When Using OSSO.....	10-8
10.20	Oracle Content Server 10g Provides Incorrect Dates for BPEL.....	10-8
10.21	Doc URL Returned With Invalid IP Address.....	10-9

## A User Interface

A.1	Icons.....	A-2
A.2	Navigator Pane.....	A-3
A.3	Navigation Train.....	A-4
A.4	Upload Document Page.....	A-4
A.5	Update Document Page.....	A-6
A.6	Export Definitions: Export Comments Page.....	A-7
A.7	Export Definitions: Applications Page.....	A-7
A.8	Export Definitions: Searches Page.....	A-8
A.9	Export Definitions: Inputs Page.....	A-9
A.10	Export Definitions: Summary Page.....	A-9
A.11	Import Definitions: File Location Page.....	A-10
A.12	Import Definitions: Select Imports Page.....	A-11
A.13	Import Definitions: Validate Imports Page.....	A-12
A.14	Search Properties Page.....	A-15
A.15	Search Results Formatting Page.....	A-16
A.16	Search Conditions Page.....	A-17
A.17	Search Parameters Page.....	A-19
A.18	Search Security Page.....	A-20
A.19	Add Security Member Page.....	A-20
A.20	Search Preview and Test Page.....	A-21
A.21	Search Summary Page.....	A-22
A.22	Application General Properties Page.....	A-24
A.23	Application Field Definitions Page.....	A-25
A.24	Application Security Page.....	A-26
A.25	Application Document Security Page.....	A-27
A.26	Application Storage Policy Page.....	A-28
A.27	Application BPEL Configuration Page.....	A-28
A.28	BPEL Server Properties Page.....	A-29
A.29	BPEL Component Properties Page.....	A-29
A.30	BPEL Payload Properties Page.....	A-30
A.30.1	Edit Format Value Page.....	A-31
A.31	Application Review Settings Page.....	A-32
A.32	Input Basic Information Page.....	A-33
A.33	Input Identify and Parse File Parameters Page.....	A-34
A.34	Input Field Mapping Page.....	A-35
A.34.1	Define Date Format Page.....	A-36
A.35	Input Security Page.....	A-38
A.36	Input Review Settings Page.....	A-39
A.37	Content Server Connection Basic Information Page.....	A-40

A.38	Content Server Connection Content Server Settings Page .....	A-41
A.39	Content Server Connection Security Page.....	A-42
A.40	Content Server Connection Review Settings Page.....	A-43
A.41	BPEL Connection Basic Information Page .....	A-44
A.42	BPEL Connection Settings Page.....	A-45
A.43	BPEL Connection Security Page .....	A-46
A.44	BPEL Connection Review Settings Page.....	A-47
A.45	Manage Security .....	A-48

## Index



---

---

# Preface

Imaging and Process Management (Oracle I/PM) integrates electronic document storage, retrieval, and annotation with business processes to facilitate document use across an enterprise. Documents are uploaded into a repository managed by Oracle Universal Content Manager using an application within I/PM. Applications are predefined by you based on your business need. Documents are uploaded to applications based on a business need. For example, one application would be used to upload an invoice and a different application would be used to upload a contract. The application determines the metadata that is associated with a document, as well as security permissions to the document and any document annotations. This guide details how to define applications and searches, connect to a BPEL server to integrate with other business processes, and configure I/PM to best meet your company needs.

## Audience

This guide is intended for administrators who need to configure and manage an Imaging and Process Management implementation.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

### Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### Access to Oracle Support for Hearing-Impaired Customers

Oracle customers have access to electronic support through My Oracle Support or by calling Oracle Support at 1.800.223.1711. Hearing-impaired customers in the U.S. who wish to speak to an Oracle Support representative may use a telecommunications relay service (TRS). Information about the TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of telephone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>. International hearing-impaired customers should use the TRS at +1.605.224.1837. An Oracle Support engineer will respond to technical issues according to the standard service request process.

## Related Documents

Imaging and Process Management (Oracle I/PM) works with Oracle Universal Content Manager to store and retrieve documents. For more information about using Oracle I/PM, see the following:

- *Oracle Fusion Middleware User's Guide for Oracle Imaging and Process Management User's Guide*
- *Oracle Fusion Middleware Oracle Imaging and Process Management Developer's Guide*

For more information about Universal Content Manager, see administrator guides included in the Oracle Content Server documentation set and any applicable documents for external repositories, as necessary.

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

---

---

# Introduction

This chapter covers the following topics:

- ["About This Guide"](#) on page 1-1
- ["About This Product"](#) on page 1-2
- ["Getting Started"](#) on page 1-1
- ["About System Administration"](#) on page 1-3
- ["Imaging and Process Management Architecture"](#) on page 1-4
- ["Integration with Key Oracle Technologies"](#) on page 1-7

## 1.1 About This Guide

This guide provides instructions for administering the Oracle I/PM product software on the WebLogic Server. The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified.

In this document and other documents in this product set, the terms application, search, input, and connection are typically being used as defined objects within the Oracle I/PM product.

## 1.2 Getting Started

This guide assumes that Oracle I/PM is already installed. For information on installing Oracle I/PM and setting initial post-installation configuration options, see *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite*.

This chapter provides an overview to the product architecture. Subsequent chapters detail security contexts, initial configuration steps, administration procedures, and reference material for administering Oracle I/PM.

After installing Oracle I/PM and prior to configuring applications and other aspects of I/PM, ensure the following:

- If using Oracle Document Capture or Oracle Distributed Document Capture, ensure that they have been configured with the Oracle I/PM 11g commit driver.
- Ensure that the agent user and GDFontpath values have been set.
- Review the chapter on managing security to familiarize yourself with the security contexts within Oracle I/PM, the levels of security within those contexts and how they will apply to users and groups.

- Obtain the necessary security information to connect to a BPEL server.
- Obtain the necessary security information to connect to a Content Server repository.

## 1.3 About This Product

Oracle Imaging and Process Management (Oracle I/PM) provides organizations with a scalable solution upon which to develop process-oriented imaging applications and image-enablement solutions for enterprise applications. It enables image capture via Oracle Document Capture and Oracle Distributed Document Capture, annotation and markup of images, routing and approval automation, and support for high-volume applications for billions of items. With Oracle I/PM, organizations can quickly integrate their content and processes directly with Oracle enterprise applications, such as Oracle E-Business Suite, PeopleSoft Enterprise, and JD Edwards EnterpriseOne. Users benefit by having a single source for all transaction-based content, eliminating the need for double entry.

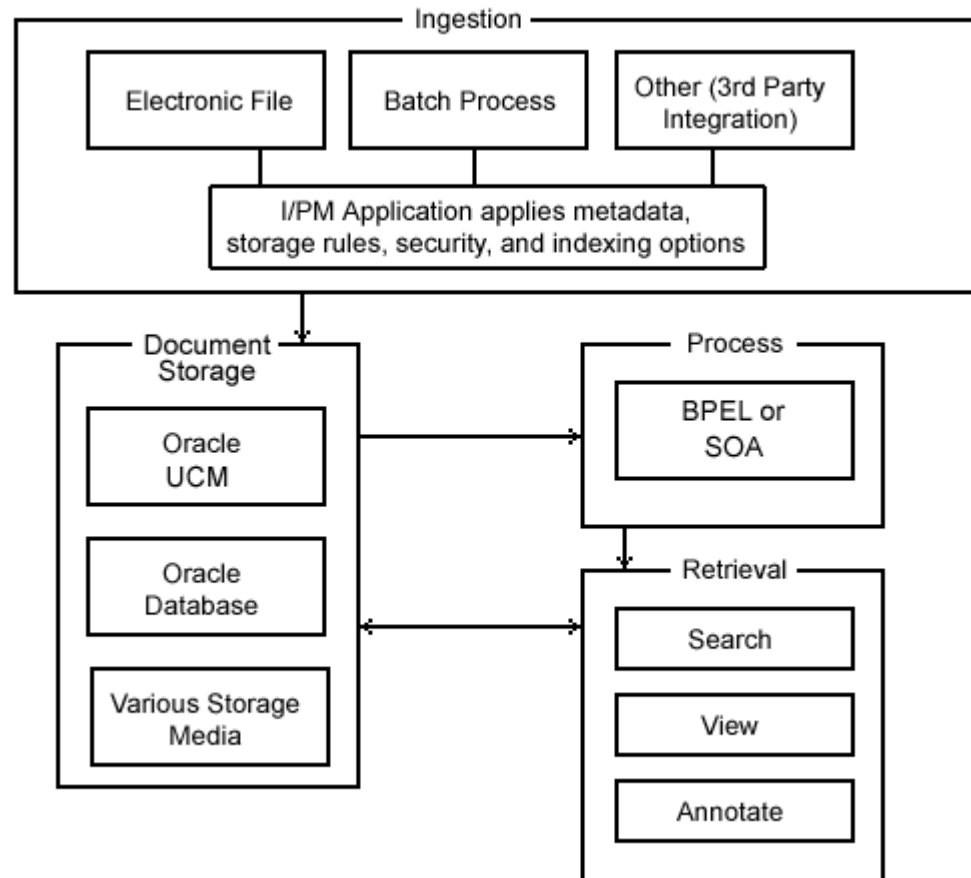
Oracle I/PM manages documents from image capture to archiving. A document is uploaded into Oracle I/PM either singly by individual users or in bulk via a background ingestion agent. Once uploaded, a document becomes part of an application. An application is a type of container for documents that defines metadata, storage information, and BPEL process configuration for all documents within it. Applications are defined by the system administrator based on a specific business need. For example, an Invoicing application may track invoice number, date sent, date due, status, and any other metadata required by an accounting department. Applications use an input definition to map metadata from an input file to the correct application fields for bulk ingestion via the input agent. The input agent ingests the metadata and documents from a local file system into I/PM.

Depending on how your repository is set up, uploaded documents can be stored within an Oracle database, on a file system, or in storage-specific hardware for retrieval. Security is applied to an Oracle I/PM document based on its application, ensuring access only by authorized users. And Oracle I/PM may be configured to initiate a business process instance within Oracle's BPEL server.

Users can retrieve stored documents using a predefined search. Predefined searches are created to find documents based on document metadata and full-text indexes. With the proper permissions, users can:

- View documents in a standard web-browser
- Print, download, or e-mail the document to others
- Annotate documents
- Upload documents and initiate a BPEL process if one is defined in the application
- Delete, copy, or move documents

Figure 1–1 Oracle I/PM Process Overview



## 1.4 About System Administration

Oracle I/PM system administrators are typically responsible for the following tasks:

- Installing Imaging and Process Management
- Configuring Oracle I/PM
- Creating Oracle I/PM applications
- Configuring BPEL injection
- Configuring Oracle I/PM repository connections
- Creating Oracle I/PM searches
- Creating Oracle I/PM inputs
- Monitoring and troubleshooting Oracle I/PM issues

### 1.4.1 Administrative Accounts

The first user to log into Oracle I/PM after installation is given full administrative privileges for the installation. This user can give permissions to access the system to others. If for any reason system security needs to be reset, you can do so following the procedure in the section "Installation Security Initialization" in chapter 2 of the full documentation set.

## 1.4.2 Administrative Tools

Administration of Oracle I/PM is done using the following administration tools:

- Oracle I/PM user interface. Administration capabilities are exposed in the interface based on user permissions.
- Oracle Enterprise Manager can be used for reviewing statistics on deployed resources, statistics of individual domains, details of web services, and other information. For more information, see the documentation that comes with Enterprise Manager..
- Oracle WebLogic Server can be used for reviewing log files, installed modules, installed Enterprise JavaBeans, configuration parameters, setting configuration MBeans for Oracle I/PM, and more. For more information, see the documentation available with Enterprise Manager.
- WebLogic Scripting Tool (WLST) is a command-line interface for navigating, monitoring, and configuring WebLogic Server. It can be used to configure I/PM parameters, review log files, and more. For more information on using WLST, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 1.4.3 System Administration Tasks Not Covered in This Guide

Some Oracle I/PM system administration tasks are not covered in this guide. The following table explains what these tasks are and where to find more information.

**Table 1–1 System Administration Tasks and Information Not Covered in This Guide**

Task	Where to Go For More Information
Administering Oracle SOA Suite	<i>Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite</i>
Administering Oracle WebLogic Server	<i>Oracle Fusion Middleware Administrator's Guide</i>
Administering Universal Content Management	See the following Oracle Universal Content Management guides: <ul style="list-style-type: none"> <li>■ <i>Getting Started with Content Server</i></li> <li>■ <i>Managing System Settings and Processes</i></li> <li>■ <i>Managing Repository Content</i></li> <li>■ <i>File Store Provider Installation and Administration Guide</i></li> </ul>
Administering Oracle Document Capture	<i>Oracle® Document Capture Administrator's Guide</i>
Administering Oracle Distributed Document Capture	<i>Oracle® Distributed Document Capture Administrator's Guide</i>

## 1.5 Imaging and Process Management Architecture

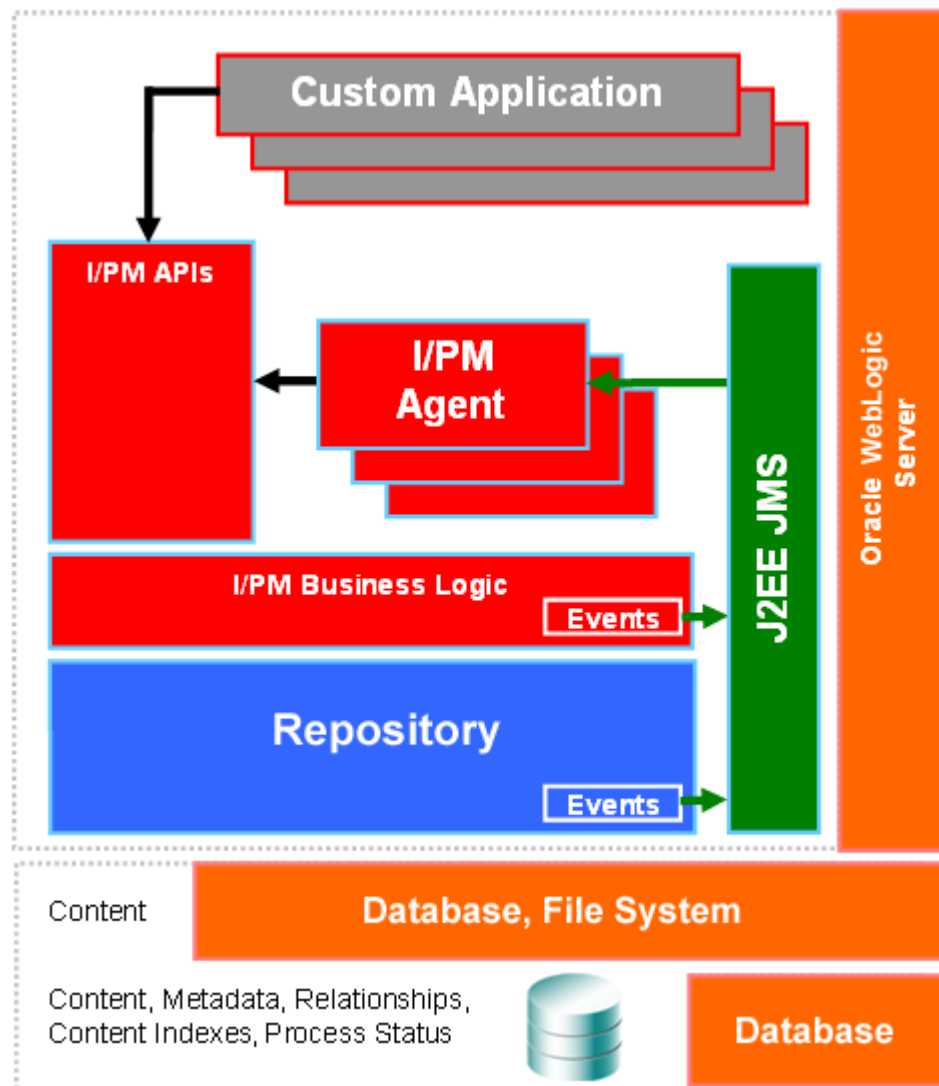
Oracle I/PM business logic produces business objects for defining applications, document control, and security. The following sections describe the underlying technology for Oracle I/PM:

- ["Application Architecture Overview"](#) on page 1-5
- ["Web Services and Java API"](#) on page 1-5
- ["Business Logic and Agents"](#) on page 1-6

## 1.5.1 Application Architecture Overview

Oracle I/PM resides within WebLogic Server, connected to a database. Oracle I/PM events are routed through WebLogic Server using Java Messaging Service (JMS) to communicate with its background agents. Custom applications can interact with I/PM through its set of custom Oracle I/PM application programming interfaces (APIs). For more information about Oracle I/PM APIs, see *Oracle Fusion Middleware Oracle Imaging and Process Management Developer's Guide*.

Figure 1–2 Oracle I/PM Architecture Overview



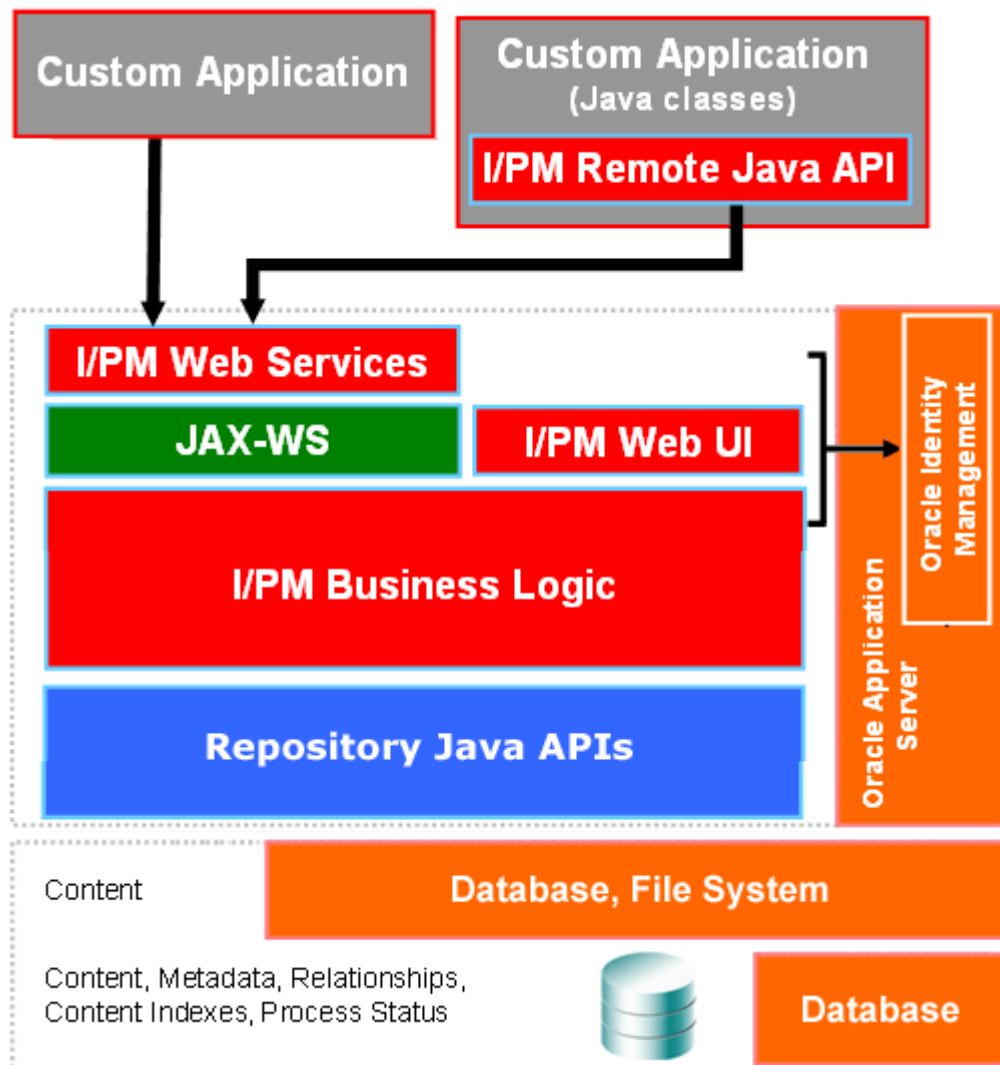
## 1.5.2 Web Services and Java API

Custom applications wishing to integrate with an I/PM system can communicate with I/PM through the I/PM public API. The API is available in two forms:

- through standard web services generated with the Java API for XML Web Services (JAX-WS)
- through Oracle I/PM Java APIs, a set of portable Java class files

The Remote Java API uses the same API as the Oracle I/PM user interface.

Figure 1-3 Oracle I/PM Web Services and Java API



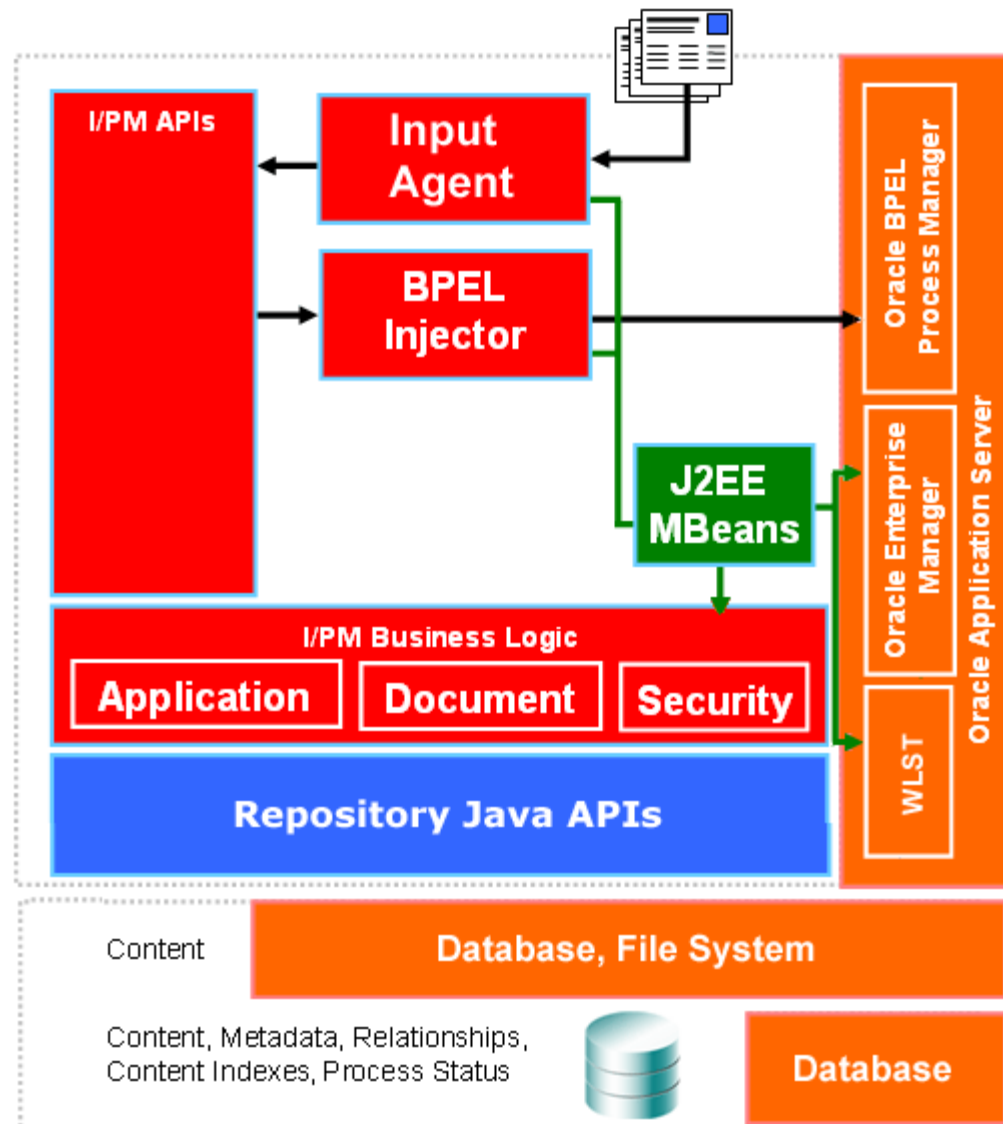
### 1.5.3 Business Logic and Agents

Oracle I/PM provides architectural concepts that are designed to help business managers simplify the process of building imaging solutions. These architectural concepts, such as applications, searches, and inputs, provide convenient constructs around which a business user can organize their solution, grant security to relevant user groups, and finally migrate between differing system instances --development and production for example. Oracle I/PM's public API provides services aligned with these architectural concepts whose implementations reside in I/PM's business logic layer. Although most requests flow directly through these layers producing immediate responses, some tasks are better performed in the background. These tasks are relegated to a collection of Oracle I/PM background processes is known as agents.

Standard Java Management J2EE Beans (or MBeans) are used to configure the operation of Oracle I/PM's business logic as well as its agents. The values of these MBean configuration objects can be manipulated through Oracle Enterprise Manager and WebLogic Scripting Tool, allowing you to choose the best system management tool for your needs.



Figure 1–4 Oracle I/PM Business Logic and Agents



## 1.6 Integration with Key Oracle Technologies

This section contains the following topics:

- ["Integration with Oracle Document Capture"](#) on page 1-7
- ["Integration with an Oracle Document Repository"](#) on page 1-8
- ["Integration with Oracle WebLogic Server"](#) on page 1-8
- ["Integration with Oracle BPEL Server"](#) on page 1-8

### 1.6.1 Integration with Oracle Document Capture

Oracle I/PM integrates with Oracle Document Capture and Oracle Distributed Document Capture to allow you to convert physical documents into an electronic format to be uploaded to Oracle I/PM. Ensure that Oracle Document Capture has been configured with the Oracle I/PM 11g commit driver. Talk to the Oracle

Document Capture administrator or see the administration documentation for Oracle Document Capture or Oracle Distributed Document Capture.

### **1.6.2 Integration with an Oracle Document Repository**

Oracle I/PM leverages Oracle Content Server as a repository for document storage and retrieval. Oracle Content Server supports both out-of-the-box content management services and open, customizable integration options that can manage a broad range of enterprise content such as emails, documents, and images from different content sources. Content Server supports Oracle and SQL Server databases to allow indexing and storage of content in a variety of ways. Depending on the database and configuration, documents and metadata can be stored within the database, on a file system, or a combination of both. Flexible search options allow you to configure the repository to support either metadata searching or full-text searching per I/PM application to provide the most applicable search capabilities.

### **1.6.3 Integration with Oracle WebLogic Server**

Oracle I/PM is designed to leverage many of the features of Oracle WebLogic Server including its standard J2EE architecture, integrations with Oracle security components, scalability including clustering, system management tools like Enterprise Manager, WebLogic Scripting Tools, and Fusion Middleware Control.

### **1.6.4 Integration with Oracle BPEL Server**

A connection to a BPEL server is used to initiate a BPEL process when documents are uploaded to Oracle I/PM, allowing for business process integration across the enterprise.

---

---

## Managing Security

This section contains the following topics:

- ["Security Model Overview"](#) on page 2-1
- ["Managing Definition and Definition Management Security"](#) on page 2-6
- ["Managing System Level Security"](#) on page 2-11

### 2.1 Security Model Overview

Access to documents within Oracle I/PM first requires access to the Oracle I/PM system. The Oracle I/PM system is managed within a WebLogic Server domain and the WebLogic Server credential store is leveraged to grant access to I/PM. Once access to the I/PM is granted, access to Oracle I/PM features and documents requires security rights assigned by an Oracle I/PM administrator.

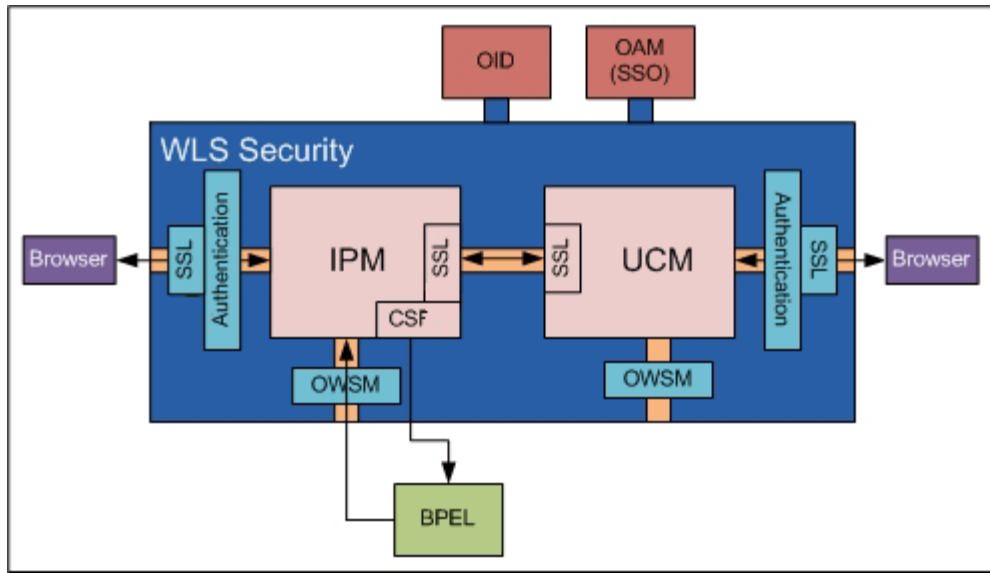
The first person to log in to Oracle I/PM after initial installation is granted full rights to all features, in order to properly set up an Oracle I/PM solution to meet company needs. After the system is properly set up, security rights can be changed or revoked if necessary. Additionally, initial security rights can be reset if the credential store has been changed during set up. See ["Installation Security Initialization"](#) on page 2-2 for more information.

#### 2.1.1 System Access

As managed servers running within a WebLogic Server domain, user and group access to Oracle I/PM and its repository is controlled by WebLogic Server. As such, system security configuration, as well as SSL configuration if desired, is handled through the WebLogic Server console. If additional services are required, such as Oracle Internet Directory or single sign on using Oracle Access Manager, these can be linked to the WLS domain managing I/PM using WebLogic Server controls.

Access to Oracle I/PM through web services is controlled by Oracle Web Services Manager (OWSM) policies. Policies are configured through the WebLogic Server console. Some policies require a keystore be defined. For example, Oracle I/PM must use access credentials stored in Credential Store Framework (CSF) to communicate with a BPEL server or to use SSL. Keystores can be defined using Keytool from the Java Development Kit. Credentials can be added to defined keystores using WebLogic Scripting Tool (WLST).

**Figure 2–1 Oracle I/PM Security Overview**



For additional information, see the following documentation:

**Table 2–1 Additional System Security Documentation**

Task	Where to Go For More Information
Administering Oracle WebLogic Server	<i>Oracle Fusion Middleware Administrator's Guide</i>
Using WebLogic Scripting Tool	<i>Oracle Fusion Middleware WebLogic Scripting Tool Command Reference</i>
Administering Universal Content Management	See the following Oracle Universal Content Management guides: <ul style="list-style-type: none"> <li>■ <i>Managing Security and User Access for Content Server</i></li> <li>■ <i>Managing System Settings and Processes</i></li> <li>■ <i>Managing Repository Content</i></li> <li>■ <i>Getting Started with Content Server</i></li> </ul>

### 2.1.2 Installation Security Initialization

The first person to log in to Oracle I/PM after initial installation is granted full rights to all features, in order to properly set up an Oracle I/PM solution to meet company needs. WebLogic Server managing Oracle I/PM can provide multiple credential store providers to its hosted applications.

During WebLogic Server installation, one of the credential stores was defined as the default. Upon installation, Oracle I/PM, it uses the default credential store. If the credential store changes after the first Oracle I/PM user logs in, system security must be reset. For example, if the security configuration is changed to point to an Oracle Internet Directory (OID) provider or a Microsoft Active Directory provider, you must reset I/PM system security.

To reset system security, do the following:

1. Create or migrate users and groups to the new policy store using the management tools associated with the policy store.
2. Open WebLogic Scripting Tool (WLST) and run `refreshIPMSecurity()` MBean command. The system security is reset. For information on using WLST to run

MBean commands, see ["Using WLST to Change MBeans"](#) on page 3-12 or *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

---

**Note:** During the refresh, users or groups for whom matching identifying information is not found are ignored. As security changes are made, invalid users or groups are removed from the I/PM database.

---

For information on configuring WebLogic Server security providers, such as Oracle Internet Directory (OID) or Microsoft Active Directory, see *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite*.

### 2.1.2.1 Migrating User Store from LDAP Server to Oracle Internet Directory

For information on migrating an existing LDAP Server user store to Oracle Internet Directory, see "Migrating Oracle I/PM Users and Groups from the Embedded LDAP Server to Oracle Internet Directory" in *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite*.

## 2.1.3 Integration with Single Sign-On

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides a wide range of identity administration and security functions, including several single sign-on options for Fusion Middleware and custom Fusions Middleware applications. OAM is the recommended single sign-on solution for Oracle Fusion Middleware 11g installations.

For smaller scale Oracle Fusion Middleware 11g installations, where you do not have an enterprise-class single sign-on infrastructure like Oracle Access Manager, you only need to provide a single sign-on capability within your specific Fusion Middleware application, you can configure a SAML-based SSO solution. If you need to provide single sign-on with other enterprise applications, this solution is not recommended.

If your enterprise uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring SSO with Microsoft Clients may also be an option to consider.

The setup required for each of these SSO solutions is described in the following documents/sections:

**Table 2-2 Single Sign-on Documentation**

For Information On...	See The Following Guide...
Configuring OAM and OSSO	<i>Oracle Fusion Middleware Security Guide</i>
Using Windows Native Authentication for Single Sign-on	<i>Oracle WebLogic Server Admin Console Help: Configure Authentication and Identify Assertion Providers</i>
Using WebLogic SAML for Single Sign-on	<i>Oracle Fusion Middleware Security Oracle WebLogic Server Guide, Section 5.7: Configuring the SAML Authentication Provider</i>

### High-Level Process for Configuring SAML-based Single Sign-On

1. Generate and register certificates.
2. Create the SAML Credential mapping provider instance.

3. Configure a relaying party.
4. Configure source site federation services.
5. Configuring the SAML Identity Assertion provider.
6. Configure destination site federation services.
7. Deploy the <application> server for SAML SSO.
8. Check your configuration.

## 2.1.4 Definition Management Security Rights and Definition Security Rights

Once a user or group has been authenticated and access to Oracle I/PM has been granted, security rights to Oracle I/PM definitions take over.

Oracle I/PM definitions include the following:

- Applications
- Inputs
- Searches
- Connections

---



---

**Note:** Document security is defined within an application and includes security rights to annotations associated with a document. See "[Working with Document Security](#)" on page 2-7 and "[Working with Annotation Security](#)" on page 2-8.

---



---

If a user has been authenticated for access to Oracle I/PM but has not yet been given security rights to any Oracle I/PM definitions or definition management, they are presented with the Home page, but no navigation links are displayed in the [Navigator Pane](#).

To properly administer an I/PM solution, a distinction must be made between definition management rights and definition rights:

- **Definition management security rights** grant a user the ability to create or administer definitions (applications, inputs, searches, and connections).
- **Definition rights** grant a user the ability to view, modify, delete, or manage access to specific definitions, such as an application named *Invoice* or search named *Purchase Order*.

Oracle I/PM definition management security rights and definition rights are managed within the Oracle I/PM user interface.

### 2.1.4.1 Definition Management Rights

Definition management security is done using the [Manage Security](#) pages, accessed from the Manage Security panel of the [Navigator Pane](#). Definition management rights have two levels of security:

Security Right	Definition
Administrator	Grants users or groups full rights to definition management and includes the ability to assign other users or groups Administrator or Create rights.

Security Right	Definition
Create	Grants the ability to create definitions. Users who create a definition are assigned all definition rights for that definition by default.

In order to ensure that only authorized people have access to sensitive documents across an enterprise, there is an additional restriction for users and groups with Administrator rights to search definitions and input definitions. They cannot modify or delete any search definitions or input definitions that are dependent on applications to which they do not have View security rights. Similarly, users with Administrator rights to applications cannot modify or delete any application definitions that are dependent on connections to which they do not have View security rights. This is designed to prevent them from changing definitions in order to gain access to documents that are restricted to them.

For example, as designed, a user in the Human Resources group with Administrator rights to search definitions could view all search definitions, including those for Accounts Payable, but because they do not have View rights to the Accounts Payable application, they would not be able to modify or delete an Accounts Payable search definition.

#### 2.1.4.2 Definition Rights

Definition security is defined when the definition is created and managed using the appropriate panel of the [Navigator Pane](#). Definition rights have four levels of security:

Security Right	Definition
View	Enabled by default. Grants the user or group the right to view this definition.
Modify	Grants the user or group the right to modify all aspects of this definition except for granting security rights.
Delete	Grants the user or group the right to delete this definition.
Grant Access	Grants a user or group the right to grant security rights to others for this definition. If this is the only security level granted, the user can modify only the security information for this definition.

### 2.1.5 Users and Groups

Definition management rights and definition rights are defined for either individual users or for user groups managed through separate security providers to WebLogic Server, such as Oracle Internet Directory (OID) or other. Once authenticated and available to I/PM, users or groups are granted various levels of access to definitions and definition management using the Oracle I/PM user interface. For example, when an application definition is created, a user or group is granted View rights to the application when they are added using the [Application Security Page](#). Additional rights are then specified as required.

Groups are an efficient way to assign security rights to many individuals in an organization with identical access needs. For example, a Managers group could contain managers across an enterprise who need View rights to documents checked in using an application called Resumes, and an HR\_Managers group can be given Write, Delete, and Grant Access rights to the same application in order to upload and delete resumes to and from I/PM or grant access to new managers.

---



---

**Note:** Group membership is loaded at the time a user logs in to Oracle I/PM and remains active throughout the session until the user logs out. If a user is removed from a group while the user is logged in, that user retains the full rights of the group until the user logs out or the session is closed. The new user rights will take effect at the next log in.

---



---

Document security is assigned when an application is defined and only allows security rights to be assigned at the group level.

## 2.2 Managing Definition and Definition Management Security

Definition and definition management security is managed through the I/PM user interface. This section covers the following topics:

- ["Working With Definition Management Security"](#) on page 2-6
- ["Working with Definition Security"](#) on page 2-7
- ["Working with Document Security"](#) on page 2-7
- ["Working with Annotation Security"](#) on page 2-8
- ["Security Example"](#) on page 2-9

### 2.2.1 Working With Definition Management Security

Definition management security is managed using the [Manage Security](#) pages, accessed from the Manage Security panel of the [Navigator Pane](#). To grant, revoke, or copy users and groups rights to applications, inputs, searches or connections, do the following:

#### Changing Existing User and Group Rights To Definitions

1. Click **Manage Security** in the [Navigator Pane](#) to expand the pane and expose the definition type you want to manage.
2. Click the definition type you want to manage:
  - Applications
  - Inputs
  - Searches
  - Connections

The [Manage Security](#) page for that definition type is displayed.
3. Click **Modify**. A toolbar is displayed above the listing of security members and the Create and Administrator security rights columns become active.
4. Enable or disable the rights next to the security member being modified and click **Submit**. The modification toolbar closes and the definition management security has been changed.

#### Revoking Existing Users and Groups Security Rights to Definitions

1. With the Manage Security page displayed, click **Modify**.
2. Select the user or group to delete from the **Security Member** column.



3. Click **Remove**. The user or group is removed from the list and definition management rights for the definition type are revoked.

#### **Granting Users and Groups Rights to Definitions**

1. With the Manage Security page displayed, click **Modify**.
2. Click **Add**. The [Add Security Member Page](#) is displayed.
3. Select **Search Groups** or **Search Users** from the choice list and enter the search criteria, then click **Search**. If no criteria is entered, a listing of all users or groups is returned.
4. Select the user or group to grant rights from the **Security Member** column. Multiple selections can be made by holding down either the Shift key on your keyboard when clicking to select a range, or the Control key when clicking to select non-sequential members.
5. Click **Add**. The Add Security Member page closes and the users or groups are listed in the Security Member column of the security page.
6. Enable or disable the rights next to the security member being added and click **Submit**. The modification toolbar closes and the definition management security has been changed.

## 2.2.2 Working with Definition Security

Definition security is defined when the definition is created and managed using the appropriate panel of the [Navigator Pane](#). For example, Searches are managed using the **Manage Searches** panel in the Navigator Pane.

Managing definition security is detailed in the sections of this guide specific to the definition:

- ["Managing Applications"](#) on page 4-1
- ["Managing Inputs"](#) on page 5-1
- ["Managing Searches"](#) on page 6-1
- ["Managing Connections"](#) on page 7-1

---

---

**Note:** Definitions can be accessed and modified by anyone with Administrator security rights to the definition. Definitions cannot be locked while being modified. Consequently, if the same definition is being modified at the same time by different people, only the last changes submitted are saved.

---

---

## 2.2.3 Working with Document Security

While application definition security and document security are different, document security is defined in the application when it is created. Groups are added and document security rights specified for each group using the [Application Document Security Page](#) when the application is defined. Note that this means if you modify document security rights in an application, all documents currently in that application are affected. The following document rights can be enabled:

Security Right	Definition
View	Grants a user group rights to view documents within a specific application. If a user does not have at least View rights to a document, the document is not listed in a search result when the user executes a search.
Write	Grants a user group rights to upload, update, and copy documents and document metadata within a specific application. Until a user has Write security rights to documents in at least one application, the Upload tool is not visible in the Tools panel of the <a href="#">Navigator Pane</a> .
Delete	Grants a user group rights to delete a specific document from an application. If a user has Delete rights to one application and Write security rights to a second application, then they can move a document from the first to the second application. Note that users with Delete permission are automatically assigned Write permission.
Lock Admin	Grants an admin group rights to unlock any locked document in the application.
Grant Access	Grants a user group rights to assign document rights to other user groups. Note that users with Grant Access rights are automatically assigned Delete and Write security rights.

## 2.2.4 Working with Annotation Security

Annotations are specific to individual documents, but security rights are defined in an application when specifying document security on the [Application Document Security Page](#). Annotation security rights granted when the application is created apply to every document in the application. Changing annotation security rights for a group in an application affects access to all annotations on documents in the application.

Note that even though annotations are associated with and specific to each document in a repository, they are stored separately. Annotations are overlaid on a document, and all or some can be hidden based on the security rights granted a group when the application is defined.

Because annotations are laid on top of documents, documents containing text data can sometimes shift underneath annotations. This can be a concern if text or images overlaid with a redaction annotation shift and become exposed. This is not an issue with improper security rights. It can happen when documents are created using fonts not available to the rendering engine when the document was uploaded. The rendering engine will then substitute fonts which may cause text shift and repagination. For information on how to avoid this problem, see "[Font Errors](#)" on page 10-4.

### 2.2.4.1 Annotation Permissions

There are three levels of security applicable to a document annotation within a specific application.

Security Right	Definition
Annotate Standard	Grants view, create, modify, and delete security rights to all annotations within the application that are not explicitly specified as Restricted or Hidden.
Annotate Restricted	Grants security rights to mark annotations within an application as Restricted and create, modify, or delete annotations marked as Restricted by others. All users have permission to view restricted annotations but must have Restricted annotation rights to create, modify, or delete them.

Security Right	Definition
Annotate Hidden	Grants security rights to mark annotations within an application as Hidden and create, modify, and delete annotations marked as Hidden by others. You must have Annotate Hidden rights to view Hidden annotations.

## 2.2.5 Security Example

Faith, John, Kay and Louis are employees at Company B. They have the following business roles and are members of the following departments and groups:

Name	Department	Role	Group
Faith	IT	Administrator for Oracle I/PM at Company B. She was the first to log into Oracle I/PM after installation and set up all definitions, definition security rights, and definition management security rights. She has full administrative access to all of Oracle I/PM across the enterprise.	IT_Admin
John	HR	The Oracle I/PM administrator for the entire department. Because John is the HR Department administrator, he requires security rights to all Oracle I/PM actions pertinent to HR, but not security rights to anything pertinent to the Accounts Payable department, for example. John is the only individual allowed to create and modify application, search and input and connection definitions for Human Resources.	HR_IT
Kay	HR	Determines salary offerings to potential new employees, making the offer to a potential employee, and receiving the document when it has been accepted. Kay uses references external to the company to determine salary offers but once an offer has been accepted, she uploads the salary acceptance document to the Oracle I/PM system in an application called Offers and annotates it with an Accepted stamp. Once it has been uploaded, stamped, and saved, a BPEL process is initiated that creates an HR new employee file that contains the stamped salary acceptance document. So Kay requires security rights to View, Create and Modify Documents called Offers.	HR_Managers
Louis	HR	Administrative assistant. Updates the database of employees' personal information. He does not use the personal salary information in an Offers document for his job, therefore, Louis would not have security rights to access, search, or upload Offers documents in Oracle I/PM	HR_Users

### Definition Management Security Rights

Within the HR\_Managers and HR\_Users group of Oracle I/PM, Kay and Louis do not have any security rights to define definitions. That is because they do not create or manage applications, inputs, searches, and connections. They only use them.

Faith and John however are granted the following definition management security rights according to the needs of their specific job responsibilities:

Security Right	Application	Input	Search	Connection
Administrator	Faith	Faith	Faith	Faith
Create	John	John	John	John

### Definition Security Rights

All four people need some level of security rights to the Offers definitions. Faith and John need to administer them. Kay must have full rights to upload, annotate (to approve and redact salary information), find, view, and initiate the BPEL process to create the HR new employee file. Louis must have rights to search and view documents to update personal information, but not to view redacted salary information.

Each are granted the following definition security rights according to the needs of their specific job responsibilities:

Security Right	Offers Application	Offers Input	Offers Search	BPEL Connection
View	Faith, John, Kay, Louis	Faith, John, Kay	Faith, John, Kay, Louis	Faith, John
Modify	Faith, John	Faith, John	Faith, John	Faith, John
Delete	Faith, John	Faith, John	Faith, John	Faith, John
Grant Access	Faith, John	Faith, John	Faith, John	Faith, John

### Document Security Rights

Only Kay and Louis work with the documents stored in the Offers application, so only the HR\_Managers and HR\_Users groups would be added on the [Application Document Security Page](#) when the Offers application was defined. Faith and John would not have access to the documents in the application, even though the application definition security rights grant them access to see and modify the Application definition.

Kay and Louis are granted the following document security rights according to their specific responsibilities:

Security Right	Documents	Group Members
View	HR_Managers, HR_Users	Kay, Louis
Write	HR_Managers	Kay
Delete	HR_Managers	Kay
Lock Admin	HR_Managers	Kay
Grant Access	HR_Managers	Kay
Annotate Standard	HR_Managers, HR_Users	Kay, Louis
Annotate Restricted	HR_Managers	Kay
Annotate Hidden	HR_Managers	Kay

These permissions allow Kay to upload and redact salary information from a document into the Offers application, where Louis can search for and view it to get updated personal information without being able to modify the redactions and see the salary information.

## 2.3 Managing System Level Security

Oracle I/PM runs as a managed server within a WebLogic Server domain. Access to Oracle I/PM and the Oracle Content Server repository is controlled by WebLogic Server. System security, including SSL configuration, is handled through the WebLogic Server console. For additional information, see the following:

Task	Where to Go For More Information
Administering Oracle WebLogic Server	<i>Oracle Fusion Middleware Administrator's Guide</i>
Administering Universal Content Management	See the following Oracle Universal Content Management guides: <ul style="list-style-type: none"> <li>■ <i>Managing Security and User Access for Content Server</i></li> <li>■ <i>Managing System Settings and Processes</i></li> <li>■ <i>Managing Repository Content</i></li> <li>■ <i>Getting Started with Content Server</i></li> </ul>

### 2.3.1 Configuring a Fusion Middleware Application to use SSL

You can configure Oracle Fusion Middleware to secure communications between Oracle Fusion Middleware components using SSL, which is an industry standard for securing communications. Oracle Fusion Middleware supports SSL version 3, as well as TLS version 1:

**Table 2-3 SSL Documentation**

For Information On...	See The Following Guide...
Configuring SSL with Oracle Fusion Middleware: Web Tier, Middle Tier, and Data Tier	<i>Oracle Fusion Middleware Administration Guide: Chapter 6, SSL Configuration in Oracle Fusion Middleware</i>
Configuring SSL with Oracle WebLogic Server	<i>Oracle Fusion Middleware Security Oracle WebLogic Server Guide: Chapter 12, Configuring SSL</i>

#### 2.3.1.1 Configuring an SSL Content Server Repository Connection

To connect to a Content Server repository over SSL, the following steps must be taken:

1. Enable SSL on the [Content Server Connection Content Server Settings Page](#)
2. Add and configure an SSL incoming socket provider to the Content Server using the procedure described in "[Configuring SSL Connection to Content Server Repository](#)" on page 7-2.

### 2.3.2 Integrating with BPEL

BPEL integration is detailed in "[Working with BPEL](#)" on page 8-1 and "[Creating a BPEL Connection](#)" on page 7-2.

### 2.3.2.1 Integration Points

Oracle I/PM connects to BPEL at the following times, using different mechanisms for each:

- [Configuration](#)
- [Runtime](#)

#### Configuration

Oracle I/PM connects to a BPEL server when application fields are mapped to BPEL payload elements. To connect, the provider, port, and credential information are passed using a BPEL JNDI-based API. Java Naming and Directory Interface (JNDI) and Enterprise JavaBeans use the T3 protocol, which is a WebLogic Server version of Remote Method Invocation (RMI). This API is used to enumerate the list of available composites, the web services exposed by each composite, and the WSDL URI for each service.

Once a composite and service are selected, the WSDL document is read from the server and parsed to obtain the list of available operations as defined by the service bindings in the WSDL. The protocol for reading the WSDL is HTTP and the address and port used are contained in part of the WSDL URI. Note that the address and port used may be different than the connection hostname and port if the BPEL server is configured with an HTTP front end load balancer such as Oracle HTTP Server (OHS).

Once read, the WSDL is used to obtain the schema of the operation payload so that application fields can be mapped to it.

Details of the connection, composite name, service name, operation name, and application field to payload mapping are stored in the Application.BpelConfig section for use at runtime.

#### Runtime

Runtime communication occurs when BPEL Agent has received a notification that a document has been created in Oracle I/PM and a BPEL process instance must be created for the document. For this communication, the connection, composite, and service name stored in BpelConfig is first used through the BPEL JNDI/EJB API to obtain the service WSDL URI.

The WSDL URI is read to obtain the operation payload schema. The payload schema is used to construct the XML for the payload and the application field values are then inserted into the XML as defined by the mapping.

Once the payload is fully defined to include the mapped field values, the payload is submitted to the BPEL service operation as a web service call using the address as specified in the WSDL document. The web service call is submitted using the HTTP protocol.

### 2.3.2.2 BPEL Connection Configuration

The first step in configuring the Oracle I/PM-BPEL integration is to create a connection definition for the BPEL system within Oracle I/PM. The procedure for creating a BPEL connection is detailed in "[Creating a BPEL Connection](#)" on page 7-2.

It is important to understand that the connection is used when connecting through the BPEL EJB API, so the information is used to communicate through the T3 protocol and not HTTP.

The parameters required for the configuration are described as follows:

Parameter	Details
Provider	<p>Specifies the hostname or names used for the connection. If the BPEL server is a single instance, it is the machine name or IP of the BPEL machine. If the BPEL server is operating within a cluster, this may be a comma separated list of machine names or IP addresses of servers in the cluster or it may be the cluster name.</p> <p>If multiple machines provided in a comma separated list, they must all be defined to use the same port as supplied by the port parameter. If the BPEL server instance in the cluster needs to be defined with different ports, then the cluster name configuration must be used.</p> <p>When the cluster name is used, the cluster name must be defined in domain name server to resolve to the multiple machines within the cluster. Neither Oracle I/PM nor BPEL defines this behavior. Rather, it is defined by the WebLogic support for JNDI in a cluster. For details on clustered JNDI support, see the section "Using WebLogic JNDI in a Clustered Environment" in the <i>Oracle Fusion Middleware Programming JNDI for Oracle WebLogic Server</i> guide.</p>
Port	<p>This specifies the port number used in the connection. For WebLogic, this is the standard listening port for the server. If the SSL option is enabled, then the port provided must be the SSL listening port for the server and T3 communication will use T3S, the SSL version of T3.</p>
SSL	<p>This indicates whether or not the port parameter is the SSL listening port of the BPEL server.</p>
Credential Alias	<p>Provides the alias of a user name and password that are stored in the Credential Store Framework (CSF). These credentials are required to make the remote JNDI connection. The parameter is not the actual user name or password, but rather an alias, or key used to look up the user name and password in the CSF, which encrypted them to provide for proper security.</p> <p>The credential must be created in the CSF before the BPEL connection configuration can be completed. A credential can be created in the CSF in one of two ways: through Enterprise Manager (EM) or through WebLogic Scripting Tool (WLST).</p>

### 2.3.2.3 SSL Configuration

The Oracle I/PM integration can be configured to use SSL to secure communications with the BPEL server instance. The procedure for enabling and configuring an SSL connection to a BPEL server is detailed in "[Configuring SSL for the BPEL Server](#)" on page 7-3.

#### Working with the Default Demo Credential Store Framework and Credential Certificates

Once SSL is enabled on the BPEL server instance, T3 communication to the server will work properly for testing if both BPEL and Oracle I/PM servers are configured to use the default DemoTrust certificates, because WebLogic configures a specific self-signed demo certificate and trust configuration when it is installed. These files are located in \$WL\_HOME/server/lib and are named *DemoIdentity.jks* and *DemoTrust.jks*. By default, WebLogic is configured to use these files.

---

---

**Note:** These files should be used for test and demonstration purposes only. In a production environment, you should obtain proper and valid certificates and follow appropriate procedures for importing and configuring those certificates to establish identity and trust. When properly signed certificates are used and configured properly, SSL will work properly without special configuration.

---

---

You can use the demo certificate to test and confirm a BPEL SSL connection. The SSL configuration allows Oracle I/PM to enumerate the composites and services, but when Oracle I/PM goes to read the WSDL, it will fail. This is because two SSL stacks are being used within the server:

- The WLS SSL stack, which is integrated with the demo identity and trust configuration, is used for T3 communication.
- The native Java SSL stack, which is not integrated with the WebLogic demo identity and trust configuration, is used by the WSLD reader, which uses a native Java API.

To make the WSDL reader work, the Java SSL stack on the Oracle I/PM server instance must be told to trust the self-signed certificate on the BPEL server.

To do this, the `javax.net.ssl.trustStore` system property must be set on the Oracle I/PM managed server JVM to point to the SSL trust store. To configure this to point to the `DemoTrust.jks`, add the following to the `JAVA_OPTIONS` in the `setDomainEnv` script:

```
-Djavax.net.ssl.trustStore=$WL_HOME/server/lib/DemoTrust.jks.
```

After pointing to the `DemoTrust.jks`, restart the managed I/PM server.

This works because all WebLogic Server shares use the same `DemoTrust.jks` file.

At runtime, there is still a potential that when WebLogic is installed and automatically generates an identity keystore (`DemoIdentity.jks`), the identity is keyed to the machine name. In some cases, the identity may only be hostname with no domain (so, `sta00319`, not `sta00319.us.oracle.com`). When Oracle I/PM goes to send the BPEL process message, WebLogic performs hostname verification as part of its SSL handshake that attempts to validate that the hostname in the HTTPS request matches the identity to the server. However, the URL that the BPEL system is giving is full DNS name, not just the hostname. So the handshake fails verification and the communication fails.

The simplest solution for demo purposes is to disable host name verification on the Oracle I/PM system. This is probably the easiest solution, but not a real world production solution. The procedure for this is documented here:

### Configuring New CSF Credentials

You can also create self-signed CSF credentials instead of using the default demo credentials. For information on configuring a CSF credential for a BPEL connection, see "[Configuring a BPEL Connection CSF Credential](#)" on page 7-4.

## 2.3.3 Configuring a Fusion Middleware Application to Use Web Services

WebLogic Web Services are implemented according to the Web Services for Java EE 1.2 specification, which defines the standard Java EE runtime architecture for implementing Web Services in Java. The specification also describes a standard Java EE Web Service packaging format, deployment model, and runtime services, all of which are implemented by WebLogic Web Services.



**Table 2–4 Web Services Documentation**

<b>For Information On...</b>	<b>See The Following Guide...</b>
Web Services consumed by JAX-WS clients	<i>Oracle Fusion Middleware Getting Started with JAX-WS Web Services for Oracle WebLogic Server</i>
Apply OWSM security to Web Services	<i>Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Appendix A: Using Oracle Web Service Security Policies</i>
Use MTOM with Web Services	<i>Oracle Fusion Middleware Securing WebLogic Web Services for Oracle WebLogic Server: Section 2.2: Example of Adding Security to MTOM Web Service</i>
Invoke secured Web Service from BPEL	<i>Oracle® Fusion Middleware Developer's Guide for Oracle SOA Suite: Chapter 7, Invoking a Synchronous Web Service from a BPEL Process</i>  <i>Oracle® Fusion Middleware Developer's Guide for Oracle SOA Suite: Chapter 8, Invoking an Asynchronous Web Service from a BPEL Process</i>
Invoke Web Service using Oracle Server Bus	<i>Oracle® Fusion Middleware Developer's Guide for Oracle Service Bus: 32 WS Transport</i>
Invoke Web Service using Oracle Enterprise Server Bus	<i>Oracle® Fusion Middleware Developer's Guide for Oracle SOA Suite: Chapter 19 Creating Mediator Routing Rules</i>

## 2.3.4 Web Services Security Configuration for I/PM

Access to Oracle I/PM through web services is controlled by Oracle Web Services Manager (OWSM) policies. Policies are configured through the WebLogic Server console. Some policies require a keystore be defined. For example, Oracle I/PM must use access credentials stored in Credential Store Framework (CSF) to communicate with a BPEL server or to use SSL. Keystores can be defined using Keytool from the Java Development Kit. Credentials can be added to defined keystores using WebLogic Scripting Tool (WLST).

Oracle Web Services Manager is designed to be flexible by allowing the end user to define the security policy that will be used rather than to have them predefined.

### 2.3.4.1 Working with Oracle Web Services Manager

When no policy is applied, the services default to using Http Basic Auth security. Http Basic Auth passes user credentials in the HTTP header in the *Authorization* field. The value of this field contains a base64 encode of the username and password. The *BasicUserToken* client class is intended to use this form of authentication. Because the password is transmitted unencrypted when using basic authentication, Oracle I/PM includes a configuration MBean called **RequireBasicAuthSSL**, allowing the service to require that SSL be used with this form of authentication.

For more robust security, OWSM policies can be applied to the services. OWSM policies can enforce various ws-security token usage, including message level encryption, transport level encryption, or supplying credentials in the SOAP header rather than HTTP header. Because SSL can be specified as part of the applied policies, the *RequireBasicAuthSSL* MBean setting does not apply when security policies are in use.

### 2.3.4.2 Setting Policies on Services

During domain creation, the Oracle I/PM application is supplied with a default deployment plan defined in the applications directory, although this plan is not yet assigned to the deployment. The default plan uses the *wss\_username\_token\_service\_*

*policy* which enforces simple username and password in the ws-security soap header and requires no encryption. This default plan assigns the *wss\_username\_token\_service\_policy* to all Oracle I/PM services.

To assign the default plan, do the following:

1. Login to the WebLogic Server Console.
2. Click **Deployments**, enable **imaging** in the Deployments table, then click **Update**. The Update Application Assistant is displayed.
3. Click **Change Path** next to Deployment plan path. Changing the source path does not redeploy with a new plan.
4. Using the links in the **Current Location** field, browse to `$MW_HOME/user_projects/applications/<domain_name>/server/ipm` and enable the **Plan.xml** file.
5. Continue through the wizard to complete the deployment.

Once this process is complete, services all have the *wss\_username\_token\_service\_policy* applied.

If you want to change the policies at runtime, do the following:

1. Login to WebLogic Server console
2. Click **Deployments** and then expand **imaging** in the Deployments table. A list of Oracle I/PM web services is displayed. You may need to scroll to see them.
3. Click the service name for each service you want to configure and do the following:

---

**Note:** No policy should ever be applied to the DocumentContentService service.

---

- a. Select the **Configuration** tab
- b. Select the **Ws-Policy** tab. The currently applied policy is displayed.
- c. Click the service end point. For example, the ApplicationServicePort. A listing of Available Message Policies and Chosen Message Policies is displayed.
- d. Select the currently applied policy from the Chosen Message Policies list on the right and click the arrow to move it to remove it from the Chosen Message Policy list.
- e. Select the preferred policy from the Available Message Policies list on the left and click the arrow to move it to the Chosen Message Polices list on the right.

---

**Note:** You need to apply the same policy to all Oracle I/PM services with the exception of DocumentContentService. No policy should be applied to the DocumentContentService service.

---

4. When changes are made to all services, update the deployment with the newly edited plan.
  - a. Enable **imaging** in the Deployments table on the main deployments page, then click **Update**. The Update Application Assistant is displayed.
  - b. Check the top option to update only the deployment plan.
  - c. Click **Finish**.

To facilitate deployment, alternative deployment plan descriptors have been created. They are located in `$MW_HOME/user_projects/applications/<domain_name>/server/ipm/plan/imaging-ws.war/WEB-INF` directory. You can copy any one of the policy-`<X>` files on to `weblogic-webservices-policy.xml` in that same directory, and then update the deployment with the plan. Note that for the default plan, `weblogic-webservices-policy.xml = policy-username_token.xml`.

### 2.3.4.3 API Usage

It is important that all services be assigned the same policies. In the client API the `ServicesFactory` is coded to obtain the appropriate client policy from the provided `UserToken`, along with the required configuration parameters for the policy, and use that client policy configuration on all service interfaces. In order to work, client code must know what service policy is in effect. The following are examples of how to code the client for each of the predefined policy types within the `UserToken` class.

The `UserToken` class exposes a number of new properties to facilitate configuring client side policies. The set of parameters exposed is a subset of the full set of possible Oracle Web Service Manager parameters, but is commonly used. Note that the properties are wrappers around a name/value pair map which is directly exposed using the `securityParameters` property. All properties in this map get passed along to the web service request context and therefore any OWSM policy is usable.

### 2.3.4.4 Examples

The following examples are detailed here:

- ["No Policy: Http Basic Auth"](#) on page 2-17
- ["Policy: wss\\_username\\_token\\_client\\_policy"](#) on page 2-17
- ["Policy: wss11\\_username\\_token\\_with\\_message\\_protection\\_client\\_policy"](#) on page 2-18
- ["Policy: wss10\\_saml\\_token\\_client\\_policy"](#) on page 2-18
- ["Policy: wss11\\_saml\\_token\\_with\\_message\\_protection\\_client\\_policy"](#) on page 2-18

#### **Example 2-1 No Policy: Http Basic Auth**

The simplest and the default. Because this is the default the `BasicUserToken` provides the client implementation.

```
UserToken userToken = new BasicUserToken("weblogic", "weblogic");
ServicesFactory.login(userToken, wsurl);
```

`BasicUserToken` is functionally equivalent to the following.

```
UserToken userToken = new UserToken();
userToken.setUsername("weblogic");
userToken.setPassword("weblogic");
```

When OWSM policies are applied to the services, the `WsmUserToken` is used to provide the client side policy configurations. This is done as follows for various policies.

#### **Example 2-2 Policy: wss\_username\_token\_client\_policy**

This is the simplest policy.

```
WsmUserToken userToken = new WsmUserToken ("weblogic", "weblogic");
```

```
userToken.setClientPolicy(WsmUserToken.USERNAME_TOKEN_POLICY);
ServicesFactory.login(userToken, wsurl);
```

**Example 2-3 Policy: wss11\_username\_token\_with\_message\_protection\_client\_policy**

Message\_protection policies provide message level encryption. However to make them work, client and server keystores need to be configured. See the section ["Working With Keystores"](#) on page 2-19 for how to create and configure the key stores. When a keystore is used client side by a JSE client, the client code needs to configure the location, type, and password for the keystore. The client side keystore must contain a *RecipientAlias* which is the key used to encrypt the message sent to the server. This same key must exist server side to decrypt and encrypt the responses.

```
WsmUserToken userToken = new WsmUserToken ("weblogic", "weblogic");
userToken.setClientPolicy(WsmUserToken.USERNAME_TOKEN_MP_POLICY);
userToken.setKeystore(".\\config\\default-keystore.jks", "JKS", "welcome");
userToken.setRecipientAlias("orakey");
```

If this policy were being used server side, for example, from a web app or servlet, the key store would be configured underneath JPS security and therefore the client would not need to specify the keystore configuration parameters. This behavior can be replicated in JSE as well by setting the *oracle.security.jps.config* environment property to point to a jps-config file.

```
System.setProperty("oracle.security.jps.config", ".\\config\\jps-config.xml");
WsmUserToken userToken = new new WsmUserToken ("weblogic", "weblogic");
userToken.setClientPolicy(WsmUserToken.USERNAME_TOKEN_MP_POLICY);
```

Once JPS is configured for the client, you can also leverage the Credential Store Framework (CSF) to define the username and password credentials. See the section ["Working with the CSF through WLST"](#) on page 2-20. To use, create the credentials on the server and copy them to your client. You can use any alias in the credential store, but the standard default is the alias *basic-credentials*.

```
System.setProperty("oracle.security.jps.config", ".\\config\\jps-config.xml");
WsmUserToken userToken = new WsmUserToken ();
userToken.setClientPolicy(WsmUserToken.USERNAME_TOKEN_MP_POLICY);
userToken.setCsfKey("basic.credentials");
```

**Example 2-4 Policy: wss10\_saml\_token\_client\_policy**

This policy is similar to username token but only the passes the username in the saml token header. Also, its not encrypted and therefore not secure.

```
WsmUserToken userToken = new WsmUserToken ("weblogic");
userToken.setClientPolicy(WsmUserToken.SAML_TOKEN_POLICY);
```

**Example 2-5 Policy: wss11\_saml\_token\_with\_message\_protection\_client\_policy**

This option encrypts and signs the message using keys and certificates from the keystore. This is the most secure of all the options and requires the most configuration. Typically, service-side code has the user identity in the form of a *java.security.Principal* object. So server-side code might look as simple as the following.

```
WssUserToken userToken = new WssUserToken (principal.getUserName());
userToken.setClientPolicy(WsmUserToken.SAML_TOKEN_MP_POLICY);
ServicesFactory.login(userToken, wsurl);
```

For JSE, the jps configuration trick works here as well.

```
System.setProperty("oracle.security.jps.config", ".config\\jps-config.xml");
WssUserToken userToken = new WssUserToken ("weblogic");
userToken.setClientPolicy(WsmUserToken.SAML_TOKEN_MP_POLICY);
```

Without JPS configuration, the client can provide the full set of keys. Since this seems like an extreme use case, the UserToken does not provide full access to all of the key properties required by the policy. This demonstrates how any policy parameters can be supplied through the securityParameters property.

```
WssUserToken userToken = new WssUserToken ();
userToken.setUsername("weblogic");
userToken.setClientPolicy(WsmUserToken.SAML_TOKEN_MP_POLICY);
userToken.setKeystore(".\\config\\default-keystore.jks", "JKS", "welcome");
userToken.getSecurityParameters().put(SecurityConstants.ClientConstants.WSS_ENC_
KEY_ALIAS, "orakey");
userToken.getSecurityParameters().put(SecurityConstants.ClientConstants.WSS_ENC_
KEY_PASSWORD, "welcome");
userToken.getSecurityParameters().put(SecurityConstants.ClientConstants.WSS_SIG_
KEY_ALIAS, "orakey");
userToken.getSecurityParameters().put(SecurityConstants.ClientConstants.WSS_SIG_
KEY_PASSWORD, "welcome");
```

In these configuration examples, the same key is used in all cases. In a production environment, the keystore should contain client and service-side certificates or signing and encrypting respectively.

### 2.3.4.5 Working With Keystores

For any of the message\_protection policies, client and server keystores need to be configured. In a production environment, you should obtain proper and valid certificates and follow appropriate procedures for importing and configuring those certificates to establish identity and trust. This example is meant to provide a workable solution for development and testing. You can create a keystore using a build in JDK tool called KeyTool. You use the following command to generate a keystore.

```
>keytool -genkey -alias orakey -keyalg RSA -keystore default-keystore.jks
Enter keystore password:  β welcome
Re-enter new password:  β welcome
What is your first and last name?
  [Unknown]:  Joe Smith
What is the name of your organizational unit?
  [Unknown]:  Human Resources
What is the name of your organization?
  [Unknown]:  Our Company
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=Joe Smith, OU=Human Resources, O=Our Company, L=Unknown, ST=Unknown, C=US
correct?
  [no]:  yes

Enter key password for <orakey>
      (RETURN if same as keystore password):  β RETURN...so welcome
>
```

You can list keys in a keystore with

```
> keytool -list -keystore default-keystore.jks
```

The above example creates the single common key used in all of the examples above. The same default-keystore.jks was used on both the server and the client.

### 2.3.4.6 Working with the CSF through WLST

The following command can be used from WLST to add credentials into the keys store. However, to use these commands, you have to run WLST from the `$ORACLE_HOME/common/bin` directory rather than from the WLS home common/bin. In JDeveloper, this is located in `Oracle/Middleware/jdeveloper/common/bin` and not `Oracle/Middleware/wlserver_10.3/common/bin`. From the `$ORACLE_HOME/common/bin`, run `wlst.sh` (Linux) or `wlst.cmd` (Windows) and the run `connect()`.

The full set credential store commands are documented in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*, but the main two used in these examples are:

```
createCred(map="oracle.wsm.security", alias="<alias>", user="<user>",  
password="<pwd>")
```

and

```
listCred(map="<map>", key="<key>")
```

The credential store can store any userid and password pair accessed by an alias. For WSM policies, the acsf aliases are used to obtain keystore aliases and passwords. These CSF aliases are configured in the `jps-config.xml` file in the following element.

```
<!-- KeyStore Service Instance -->  
<serviceInstance name="keystore" provider="keystore.provider"  
location="./default-keystore.jks">  
  <description>Default JPS Keystore Service</description>  
  <property name="keystore.type" value="JKS"/>  
  <property name="keystore.csf.map" value="oracle.wsm.security"/>  
  <property name="keystore.pass.csf.key" value="keystore-csf-key"/>  
  <property name="keystore.sig.csf.key" value="enc-csf-key"/>  
  <property name="keystore.enc.csf.key" value="enc-csf-key"/>  
</serviceInstance>
```

The keystore needs one alias named `keystore-csf-key` that includes the password for the key store. In this example, it is the first password entered in the keytool, above. The username here is ignored. Then the keystore needs a second alias named `enc-csf-key`. The username is a keystore alias and the password is the private password for that keystore alias, which is the second password in the keytool, above.

---

---

## Changing Configuration Settings

This section describes the configuration options available to an Oracle I/PM administrator and how they are accessed. It contains the following topics:

- ["Configuration Overview"](#) on page 3-1
- ["Post-Installation Configuration"](#) on page 3-2
- ["Configuration of Repository Options"](#) on page 3-2
- ["Exporting and Importing Definitions"](#) on page 3-8
- ["File Size Limits"](#) on page 3-9
- ["Configuring MBeans"](#) on page 3-9
- ["Setting Font Variables"](#) on page 3-14
- ["Configuring Display of Seconds in Search Results"](#) on page 3-15
- ["Configuring I/PM Logging"](#) on page 3-16

### 3.1 Configuration Overview

Imaging and Process Management runs within Oracle WebLogic Server and connects to one or more Oracle Content Server repositories. Configure Oracle I/PM in one of the following ways:

- Use Content Server repository product configuration tools to set configuration settings, such as adding users and managing user roles and system access rights. For more information, see the Oracle Universal Content Management *Managing Security and User Access for Content Server* guide.
- Use the Oracle I/PM web-based interface for the creation and modification of applications, searches, inputs, and connections to set application security, searches security, document security, repository connections and BPEL configurations.
- Use WebLogic Scripting Tools (WLST) to configure MBeans. For more information about changing Oracle I/PM custom MBeans, see ["Configuring MBeans"](#) on page 3-9.
- Use Enterprise Manager (EM) to configure MBeans. For more information about using Enterprise Manager to configure MBeans, see *Oracle Fusion Middleware Administrator's Guide*.

## 3.2 Post-Installation Configuration

The first user who logs in to Oracle I/PM is granted security rights to complete the following post-installation configuration steps:

- connecting to an Oracle Content Server repository
- configuring the AgentUser and GDFontPath MBeans
- setting environment variables for OutsideIn
- connecting to a BPEL server

These steps and the full installation procedure are documented in the *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite*.

## 3.3 Configuration of Repository Options

Oracle I/PM uses the functionality of the Oracle Content Server to store and retrieve documents. Documents are stored and secured based on criteria specified in the application into which they were uploaded. You must create a connection for Oracle I/PM to recognize the repository you are using. For more information about creating a connection, see "[Managing Connections](#)" on page 7-1.

Configuring repository options, such as defining the maximum number of search results returned or if the full-text of a document can be indexed, must be done through the Oracle Content Server repository. It is recommended that you make all necessary repository configuration prior to defining any application, input, search, or connection objects in Oracle I/PM. For more information, see the Oracle Universal Content Management *Managing Repository Content*, *Managing System Settings and Properties* and *Getting Started with Content Server* guides.

### 3.3.1 Storage Management

Oracle Content Server uses file store providers to determine where and on what type of media content is stored. Oracle Content Server does not have the option to move documents from one media to another based on time, nor can documents be deleted based on lifecycle. File store providers are configured in Oracle Content Server independent of I/PM. If you need to move content to a different file store or delete documents and all revisions, you must do so explicitly using the Oracle Content Server Repository Manager tool. For more information on working with the Oracle Content Server repository, see the Oracle Universal Content Management *File Store Provider Installation and Administration Guide*, *Managing Repository Content* and *Getting Started with Content Server* guides.

For more information about configuration options provided by I/PM on the Storage Policy page, see "[Application Storage Policy Page](#)" on page A-28.

### 3.3.2 Repository Capacity

An Oracle Content Server repository can get full to the point of reducing its operating efficiency at which time it will not accept any new Oracle I/PM applications. However, you may continue to upload documents to existing applications in that repository.

An Oracle Content Server repository is considered full if any of the following are true:

- The number of security groups exceeds the value of the environment variable IpmMaxGroupLimit.



- The number of roles assigned permission to security groups exceeds the value of the environment variable `IpmMaxGroupRoleLimit`.
- The number of metadata fields exceeds the value of the environment variable `IpmMaxMetadataFields`.
- The Content Server configuration setting `IpmRepositoryForceFull=True`  
Setting `IpmRepositoryForceFull` equal to `True` allows you to configure Content Server to identify itself as full to I/PM in order to prevent additional applications from being created. This does not prevent documents from being uploaded.

To get additional space for applications, do one of the following:

- Install an additional Oracle Content Server repository as a master, or set it as a proxy to the main Content Server. For information on how to configure a master or proxy server, see the Oracle Universal Content Management *Managing System Settings and Processes* guide.
- Increase the values of the `IpmMaxGroupRoleLimit` environment variable (maximum number of security group versus security group role mappings that have privileges assigned before a Content Server is considered full) and `IpmMaxMetadataFields` environment variable (maximum number of metadata fields before a Content Server is considered full) by editing the `config.cfg` file directly or by using the Oracle Content Server administrative server. The default value for both of these variables is 500. For more information about changing Oracle Content Server environment variables, see the Oracle Universal Content Management *Managing System Settings and Processes* guide.

### 3.3.3 Storage Media

Oracle Content Server defines where and how it stores content using file store providers, which are configured in Oracle Content Server and can be a combination of any media supported by Oracle Content Server. Because document storage location is not defined by the media being used for storage, the term *volume* is used to represent a storage location when defining an application in the I/PM user interface. Note that Oracle I/PM cannot be used to create or define a volume. It only connects to one defined and configured by a Content Server administrator from within Oracle Content Server.

### 3.3.4 Oracle Content Server File Store Provider Rules

File Store Provider functionality within Content Server allows you to have more control over how and where files are stored and managed within Content Server. For example, typically you would only be able to store all content on a single file system in the vault and weblayout directories. However, using `FileStoreProvider`, you have the ability to store content across multiple file systems, while also being able to store content within a database.

#### 3.3.4.1 Disabling the Repository Weblayout Directory

Content Server traditionally uses a weblayout directory on a file system to store content in a format for viewing in a web browser, even though the main storage volume may be set up in a database. This can allow for faster retrieval of content when content server is being used to manage a web site, or can be used to store a secondary file used to describe the primary content item, but it doesn't have much use in an I/PM solution. Retaining a web layout directory for an exclusively I/PM solution would copy files to a web layout directory that would never get used, taking up unnecessary storage space. It is recommended that any file store provider configured

for use as an I/PM volume should have the weblayout functionality disabled. For information about disabling the weblayout directory, or about FileStoreProvider in general, see the Oracle Universal Content Management *File Store Provider Installation and Administration* guide.

### 3.3.5 Additional Oracle Content Server Components

Oracle I/PM uses Oracle Content Server components to provide compatibility and additional options. Ensure that they are installed and enabled.

#### 3.3.5.1 Required Components

The following component is required to be installed and enabled to ensure compatibility with Oracle Content Server:

- **IpmRepository:** Sets global profile rules to support document profiles specific to Oracle I/PM applications, for compatibility with other products supported by Content Server, including:
  - Folders
  - Universal Records Manager (URM)
  - Information Rights Management (IRM)

For more information, see "[Oracle Content Server Document Profiles](#)" on page 3-4.

#### 3.3.5.2 Optional Components

The following components provide useful functionality that can be leveraged by Oracle I/PM:

- **OracleTextSearch:** Provides full-text indexing capability.
- **ContentTracker:** Provides audit capability for content access.
- **Folders:** Provides integration with LDAP and would allow I/PM to be configured to automatically add documents to specific folders.

### 3.3.6 Oracle Content Server Document Profiles

When an application is created in Oracle I/PM, a corresponding profile and set of profile rules are created in the Content Server repository. The application profile is created with **Exclude non-rule fields** enabled so that fields from other applications are not shown at the same time. Because of this, any field not specifically identified in a profile rule is not displayed on the various document related pages, such as the check in form or the document information page.

#### 3.3.6.1 Global Profile Rules

The IpmRepository component sets up global profile rules to group system fields and ensure their display when an application profile is created. These profiles are created or updated each time Content Server is started.

---

---

**Note:** You can disable the automatic update of the global profile rules by setting the Content Server configuration setting IpmUpdateProfileRules to 0 (zero). For information about configuring Content Server, see the Oracle Universal Content Management *Managing Repository Content* and *Getting Started with Content Server* guides.

---

---

The IpmRepository component creates the following rules:

Name	Description
IpmStandardFields1	Groups standard fields such as Title, Author, Security Group, etc.
IpmStandardFields2	Groups standard fields such as Content ID and Revision, etc.
IpmStandardFields3	Groups standard fields such as Release Date and Expiration Date, etc.
IpmSystemFields	Groups Imaging system fields
IpmFolderFields	Groups Folder fields
IpmUrmFields	Groups Universal Records Management fields
IpmIrmFields	Groups Information Rights Management fields

Because these rules are global, they do not need to be referenced by a specific profile in order to be active.

---

**Note:** If any of the global rules are defined without any fields, then the **Is global** rule with priority setting is turned off. For example, this happens if URM has never been installed on a Content Server instance.

---

### 3.3.6.2 Application Profile and Profile Rules

When an application is created, a profile and rules are created to handle the display of the application fields. The rules created for a profile group the application fields and provide any default values for those fields. The following table describes the rules:

Name	Description
IpmApp_<X>_Fields	Groups the application fields
IpmApp_<X>_Defaults	Sets defaults for Imaging system (Security Group, IPN Application ID) fields and application specific fields

In the rule names above, <X> is replaced with an internal application identifier. These rules are not global, and need to be reference by a profile to become active.

A profile is created for the application and is given IpmApp\_<X> as the profile name, where <X> is an internal application identifier. The label for the rule is the application name.

### 3.3.6.3 Working With Folders

Oracle I/PM does not automatically assign application documents to a folder. However, by modifying an application profile and profile rules, you can automatically assign documents to a specific folder. To modify application rules to automatically assign documents to a specific folder, do the following:

1. Create a new contribution folder to hold the application content. Make a note of the folder's identifier, for example 932000007.
2. Add a new profile rule. Make a note of the name. For example App\_<X>\_Folder.
3. Add the Folder field. The Folder field is the xCollectionID field.
4. Set Type to **Info Only**.

5. Enable **Use default value** and set the default value to the folder identifier obtained above. For example, 932000007. This allows people using the Content Server check in form to see the assigned folder.
6. Enable **Is derived field** and set the default value to the folder identifier obtained above. For example, 932000007. This allows the value to be set upon check in from any source. For example, IPM upload.

Setting the rule in this manner will not allow users to move content from one folder to another. This includes the trash folder. To allow movement between folders and deleting content, change derived value to use custom script and add something similar to:

```
<$if not (IDC_SERVICE like "COLLECTION_DELETE_LOT|COLLECTION_RESTORE_ITEM")$>
  <$dprDerivedValue="932000007"$>
<endif$>
```

7. Now edit the application profile rule.
8. Add the rule just defined (App\_X\_Folder) to the rules section.

---



---

**Note:** If an application is modified in Oracle I/PM, and the modification includes an application name change, then the rule you just added to the application profile will need to be added again.

---



---

### 3.3.6.4 Working With Universal Records Manager

Oracle I/PM does not automatically assign documents to a retention category or life cycle. However, by modifying an application's profile and profile rules, you can automatically assign documents to a retention category or life cycle. The following steps are for assigning a retention category value. If you wish to assign a life cycle, substitute xLifeCycleID for xCategoryID.

1. Create a new retention category. Make a note of the retention category identifier. For example, you could use App X Category.
2. Add a new profile rule. Make a note of the name. For example, you could use App\_X\_Category\_rule.
3. Add the Retention Category field. The Retention Category field is xCategoryID.
4. Set the Type to **Info Only**.
5. Enable **Use default value** and set the default value to the retention category identifier obtained above. For example, App X Category. This allows people using the Content Server check in form to see the assigned category.
6. Enable **Is derived field** and set the default value to the retention category identifier obtained above (App X Category). This allows the value to be set upon check in from any source. For example, IPM upload.

---



---

**Note:** If the category to which you are mapping the documents is a category that is a records-only category, you will also need to add a field for xIsRecord and set its default and derived values to "1".

---



---

7. Now edit the application's profile rule.
8. Add the rule just defined (App\_X\_Category) to the rules section.

---



---

**Note:** If an application is modified in Oracle I/PM, and the modification includes an application name change, then the rule you just added to the application profile will need to be added again.

---



---

### 3.3.6.5 Working With Information Rights Manager

Oracle I/PM does not automatically assign application documents to an IRM classification. However, by modifying an application profile and profile rules, you can automatically assign documents to an IRM classification.

1. Add a new profile rule. Make a note of the name. For example App\_X\_IRM).
2. Add the IRMProtection field. The IRMProtection field is xIRMProtection.
3. Set the Type to **Info Only**.
4. Enable **Use default value** and set the default value. This value must match an Oracle IRM context. This allows people using the Content Server check in form to see the assigned IRM classification.
5. Enable **Is derived field** and set the default value. This value must match an Oracle IRM context. This allows the value to be set upon check in from any source. For example, IPM upload.

---



---

**Note:** If IRM is not configured correctly, or the value does not match a valid context, you will be unable to check content into Content Server because it will fail IRM validation.

---



---

6. Now edit the application profile rule.
7. Add the rule just defined (App\_X\_IRM) to the rules section.

---



---

**Note:** If an application is modified in Oracle I/PM, and the modification includes an application name change, then the rule you just added to the application profile will need to be added again.

---



---

### 3.3.6.6 Working With WebCenter Spaces

Oracle I/PM documents are not automatically accessible within WebCenter Spaces, but documents can be automatically assigned to Folders visible within WebCenter Spaces. Manual configuration and modification of an application profile and profile rules are required to ensure that I/PM documents will be accessible.

1. Configure Content Server and Oracle I/PM to use the same LDAP-based identity store that Oracle WebCenter has been configured to use.

For information on configuring WebCenter and Content Server to use an LDAP identity store, see *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

2. Configure Content Server as the bridge between I/PM and WebCenter Document Service using an I/PM supported version of Java.
3. WebCenter Spaces' Document Service uses the Folders component, and I/PM must be configured to automatically specify Folders for checked in content. For more information regarding configuring I/PM with Folders, see the section "[Working With Folders](#)" on page 3-5.

For further information regarding WebCenter Spaces integration with Oracle Content Server, see *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

## 3.4 Exporting and Importing Definitions

When deploying an Oracle I/PM solutions, you must define applications, searches, inputs, and connections. Applications are the core of Oracle I/PM. An application is a type of management container for documents, defining a metadata set, storage information, and security for all documents within it. Searches enable a user to quickly retrieve a document they need, and an input definition is used to map information from an input file to the metadata fields defined in an application. Applications, searches, inputs, and connections are defined using the Oracle I/PM user interface.

You can reuse the application, search, and input definitions by exporting the desired definition to an XML file format. You can then import that definition file into other systems to make those same items available there. For example, if you created an Invoices application for Accounts Receivable and now want to create a similar application for Accounts Payable, you can start with the imported application definition and then modify it as necessary in the Oracle I/PM user interface.

Note that when exporting an application, you can explicitly export it by selecting the application and following the procedure detailed in "[Exporting Definitions](#)" on page 3-8. However, you can also implicitly export application definitions by selecting a search or input that references the application and following the export procedure. Explicitly exported application definitions can modify existing application definitions if you specify them to do so. Implicitly exported application definitions cannot modify existing definitions.

### 3.4.1 Exporting Definitions

To export a definition file, do the following:

1. Under **Tools** in the navigator pane, select **Export Definitions**. The [Export Definitions: Export Comments Page](#) page displays.
2. Enter any comments about the exported definitions, such as the need for exporting, and click **Next**. The [Export Definitions: Applications Page](#) is displayed.
3. Enable any application definitions needed for export.
4. Click **Next**. The [Export Definitions: Searches Page](#) is displayed.
5. Enable any search definitions needed for export.
6. Click **Next**. The [Export Definitions: Inputs Page](#).
7. Enable any input definitions needed for export.
8. Click **Next**. The [Export Definitions: Summary Page](#) is displayed.
9. Review the information on the summary page and ensure it is accurate. Use the navigation train to go back and make any changes. When satisfied, click **Create Export File**.

### 3.4.2 Importing Definitions

After you have created an definition file, complete the following steps to import it:

1. Under **Tools** in the navigator pane, click **Import Definitions**. The [Import Definitions: File Location Page](#) displays.

2. Enter the path or click **Browse** to navigate to the definition file that contains the exported definitions you want to import. Add any necessary comments, and click **Next**. The [Import Definitions: Select Imports Page](#) displays.

---

**Note:** If using your keyboard rather than your mouse to select the Browse button, use the **Space** bar to execute the Browse button function and open the dialog box. The Enter key does not execute the Browse button function.

---

3. Select the action for each application, input and search definition to be imported. Options are:
  - **Overwrite:** the imported definition overwrites the current definition
  - **Add:** the imported definition is added to the system

---

**Note:** Remember that implicitly exported application definitions cannot overwrite existing definitions. Implicitly exported application definitions are those applications that were not explicitly selected for export, but are referenced by a search or input definition that was selected.

---

If more than one repository is available, select the repository to be used with the imported definition. Click **Next**. The [Import Definitions: Validate Imports Page](#) displays.

4. Select your decisions about whether to change the Security, Document Security, Storage Policy, and BPEL settings of the imported definitions. Click **Submit**. The Import Summary page displays.

Click **Close**.

## 3.5 File Size Limits

File size limitations are primarily a factor when retrieving a document for viewing. System architecture, hardware limitations, network load and other factors can influence document retrieval times and cause the viewer to time out. Oracle I/PM has been optimized to store tiff image files of sizes to 200KB. If the documents you need to upload and view are larger than to 200KB, test the performance of with those files in the specific network architecture you are planning to use while simulating peak network load.

## 3.6 Configuring MBeans

Java Management Beans, called MBeans, are part of the greater Java Management eXtensions (JMX) standard which defines ways for administration applications to configure and control Java applications externally. At installation, Oracle I/PM registers its MBeans with the hosting application server's MBean server. This allows other applications to interact with Oracle I/PM's configuration data. This includes WebLogic Scripting Tools (WLST) and Oracle Enterprise Manager MBean browser.

### 3.6.1 Oracle I/PM MBeans

The following table describes MBeans specific to Oracle I/PM.

MBean	Description
AgentUser	<p>Specifies account used by all Oracle I/PM agents use to login. Requires a restart.</p> <p>Value limits: Any String field that security store can handle.</p> <p>Default: None (empty string)</p>
CacheAgeLimit	<p>Render page-cache timeout duration (used to set the JOC IdleTime). Takes effect at server restart.</p> <p>Value limits: Cache idle time in minutes</p> <p>Default: 60 minutes</p>
CacheLocation	<p>Render page-cache temp file location. Takes effect at server restart.</p> <p>Value limits: Value is used as third parameter to File.createTempFile; a valid system file path spec.</p> <p>Default: If value is not supplied, system temp location is used.</p>
CheckInterval	<p>Configures how often (in minutes) input agent checks for work. Takes effect on the next check cycle.</p> <p>Value limits: Min=1, Max=60</p> <p>Default: 15 minutes</p>
DefaultColorSet	<p>Name of default skin used by UI if user has not set a preference. If blank, the default is blafplus-rich. String values that are skin names found in the UI are valid. Takes effect on next login.</p> <p>Value limits: Any valid skin names on the install</p> <p>Default: blafplus-rich</p>
DefaultSecurityGroup	<p>The default security group to use for document security when creating an application. If blank the user must specify the group during application creation. Takes effect on next application creation.</p> <p>Value limits: Any valid security group name.</p> <p>Default: None (empty string)</p>
GDFontPath	<p>Path referencing a location containing TTF font files for use by OIT rendering package. Takes effect on session bean initialization.</p> <p>Value limits: This value is specifically for LINUX and is ignored on Windows systems. It is an OIT requirement.</p> <p>Default: No default provided - this must be explicitly defined.</p>
InputAgentRetryCount	<p>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.</p> <p>Default: 3</p>

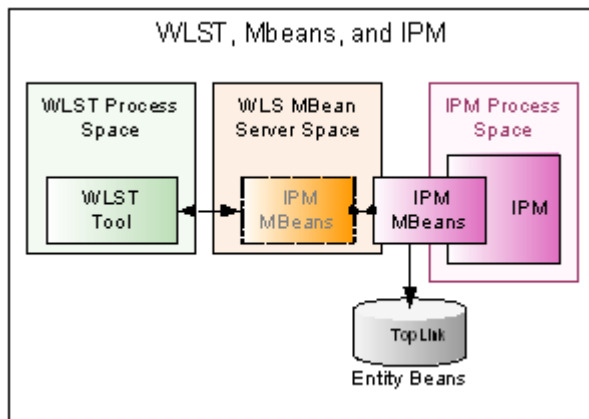


<b>MBean</b>	<b>Description</b>
InputDirectories	<p>Provides list of directories stored as CSV strings where input sources should look for work. Takes effect immediately.</p> <p>Value limits: Any valid directory path the server can access with a minimum of 1 entry and maximum of 10.</p> <p>Default: IPM/InputAgent/Input</p>
IPMVersion	String file of the I/PM version number.
JpegImageQuality	<p>Specifies desired compression level used when creating JPG images. Takes effect each image rendering.</p> <p>Value limits: Value in range 0-100</p> <p>Default: 75</p>
LogDetailedTimes	<p>Provides detailed logging of UI activity with durations of many of the UI activities. Takes effect at server restart. Turn on LogDetailedTimes only when you are experiencing long delays with the UI because it floods the log with entries which you generally only need to identify slowdowns.</p> <p>Value limits: True - Turns on the logging; False - Turns off the logging</p> <p>Default: False</p>
MaxSearchResults	<p>Maximum number of rows a search is allowed to return. After this value is reached, the search is stopped. Takes effect on next search.</p> <p>Value limits: Min = 1, Max = 10000</p> <p>Default: 1000</p>
RequireBasicAuthSSL	Forces the use of SSL in all web service communication when set to true. By default, it is false. Note that the RequireBasicAuthSSL setting only applies when no HTTP Basic Authentication is in use because no OWSM security policies have been applied.
SampleDirectory	<p>Specifies which directory holds the sample data for the input UI. Takes effect immediately.</p> <p>Value limits: Any valid directory path to which the server has access.</p> <p>Default: IPM/InputAgent/Input/Samples</p>
TiffCompressionType	<p>Compression algorithm used when creating TIFF images. Takes effect each time a TIFF is generated.</p> <p>Value limits: Allowable values are: LZW and FAX4</p> <p>Default: LZW</p>
UseAdvancedAsDefaultViewerMode	<p>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.</p> <p>Value limits: True - Makes the advanced viewer the default; False - Makes the basic viewer the default</p> <p>Default: True</p>

### 3.6.2 Using WLST to Change MBeans

WebLogic Server Scripting Tool (WLST) is a command line scripting environment that you can use to create, manage, and monitor WebLogic server domains including Oracle I/PM MBeans. For a list of custom Oracle I/PM MBeans, see "[Oracle I/PM MBeans](#)" on page 3-9. WLST commands are issued on a command line and provide a way to navigate through WebLogic Server domains into MBean servers and down to specific application MBeans. From there, you can change Oracle I/PM MBean settings. To view or change these settings, you can use the WebLogic Server Scripting Tool (WLST) provided with WebLogic server. To learn more about the WLST commands and command line protocol, see *Oracle Fusion Middleware Administrator's Guide*.

**Figure 3–1 WebLogic Scripting Tool Use Within Oracle I/PM Architecture**



Note that:

- Strings must be surrounded by single quotation marks (')
- Boolean must be entered as: Boolean(true) or Boolean(false)
- MBean settings are case-sensitive
- Long must be entered as: Long(123456)

The following procedure describes how to use WLST to view Oracle I/PM MBean settings.

1. Log in to the target system on which the Oracle I/PM installation resides.
2. Open a command-line shell.
3. Change directories to Middleware Home.

For Windows systems, enter:

```
>cd ('%MW_HOME%\wlserver_10.3\common\bin')
```

For Linux systems, enter:

```
>cd ('$MW_HOME/wlserever_10.3\common\bin')
```

4. Start WebLogic Server Scripting Tool.

For Windows systems, enter:

```
wls> wlst.cmd
```

For Linux systems, enter:

```
wls> ./wlst.sh
```

This starts the WLST shell in a disconnected mode.

5. Connect to the WebLogic administration server using the correct I/PM managed server port. For example:

```
wls:/offline>connect()
wls:/base_domain/serverConfig> connect()
Please enter your username [weblogic]: <enter>
Please enter your password [welcome1]: <enter>
Please enter your server URL [t3://localhost:7001]:t3://localhost:16000
Connecting to t3://localhost:16000 with userid weblogic...
Successfully connected to managed Server 'IPM_server1' that belongs to domain
'base_domain'.
```

Note that the port listed in the above example is the default listing port of the I/PM managed server and not that of the WLS administration server.

6. Switch to the custom MBean server where the Oracle I/PM MBean is exposed.

```
wls:/base_domain/serverConfig> custom()
```

Location changed to custom tree. This is a writable tree with no root.

```
wls:/base_domain/custom> ls()
drw-   EMDomain
drw-   JMImplementation
drw-   com.oracle.igf
drw-   com.oracle.jdbc
drw-   com.oracle.jps
drw-   oracle.adf.share.config
drw-   oracle.adf.share.connections
drw-   oracle.as.util
drw-   oracle.dfw
drw-   oracle.dms
drw-   oracle.dms.event.config
drw-   oracle.imaging
drw-   oracle.j2ee.config
drw-   oracle.joc
drw-   oracle.jocssl
drw-   oracle.jrf.server
drw-   oracle.logging
```

The `ls()` command in this example lists the contents of the custom directory. Locate the `oracle.imaging` entry. Note that if the `oracle.imaging` MBean is not listed, you are not connected to the correct I/PM managed server port and should disconnect and then reconnect using the correct port.

7. The MBeans are arranged in a directory structure, so change to the directory that contains the Oracle I/PM settings.

```
wls:/base_domain/custom> cd('oracle.imaging')
wls:/base_domain/custom/oracle.imaging> cd('oracle.imaging:type=config')
```

8. Now you are in the directory that contains all of the Oracle I/PM settings. Enter the `ls()` command to see all of the configuration options and their settings, or the `get('<name>')` function to get a specific value.

```
wls:/base_domain/.../> ls()
.
.
```

```
.  
wls:/base_domain/.../> get('TiffCompressionType')  
'FAX4'
```

9. Use the `set(name, value)` function to change a value. See ["Oracle I/PM MBeans"](#) on page 3-9 for information about when the change will take effect because it differs for each MBean.

```
wls:/base_domain/.../> set('CheckInterval', 5)
```

### 3.6.3 Using Enterprise Manager to Set an MBean Value

If you use Enterprise Manager (EM) to monitor server performance, you may want to also use the Enterprise Manager System MBean Browser to view and change Oracle I/PM MBean values. To use the System MBean Browser, following this procedure:

1. Log on to Enterprise Manager.
2. Under Deployments, click the appropriate target (such as `IPM_server1`). The Summary page displays.
3. To view MBeans, select System MBean Browser on the WebLogic Server menu. On the left navigation pane, under Application Defined MBeans, expand `oracle.imaging`. Select the appropriate server.
4. Expand the appropriate server.
5. Expand config.
6. Double-click config to display the list of Oracle I/PM MBeans and their settings.
7. Change the appropriate MBean setting and click Apply. See ["Oracle I/PM MBeans"](#) on page 3-9 for information about when the change will take effect because it differs for each MBean.

## 3.7 Setting Font Variables

Using unsupported fonts in your documents can cause the document to be unreadable, create incorrect text formatting, or cause shifting of data on text documents, including potentially exposing redacted content. For example, a redaction annotation is laid on top of a document. If that document is rendered using fonts on one system and the redaction is placed over a word based on the rendering, different fonts on a different system may cause the document text to render in a slightly different position. It would be possible for the data hidden beneath a redaction annotation to move and be exposed.

To help ensure that rendered text does not mistakenly shift beneath a redaction, ensure that all client machines being used to place redactions have the same fonts as the I/PM server. This allows the OutsideIn rendering engine to render the document using the same fonts as the client machine used to place the redaction. Once a TIFF image of the redacted file is rendered, redactions and text are displayed as an image, without use of fonts, unless a person has the proper security rights to see redacted text. This ensures that a user cannot try to force text to shift below a redaction by deleting a font and attempting to view the document, because the viewed document has already been converted to an image.

If running I/PM on a UNIX system, ensure that your UNIX servers are configured to use TrueType fonts (\*.ttf or \*.ttc files). Use WLST to set the I/PM server `GDFontPath` configuration MBean to include one or more paths to supported font files. If

GDFontPath cannot be located, the current directory is used, which may or may not have the required fonts.

---



---

**Note:** Setting the GDFontPath is required for UNIX systems only. It is not required to be set on Windows systems.

---



---

### 3.7.1 Configuring the AgentUser and GDFontPath MBeans

Three agents run outside of Oracle I/PM, so you need to log into the Oracle I/PM system using a standard user in the security store. Oracle I/PM assigns security to this user name, which you need to configure as the agent user, by setting the AgentUser MBean. You can also set the GDFontPath MBean.

#### To configure the AgentUser and GDFontPath MBeans with Fusion Middleware Control:

1. Access the Oracle I/PM domain in Oracle Enterprise Manager 11g Fusion Middleware Control at the following URL:

```
http://adminServerHost:adminServerPort/em
```

For example:

```
http://machineName:7001/em
```

2. Log in as the Administration user (for example, `weblogic`).
3. In the navigation tree, expand **Application Deployments**, and then click **imaging(11.1.2.0)**.
4. On the **Application Deployment** menu, select **System MBean Browser**.
5. On the System MBean Browser page, close the **com.bea** folder under **Configuration MBeans**.
6. Expand the **oracle.imaging** folder under **Application Defined MBeans**.
7. Expand the **Server: IPM\_server1** and **config** folders.
8. Click **config**.
9. Set **AgentUser** to **agentadmin**.
10. Set **GDFontPath** to the location of your TTF files on the UNIX system (for example: `/usr/share/X11/fonts/TTF`).
11. Click **Apply**.
12. Restart the Oracle I/PM server.

## 3.8 Configuring Display of Seconds in Search Results

By default, the Oracle Content Server repository is not set to return seconds to Oracle I/PM when returning time information for display in a search results table. If you require seconds to be displayed in a search results table date and time field, you must configure the Content Server repository to return seconds using the SystemProperties applet. In order to run the SystemProperties applet, you must first temporarily disable JpsUserProvider. To configure Content Server to return seconds, do the following:

1. Log in to the target system on which the Oracle Content Server installation resides.
2. Open a command-line shell.

3. Change directories to `<domain_home>/ucm/cs`.  
For Windows systems, enter:  

```
>cd ('%UCM_HOME%/ucm/cs')
```

  
For Linux systems, enter:  

```
>cd ('$UCM_HOME/common/bin')
```
4. Run ComponentTool and disable JpsUserProvider using the following command:  

```
./bin/ComponentTool --disable JpsUserProvider
```
5. Launch the SystemProperties applet by using the following command:  

```
./bin/SystemProperties
```

  
The SystemProperties applet is displayed.
6. In the SystemProperties user interface, click the **Localization** tab.
7. Select the Locale you want to modify. For example, **English-US**, then click **Edit**. The Configure Locale dialog box is displayed.
8. Remove the square brackets ([]) from around the seconds in each field to require seconds be displayed. For example, change  

```
M/d/yy {h:mm:ss} {aa}{zzz}!mAM,PM
```

  
to  

```
M/d/yy {h:mm:ss} {aa}{zzz}!mAM,PM
```
9. Click **OK**. The Configure Locale dialog box closes.
10. Run ComponentTool and enable JpsUserProvider using the following command:  

```
./bin/ComponentTool --enable JpsUserProvider
```
11. Restart Content Server. For information on how to restart Content Server, see the Oracle Universal Content Management *Getting Started with Content Server* guide.

## 3.9 Configuring I/PM Logging

Configure and view log files for Oracle I/PM using Oracle Enterprise Manager (EM) by doing the following:

1. Log in to Enterprise Manager.
2. Expand the WebLogic Domain navigation tree for Application Deployments and select your imaging server. The status of your Oracle I/PM server is displayed.
3. On the **Application Deployment** menu, select **Logs** then **Log Configuration**.
4. Select the **Log Levels** tab, which allows you to control the logging level. Under the Logger name section, expand **Root Logger, oracle**, then **oracle.imaging** to display the logger names associated with Oracle I/PM. From here you can change the logging level which affects the severity level of error messages collected. See the Enterprise Manager documentation for information on the available logging level options.
5. Optionally enable the **Persist log level state across component restarts** to ensure logging levels between restarts.
6. Click **Apply**.

7. Select the **Log Files** tab to display the Handler Name, Log Path, Log File Format and Rotation Policy of the logging file. From here you can create a new file, or copy, edit, or view the configuration of an existing file.

For more information about managing log files, log levels, and diagnostic data, see the *Oracle Fusion Middleware Administrator's Guide*.





---

---

## Managing Applications

This section describes how to create and configure applications in Oracle I/PM. It contains the following topics:

- ["Application Overview"](#) on page 4-1
- ["Creating An Application"](#) on page 4-2
- ["Modifying an Existing Application"](#) on page 4-7

### 4.1 Application Overview

Applications are the core of Imaging and Process Management. Consider an application as a type of management container for documents. An application defines a metadata set, storage information, and BPEL process configuration for all documents within it. When creating an application, you assign permissions, associate metadata, define indexing options, determine a storage policy, and specify BPEL processes to initiate as part of the document business flow.

You can reuse an existing application definition within Oracle I/PM by exporting the desired definition to a transportable format via XML. You can then import that definition file into other systems and then modify it appropriately. For more information about exporting and importing, see ["Exporting and Importing Definitions"](#) on page 3-8.

#### 4.1.1 Document Overview

Documents, either in the original electronic file format or as images of physical documents, are stored in an application. A document consists of a file and the following information that describes the file:

- ID: Unique identifier
- Name: Original file name when added to the system
- Properties: File size, MIME type, file name, creator, lock, version, application ID and application name
- Field Values: Application metadata
- Permissions: Access to documents
- Supporting Documents: Associated artifacts such as text or images
- Annotations: Online notes within the document such as an approval stamp or text.

Because documents reside in applications, they also have an application ID and application name as properties. An application defines the metadata set for all

documents within that application. When a document is added to the system, the application determines the metadata set, and the user or input file supplies the field values. If an application metadata set is modified, it affects all documents in the application.

With the proper permissions, users can make annotations to documents. These annotations are also stored in the system.

### 4.1.2 Uploading Documents

Uploading, sometimes called ingesting, is the process for getting documents into the Oracle I/PM system, associating the document with application metadata, and indexing. Document metadata and full-text of a document is indexed at the time of uploading based on the application in which it resides. The indexing process varies depending on the format of a document and the way it is uploaded.

Once a document is uploaded, it can be retrieved by searching and printed or viewed. The viewing process uses Oracle Outside In Technology which supports more than 400 file formats. To learn more about Oracle Outside In Technology, see the Oracle OutsideIn Technology web site at <http://www.oracle.com/technologies/embedded/outside-in.html>. Once uploaded, the document can be viewed using the Oracle I/PM document viewer. The advanced mode of the document viewer also allows the annotating a document.

Upload a document in one of the following ways:

- Upload individual documents using the Upload Document Tools interface.
- Upload documents in bulk using the Oracle I/PM input Agent. For more information, see "[Managing Inputs](#)" on page 5-1.
- Use a custom application to upload documents using the Oracle I/PM APIs. For more information about using Oracle I/PM APIs, see the *Oracle® Fusion Middleware Developer's Guide for Imaging and Process Management*.

For more information about uploading documents, see *Oracle® Fusion Middleware User's Guide for Imaging and Process Management*.

## 4.2 Creating An Application

---

---

**Note:** The Oracle I/PM user interface displays different panels in the navigator pane based on your permissions. Unless you have application system permissions, or administration permissions to at least one individual application, the Manage Applications panel is not displayed in the navigator pane. You must have either Create or Administrator permission to create an application. The user creating an application must also have at least View permission to the connection (repository) being used.

---

---

Applications assign permissions and associate metadata to documents at the time they are uploaded. Open the Manage Applications panel in the navigator pane of the Oracle I/PM user interface to start the process of defining an application.

You will complete the following tasks in the following order:

1. [Specifying General Properties](#): Name and describe the application
2. [Defining Application Fields](#): Define fields used and indexed in the application

3. [Assigning Application Security](#): Assign application security permissions.
4. [Assigning Document Security](#): Assign document security permissions.
5. [Assigning a Storage Policy](#): Define a storage policy for content.
6. [Configuring BPEL Integration](#): Configure any BPEL processes for content within the application.
7. [Reviewing Application Settings](#): Review application settings and submit.

---

---

**WARNING:** Changes to the repository DOCMETA table caused by creating, deleting, or modifying an application can potentially cause a problem on an active repository server if any other operation is also affecting the table. While this is unlikely, it can cause data loss, and so it is important to coordinate changes to an application with idle time on the Oracle Content Server repository server.

To help mitigate any potential problems, multiple Oracle Content Server repository instances can be used to isolate business units so that any one application change has less impact on the enterprise organization.

---

---

## 4.2.1 Specifying General Properties

You must provide each application with a name. The application name is displayed in the Applications panel in the navigation pane. A brief description of the application is also displayed on the application summary page when an application is selected. It is also required that you specify the repository for the application. Once the application is created, you cannot change the repository selection. To view this page, see "[Application General Properties Page](#)" on page A-24.

To specify the application general properties, do the following:

1. Expand the Manage Applications panel in the [Navigator Pane](#) and click the **Create Application** icon. The [Application General Properties Page](#) is displayed.
2. Enter a name for the application the **Name** field. The application name is displayed to users on the Upload Document page and to system administrators when creating inputs and searches. This field is required.
3. Enter a description of the application in the **Description** field. This description is displayed beneath the title on the application Summary page, when using the Document Upload Tool, and when you hover your cursor over the application name in the Manage Applications panel in the [Navigator Pane](#).
4. Select a repository for the application from the field. Multiple Content Server repositories can be used for different applications to balance the load. This field specifies which Content Server repository to use for this application. Once defined and the application is created, the repository cannot be changed. This field is required.
5. Specify if you want full-text indexing of content. Enabling Full-Text Search indexes metadata and the full-text of any documents with text information. Images of documents do not contain text information, and so cannot be full-text indexed. For example, a Microsoft Word has text that can be indexed, but a TIFF image of a Microsoft Word document does not, and so cannot be indexed.
6. Click **Next** to go to the [Application Field Definitions Page](#).

## 4.2.2 Defining Application Fields

Fields defined for an application track metadata associated with content in an application. You can specify one of four types of field definitions, whether they are required, and if they are indexed to improve searching speeds. You must define at least one field. The four available field types are:

- **Text:** Field accepts text string. Possible string length is specified in Length element.
- **Number:** Field accepts integers from -2.14 billion to 2.14 billion.
- **Decimal:** Field accepts 1 to 15 non-negative decimal values such as 1.5. The decimal scale is set in the Scale element.
- **Date:** Field accepts date in the regional short-date format.

All field types can be indexed. Enabling indexing of a metadata field applies only to that field. The information specified will appear under the Field Definitions category on the application Summary page. Indexes are applied to the underlying repository database tables. The application of either too many or too few indexes will be detrimental to the system's performance. Generally, indexes should be applied to those fields that will be the core of the document searching that will be performed. Defining this list of fields should be done as part of the business process analysis with the additional help of a database administrator.

You can add and remove fields in applications when creating and modifying applications. There is a restriction that when adding or modifying an application you cannot delete an existing field and re-add it with the same name during the process. If this happens, click **Cancel** and start again.

For more information on available field types and options and to view the page, see "[Application Field Definitions Page](#)" on page A-25.

To define fields, do the following:

1. On the [Application Field Definitions Page](#), click **Add** and for this example, select **Number** as the type of field and enable **Required** and **Indexed**.
2. Change the name of the field to a descriptive name. For example, **Lease Number**.
3. Click **Add**, select **Date** as the field type, and enable **Required** and **Indexed**.
4. Change the field name to a descriptive name, for example, to **Lease Expiration**.
5. Click the **Edit Default Value** icon to enter a default value, for example, to **12/31/2009**. The default value is only a suggestion to users. The field is not automatically set to this value when left blank.

Note that there is also an option to add a picklist to any field by clicking the **Add Picklist** icon in the Picklist column. Although we won't use picklists in this example, use this icon to add a list of selectable options for the metadata field. Leading and trailing spaces on picklist items are not retained. Click the pencil icon in the Picklist column to edit an existing list, or click the Remove Picklist icon to delete an existing picklist. If a picklist is defined, the user must select from the picklist to populate the field and cannot enter data directly into the field.

6. Click **Next** to go to the [Application Security Page](#).

## 4.2.3 Assigning Application Security

---



---

**Note:** The user creating an application must also have View permission to the connection (repository) being used.

---



---

Permission to view, modify, delete and grant access to an application is assigned at the user or group level when defining an application on the [Application Security Page](#). To assign application security permissions, do the following:

1. On the [Application Security Page](#), click **Add**. The [Add Security Member Page](#) displays. Type a user or group name or click **Search** to display a list of users from which to select.
2. Select the user you want to add. The user name is added to the Display Name column on the [Application Security Page](#).
3. Enable the permissions you want to assign to this user by selecting the field in the appropriate column. Options are:
  - **View:** Enabled by default. Grants the user or group the right to view and upload into this application.
  - **Modify:** Enable to grant the user or group the right to modify all aspects of this application except for granting security rights.
  - **Delete:** Enable to grant the user or group the right to delete this application.
  - **Grant Access:** Enable to grant a user or group the right to grant security rights to others for this application. If this is the only security level granted, the user can modify only the security information for this application.

A user with Grant Access permission can grant themselves all other rights. At least one user must be given Grant Access rights.

4. Click **Next** to go to [Application Document Security Page](#).

### 4.2.3.1 Copying Permissions From One User to Another User

You can copy the permissions from one user to another by completing the following steps:

1. Select and highlight the user whose permissions you want to copy from the Display name column and click **Copy**. The [Add Security Member Page](#) displays.
2. Select the new user to whom you are copying the permissions. The new user's name is displayed in the Display Name column with the copied permissions enabled.
3. Click **Next** to go to the [Application Document Security Page](#).

## 4.2.4 Assigning Document Security

Assigning access and modification permissions to documents are managed separately from assigning access and permissions to applications. This protects an application from being inadvertently modified by users who need greater access to content. Likewise, sensitive documents are protected from those with rights to access and modify applications.

Permission to view, write, delete, grant access, lock, and annotate documents is assigned at the group level on the [Application Document Security Page](#).

To assign document security permissions, do the following:

1. On the [Application Document Security Page](#), click **Add**. The [Add Security Member Page](#) is displayed.
2. Type a group name or select the group you want to add from the list. This group name is added to the Display Name column of the [Application Document Security Page](#).
3. Enable the permissions you want to assign to the group. Note that anyone in a group with Grant Access permission can grant the group all other rights. Document security adds permissions for modifying either metadata or document content, and the ability to lock documents to prevent changes.
4. Click **Next**.

### 4.2.5 Assigning a Storage Policy

Oracle Content Server does not support time-based storage of content, so currently there is a single storage stage with an indefinite duration. The user can only choose the volume to apply. Once chosen, the content stays on that volume indefinitely. Note that the status of the volume chosen is not indicated on the user interface for creating an application.

To create an application storage policy, complete the following steps:

1. Select the name of the storage volume used to store documents from the Document Storage Volume field. This may be a file store, database, or storage device.
2. Select the name of the storage volume used to store annotation from the Supporting Content Storage Volume field. This may be a file store, database, or storage device.
3. Click **Next** to go to the [Application BPEL Configuration Page](#).

### 4.2.6 Configuring BPEL Integration

Processes in BPEL export and import information by using Web Service interfaces. A BPEL server defines services that can be used by other applications. If a connection has been defined to a BPEL server, the BPEL Configuration option is enabled in the Application definition navigation train. To add a BPEL configuration to an application, do the following:

---

---

**Note:** The user creating an application must also have View permission to the BPEL connection being used.

---

---

1. On the [Application BPEL Configuration Page](#), click **Add**. The [BPEL Server Properties Page](#) is displayed.
2. Select the connection from the Connection field and click **Next**. The [BPEL Component Properties Page](#) is displayed.
3. Select the component properties of the business process being configured. Composite, Service, and Operation are required values. Click **Next**. The [BPEL Payload Properties Page](#) is displayed.
4. Select a Mapped Value for each Payload Element. Note that if selecting Format Value, you can construct a value from parts of text and application fields using the

[Edit Format Value Page](#). For example, you would use this page to construct custom URLs or to concatenate multiple values together into a single value.

5. Click **Finish** to exit BPEL configuration and return to the main application definition navigation train. The [Application BPEL Configuration Page](#) is displayed.
6. Click **Next** to move to the [Application Review Settings Page](#).

You can also modify or delete an existing BPEL configuration in an existing application by doing the following:

1. Click on an existing application name in the Manage Application panel of the navigator pane. The [Application Review Settings Page](#) is displayed.
2. Click **Modify**. The [Application General Properties Page](#) is displayed.
3. Click **BPEL Configuration** in the Application navigation train. Note that the BPEL Configuration option in the navigation train is only available if a connection to a BPEL server has been defined. The [Application BPEL Configuration Page](#) is displayed.
4. Click **Modify**. The [BPEL Server Properties Page](#) is displayed. Follow the procedure in the section "[Configuring BPEL Integration](#)" on page 4-6.

#### 4.2.7 Reviewing Application Settings

To review application settings, do the following:

1. From the [Application Review Settings Page](#), review the application settings and ensure they are correct.
2. Make any necessary changes by clicking **Back** to return to the necessary section, or click the specific section in the navigation train to return the section directly.
3. Once you are satisfied that the application is correct, return to the [Application Review Settings Page](#) and click **Submit**.

### 4.3 Modifying an Existing Application

Once an application is created, all aspects of the application can be modified with the exceptions of which repository is used and what scale is used for decimal field definitions.

---

---

**WARNING:** Changes to the repository DOCMETA table caused by creating, deleting, or modifying an application can potentially cause a problem on an active repository server if any other operation is also affecting the table. While this is unlikely, it can cause data loss, and so it is important to coordinate changes to an application with idle time on the Content Server repository server.

To help mitigate any potential problems, multiple Content Server repository instances can be used to isolate business units so that any one application change has less impact on the enterprise organization.

---

---

---

---

**Note:** Unlike documents, definitions cannot be locked while being modified. Consequently, if the same definition is being modified at the same time by different people, only the last changes submitted are saved.

---

---

To modify an existing application, do the following:

1. From the navigator pane, click the application name to change. The application summary page displays.
2. Click **Modify**. The [Application General Properties Page](#) is displayed.
3. In the navigation train, select the page on which to make changes. For information on the page options, see the pertinent subsection of the section "[Creating An Application](#)" on page 4-2, or the appropriate page in the [User Interface](#) appendix.
4. When you have changed all the appropriate settings, select **Review Settings**. The [Application Review Settings Page](#) is displayed.
5. Review the application settings and ensure they are correct.
6. Make any necessary changes by clicking **Back** to return to the necessary section, or click the specific section in the navigation train to return the section directly.
7. Once you are satisfied that the application is correct, return to the [Application Review Settings Page](#) and click **Submit**.

---

---

**Note:** Content Server cannot store null values in a numeric field. When an application containing documents is modified to have a number field, search results will display -1 for that new field on documents that were in Content Server prior to when the new field was added. When a new document is uploaded after the field is added and the number field is left blank, search results will display 0 for the number field value.

---

---



---

---

## Managing Inputs

This chapter contains the following topics:

- ["Enabling Input Agent"](#) on page 5-1
- ["Understanding Input Files"](#) on page 5-2
- ["Using Input Filing Commands"](#) on page 5-3
- ["Creating Input Definitions"](#) on page 5-4
- ["Input Agent Processing"](#) on page 5-6
- ["Checking Results and Error Files"](#) on page 5-8

### 5.1 Enabling Input Agent

---

---

**Note:** The AgentUser MBean must be set for Input Agent to work. To check if AgentUser has been set, view the AgentUser MBean using the Enterprise Manager MBean browser or WLST. For information on setting the AgentUser MBean, see ["Configuring the AgentUser and GDFontPath MBeans"](#) on page 3-15.

---

---

The Input Agent is an Oracle I/PM service used to upload and index documents in bulk into the Oracle I/PM system. This section describes how to enable the Input Agent and create the input files for batch uploading in Oracle I/PM. Input Agent indexes Oracle I/PM documents in bulk by using an application definition, input definition, and a specially formatted text file called an input file. The input file specifies the list of images to index and the metadata to associate with them in the application. Input Agent is multithreaded and is configurable to handle large and small volumes of data.

To enable the Input Agent, do the following:

1. Start the managed servers, using WLST or the Enterprise Manager MBean browser, navigate to the Oracle I/PM configuration MBean.
2. If the AgentUser MBean has not been set, set a valid user name from the credential store. Input Agent creates documents with the user name, so it is important to pick a user associated with the agent activities. You must restart the I/PM server after changing this parameter.
3. Set CheckInterval to a value that is appropriate for your environment. The CheckInterval MBean is a system setting that specifies how many minutes to pause before checking for new work to do. The default is 15 minutes.

4. Set the `InputAgentRetryCount` to control how many times a job can be retried after it has failed. The default is 3, after which the job is placed in the failed directory.
5. Set the `InputDirectories` MBean to specify the paths to the input files. This value can be expressed as an array of locations. If using a multinode installation of I/PM, this location is shared among all the Input Agents and must be accessible by all agents. If Input Agents are on different machines, this must be a shared network.

---

---

**Note:** In order to process input files, the Input Agent must have the appropriate permissions on the input directory. The Input Agent requires that the user account that is running the WLS service have read and write privileges to the input directory and all files and subdirectories in the input directory. These privileges are required so that Input Agent can acquire read/write locks, move input files and create subfolders under the input directory.

---

---

After completing these steps, the Input Agent is active and ready to process work. Once you create an application (see "[Creating An Application](#)" on page 4-2) and input definitions (see "[Creating Input Definitions](#)" on page 5-4), the Input Agent will start processing jobs.

## 5.2 Understanding Input Files

The Input Agent performs work based on input files. These are simple text documents, similar to CSV (comma-separated values) files, that contain lists of files and associated metadata to index into the Oracle I/PM system. The input file can use different encodings as long as the correct encoding is specified in the input definition. Input Agent looks for all input files that match the input mask of the input definition and not the sample file that is used to define the input definition. Note that sample files are not required when creating an input through the API. They are only used when creating an input through the user interface so a user can see the data to help choose the columns.

---

---

**WARNING:** Input file masks must be unique to the Oracle I/PM system and cannot overlap. Input Agent only processes an input file for one input and will not restage a file to be processed again for a different input definition. The order in which inputs are processed is random so it is unknown as to which input will pick up a shared input file.

---

---

A sample input file looks like:

```
C:\IPMData\Input Files\print\NewPrintstreams\doc16.txt|NEW
ORDER|10/06/94|B82L|218482
C:\IPMData\Input Files\print\NewPrintstreams\doc17.txt|NEW
ORDER|10/06/94|N71H|007124
C:\IPMData\Input Files\print\NewPrintstreams\doc18.txt|NEW
ORDER|10/06/94|B83W|24710
```

The detailed structure of an input file is defined as:

```
[path to document file][delimiter][metadata value
1]<[delimiter]<metadata value 2> ... <delimiter>>
```

- Items in brackets ([ ]) are required and items in angle brackets (<>) are optional.
- `path to document file` is the location of the tiff, jpeg, doc or other file type that is being saved to Oracle I/PM. It must be a path that is accessible to the user account running the Input Agent.
- `delimiter` is the character that separates the values from one another, such as the | character.
- `metadata value x` are the index values that the application uses to index the document.
- The delimiter character must be the same character throughout the entire input file and match what is specified in the input definition. The default is a pipe character (|).
- Only one metadata value is required per required field in the application. For example, if a Name and Date field are both marked as Required in an application, then the input file must have values for both the Name and Date field as well. Additional values are optional but they must continue to follow the `[delimiter]<metadata value>` format.
- There is no length restriction per line, but all metadata pertaining to the file must be on a single line because the newline character specifies the start of a new document.
- Each value is separated by a delimiter, with the delimited values treated by the Input Agent as Column 1 .. Column N. Any commands on the line do not count as a column. See "Using Input Filing Commands" on page 5-3.
- Columns in the input file need not match the ordering of the Application, but they must be in the same locations as specified in the input definition to be indexed correctly.

---



---

**Note:** Dates and times specified in the input file are subject to current Daylight Savings Time rules, and not the DST rules in effect for the specified date. This can cause the timestamp of the document to shift forward or back up to two hours. If the timestamp shifts forward or back across midnight, the date used for the document input may also shift.

---



---

## 5.3 Using Input Filing Commands

Input Agent gives users more control over the filing process by inserting special command sequences in the input file. An Input Definition applies to all files, but commands can be inserted by Input Agent in the input file as needed and can change from file to file, offering the flexibility of setting a specific behavior per file, such as the file locale for changing date formats or numeric display.

These commands can be used for processing the entire input file or just a single row of the file, depending on the command. The details of the individual commands are specified below.

### 5.3.1 Locale

The locale command changes the locale which the agent uses to parse the data. This command can only be used once at the beginning of the input file before any documents are specified. If the command is used after data has been processed then an error will occur and the filing will stop.

**Syntax**

@Locale[delimiter][locale]

**Example**

@Locale|es-es

**Notes**

This command can only be used at the very beginning of the input file and applies to the whole file. If multiple locales need to be used then that data must be separated into different files. The delimiter must be the same as is used throughout the input file. The locale follows the format of ISO Language - ISO Country code.

### 5.3.2 New

The new command creates a new document in the Oracle I/PM system and behaves the same as leaving the index data on a line by itself. The command only applies to the line that is annotated and will reset on the next line.

**Syntax**

@New[delimiter][line data]

**Example**

@New|TestTiff.TIF|98.765|Good Company LTD|10/08/2003|0000|1.733,12|10/09/2003

**Notes**

The @New at the beginning of the line is not counted as one of the columns to be mapped.

## 5.4 Creating Input Definitions

An input definition is an object that defines the mapping between an input file and the metadata fields of the selected application when a document is uploaded. The input file includes what document files to upload on the file system, what application to use when uploading the files, and other initial document creation options.

You can reuse an existing input definition within Oracle I/PM by exporting the desired definition to an XML file. You can then import that definition file into other systems and modify it appropriately. For more information about exporting and importing, see "[Exporting and Importing Definitions](#)" on page 3-8.

Note that you must have Create or Administrative rights for the type of input you are creating, and View rights for the application to which the documents are uploaded. To create an input definition, do the following:

1. From the navigator pane under **Manage Inputs**, click the **Create Input** icon. The [Input Basic Information Page](#) displays.
2. Enter the name of the input. This name will appear under Manage Inputs in the navigator pane. This is a required field.
3. In the **Description** field, type a short description of the Input being created.
4. Enabling **Online** tells the Input Agent to start polling the definition files of this input once it is completed.

5. The **Auto-detect input file character set** field is enabled by default. If you disable it, a picklist displays from which you can select the file character set to be used. Note that this is the character set used to create the input definition file, not the character set of the documents to be uploaded.

---

---

**Note:** Auto-detect does not work if the provided sample file is not large enough to get an accurate determination of the character set. If the sample file is too small, disable **Auto-detect input file character set** and manually select the character set.

---

---

6. Select an sample file to use. There are two options to locate an input file:
  - **Browse:** Displays a list of input files in the Samples directory that are available to use.
  - **Upload:** Opens a standard file navigation dialog to locate and upload a new input file from a local or shared network drive to the Samples directory. Although any delimited text file is accepted, preferable file types are ASCII or UTF-8 text files.
7. When a sample file has been selected, click **Next**. The [Input Identify and Parse File Parameters Page](#) is displayed and the Input Mask field lists the selected sample file.
8. Ensure the delimiter is the same single character that is used to separate columns within the sample file. By default, a pipe is indicated.
9. Select an application for mapping from the **Applications** field.
10. Click **Next**. The [Input Field Mapping Page](#) is displayed.
11. Define how the input file fields will map to the application. At least one field must be mapped and the file path must be specified. Table columns are defined as follows:
  - **Application Fields:** Name of field within application
  - **Input Column:** Number of corresponding column within input file
  - **Sample Data:** Column data taken from sample file
  - **Use Application Default:** Specifies whether to use the default value specified in an application when the definition file contains empty data for the field.
  - **Date Format:** Specifies how the Input Agent parses the date string. If no date format is specified, the server's locale is used to parse date values. To specify a date format, click the **Add a date format for this mapping** icon. Click the **Edit date format** icon to change an existing date format. Click the **Delete** date format icon to delete the date format specified.
12. Click **Next**. The [Input Security Page](#) is displayed.
13. Click **Add**. The [Add Security Member Page](#) displays. Type a user name or click **Search** to display a list of users from which to select.
14. Select the user you want to add. The user name is added to the Display Name column on the [Input Security Page](#) page.
15. Enable the permissions you want to assign to this user by selecting the field in the appropriate column. Options are:

- **View:** Enabled by default. Grants the user or group the right to view this input.
- **Modify:** Enable to grant the user or group the right to modify all aspects of this input except for granting security rights.
- **Delete:** Enable to grant the user or group the right to delete this input.
- **Grant Access:** Enable to grant a user or group the right to grant security rights to others for this input. If this is the only security level granted, the user can modify only the security information for this input.

A user with Grant Access permission can grant themselves all other rights. At least one user must be given Grant Access rights.

16. Click **Next**. The [Input Review Settings Page](#) is displayed.
17. Review your settings. Click **Back** to return to the appropriate pages to make any necessary changes. When done, return to the [Input Review Settings Page](#) and click **Submit**.

## 5.5 Input Agent Processing

This section describes how the Input Agent processes the input files.

### 5.5.1 Input Directory Structure

The input directory specified in the configuration MBean is the top level of the directory structure. Below the top level input directory, the Input Agent creates and manages other directories in the following structure to process its work. Directory definitions follow the following file structure.

*Input*

- *Errors*
- *Failed*
  - *YYYY-MM-DD*
- *Processed*
  - *YYYY-MM-DD*
- *Samples*
- *Stage*

Directory	Definitions
<i>Input</i>	This is the top level that is defined in the configuration MBean. This is where Input Agent looks for new input files. There can be multiple input directories defined in the MBean and each entry in the MBean will have this same structure below it.
<i>Errors</i>	Whenever an input file has a mixture of failed index attempts along with some successful indexes, an error file is created for that filing in this directory.
<i>Failed</i>	This directory separates out failed input files by placing them in a directory matching the date it was processed. Each input file located under these directories failed completely. Those input files with partial failures are located in Processed directory.
<i>YYYY-MM-DD</i>	These directories are date values in the form of year-month-day (such as 2009-04-01) that organize the input files by the date they were processed. This gives the date of when the file was processed and prevents any one directory from getting too many files in it.

<b>Directory</b>	<b>Definitions</b>
<i>Processed</i>	Files under this directory have gone through the filing process and had at least one document successfully created in the Oracle I/PM system.
<i>Samples</i>	This directory contains all the sample files that work with input objects via the user interface. Files in this directory are visible in the input wizard under the user interface and should not contain production data. Note that the Samples directory location is configured separately from the input directories and may not be under the input directory.
<i>Stage</i>	Files in this directory have been selected for processing and are being worked on by the agent. Once the filing is complete, the file is moved to the appropriate Failed or Processed directory.

## 5.5.2 Input Agent Processing Order

Input Agent polls for input files, stages them, and posts a message to the JMS queue that there are files available for processing. Input ingestors listen to the JMS queue and start processing staged files. The sequence of events is as follows:

### 5.5.2.1 Polling

First, Input Agent polls for files:

1. Upon Input Agent wake up (specified by the CheckInterval MBean), Input Agent gets a list of the currently online input definitions.
2. For each of the input definitions, Input Agent checks all input directories for files that match the input file mask.
3. When a file is found, it is moved to the Stage directory and a message is generated on a JMS queue to process the file, at which point input ingestors are notified and processing can begin.
4. Steps 2 and 3 are repeated until all input definitions and directories have been checked.

### 5.5.2.2 Processing

Once input ingestors are notified that there are files staged for processing in the JMS queue, they begin processing the files:

1. The ingestor opens a connection to the repository and creates an error file and a new batch object for tracking the documents.
2. The thread begins parsing the input file and indexing the documents into Oracle I/PM. Any errors that are encountered during indexing are recorded in the error file. This step is repeated for all entries in the input file.
3. After all the documents have been processed, the batch is closed and, if there were no error entries, the error file is deleted.
4. The ingestor closes the connection to the repository and the input file is moved to the current date directory under the Processed or Failed directory, and the ingestor moves on to the next staged input file.

## 5.5.3 Changing WLS Work Manager Settings

A work manager is a WebLogic Server (WLS) concept for controlling how many threads are assigned to a process. In Oracle I/PM, they are used to control how many

threads are assigned to the Input Agents and for increasing or decreasing their load on the system. On a new installation, Input Agent is assigned 10 threads. You can reconfigure how many threads WebLogic Server should provide to the Input Agents by changing the default settings of the WLS work manager `InputAgentMaxThreadConstraint` (default 10) to match your system needs.

To update thread settings, complete the following steps from the WLS administration console. For more information about the WebLogic server, see *Oracle® Fusion Middleware Configuring Server Environments for Oracle WebLogic Server*.

1. Bring up the WebLogic console for the domain and go to the deployments section.
2. Select the Imaging application to display the details for Oracle I/PM.
3. Select the Configuration and then Workload tabs to get to the Work Manager list.
4. Select InputAgent to adjust.
5. Select the Max Threads Constraint at the bottom of the page.
6. Update the count to the new maximum thread count and click Save.
7. Restart the managed server(s) and the new thread count will be in effect.

## 5.6 Checking Results and Error Files

Input Agent has a retry mechanism to allow it to reattempt processing the input file in the event of a recoverable error. An example of this type of error is when the repository is not yet available and needs to finish initializing. When Input Agent detects a recoverable error, it puts the filing back on the JMS queue. The queue has a configurable retry wait timer that prevents the input file from being reprocessed immediately. You can also set the `InputAgentRetryCount` MBean to control how many times a job can be retried. The default is 3, after which the job is placed in the failed directory.

To troubleshoot any input file errors, do the following:

1. Determine if the input file was a complete or partial failure by locating whether the file is in the Failed or Processed directory.

The directory structure can be used by finding the input file under the appropriate date directory in the Processed or Failed directory. If the file is under the Failed directory, none of the indexes have been saved to Oracle I/PM and the error file should be examined for an exception from `InputFilingMDB` to determine why it was rejected. If the file is under the Processed directory, then at least one file was successfully indexed into Oracle I/PM.

2. Check the Errors directory for the input file's error report. For every input file that had indexing issues, a matching file with the format of *<original file name>.<MM-DD-YYYY>.<HH-mm-SS>.txt* is created in the Errors directory. For example, the input file `invoices.dat` could have an error entry of `invoices.dat.05-21-2009.16_36_07.txt`. If no error report exists for the input file, a higher level issue such as a repository error could be the problem.

If an error report does exist and the file shows a list of all lines for the original input file with an additional column at the end of the file displaying the error message. So, an original line of:

```
C:\IBPM Data\WorkFiles\Filer\input\Images\C885\Identifier
165|27/06/2008|28215|495.75|
```

would be listed in the error file as the following:



```
C:\IBPM Data\WorkFiles\Filer\input\Images\C885\Identifier  
165|27/06/2008|28215|495.75|Could not find file C:\IBPM  
Data\WorkFiles\Filer\input\Images\C885
```

The error file also gives the results of a filing if information or a better logging level is enabled for Oracle I/PM. If the filing was placed in the processed directory, a log entry is created stating:

```
Filing <Input Name> completed successfully with <indexed doc count> documents  
processed successfully out of <total doc count> documents.
```

If the filing failed, then a log entry is created that states:

```
An error occurred while completing a batch.
```

Common causes of errors on a line by line basis are problems with proper formatting of metadata to be loaded, or invalid value ranges and truncation of data.

3. Refer to the server's Oracle Diagnostic Logging (ODL) framework logs. The most common way to check this is via the Enterprise Managers's Log viewer for the imaging application. Typical problems here are from underlying repository or file permissions issues.



---

---

## Managing Searches

This section discusses the following topics:

- ["Search Overview"](#) on page 6-1
- ["Creating a Search"](#) on page 6-1
- ["Modifying an Existing Search"](#) on page 6-3

### 6.1 Search Overview

At the core of Oracle I/PM is the capability to define and execute searches that retrieve the relevant documents for the user. Search management allows the creation and modification of searches that other users may use to find specific documents. The ability to manage searches is controlled by the security rights that a user has to applications. This means that to ensure security, a person managing searches can be limited to creating searches by the security assigned to the applications defined in Oracle I/PM.

A search manager may only create or modify a search of applications to which the manager has view rights. If the manager does not have view rights to an application, the manager cannot create a search of that application. For a detailed description of security rights, see ["Managing Security"](#) on page 2-1.

At a high level, creating a search involves the following:

1. Selecting the applications to search.
2. Configuring the fields that are displayed in the results.
3. Selecting the conditions that comprise the where clause of the search.
4. Customizing the parameters and the operators used in the search.
5. Assigning security rights so that groups and individuals may use or modify the search.

### 6.2 Creating a Search

Create a search using the **Manage Searches** panel in the navigator pane of the Oracle I/PM user interface.

You can reuse an existing search definition within Oracle I/PM by exporting the desired definition to XML. You can then import that definition file into other systems and modify it appropriately. For more information about exporting and importing, see ["Exporting and Importing Definitions"](#) on page 3-8.

---

---

**Note:** The Oracle I/PM user interface changes based on your security rights. You must have either Definition Management security rights of Create or Administrator, or have Search Definition security rights of Modify, Delete, or Grant Access for the Manage Searches panel to display in the navigator pane.

---

---

To create a search, complete these steps:

1. Open the **Manage Searches** panel and click the **Create New Search** icon. If you have View security rights to at least one application, the [Search Properties Page](#) displays.

---

---

**Note:** If you do not have View security rights to at least one application, and error message is displayed.

---

---

2. In the **Search Name** field, type a descriptive name for the search. This search name is displayed under the Searches panel in the navigator pane. This field is required, and it must be unique within I/PM.
3. In the **Description** field, type a description of the new search that will be helpful to the user. The description is displayed when the cursor hovers over the search name in the navigator pane. The field contains a maximum of 2000 characters.
4. Enter instructions for the search. The instructions provide helpful information about what criteria is being searched for and how a user should use the search. These instructions are available on the search form and also appear on the Search Tab display. The field contains a maximum of 2000 characters.
5. In the **Maximum Search Results** field, enter the maximum number of search results returned. This limits how many results retrieved from the repository are displayed, per the number of applications being searched. For example, if the search spans 2 applications and the Maximum Search Results is set to 10, the results table would have 20 rows. A setting of 0 defaults to the maximum number of rows set in the I/PM MBean configuration variable.
6. Click **Next**. The [Search Results Formatting Page](#) is displayed.
7. Select the application in which to search from the **Source Application** field.
8. Click **Next**. The [Search Conditions Page](#) is displayed.
9. Select the fields you want to use to find the documents in the selected applications and click **Next**. The [Search Parameters Page](#) is displayed.
10. Select how you want the user to be prompted to enter parameters into the search:
  - a. Enter a name for each field to be used to enter parameters.
  - b. Enter the prompt text for each field. The prompt text precedes the operator on the search form to more clearly define the required entry for the parameter. This can help clarify the field name and is especially useful if the parameter spans multiple fields.
  - c. Click the icon in the **Operator Text** column. The Operator Properties dialog box is displayed. Use the Operator Properties dialog box to enable users to choose from a set of operator options, then click **OK**.
  - d. Click the icon in the **Default Value** column. The Modify Default Value dialog box is displayed.

- e. Select the value data type and default value and click **OK**.
  - f. Enable which parameters, if any, that you want to be required or Read Only, and click **Next**. The [Search Security Page](#) is displayed.
11. Click **Add** to search and select users and groups who will be able to use this search. The [Add Security Member Page](#) page is displayed.
    - a. On the [Add Security Member Page](#), select whether you want to search for groups or users and click **Search**. A listing of results is displayed.
    - b. Select the users or groups you want to add and click **Add**. You can select more than one from the results listing by holding the **Ctrl** key on your keyboard while clicking on the search results. The [Add Security Member Page](#) closes.
  12. Select the permission each user and group will have: **Modify**, **Delete**, or **Grant Access** and click **Next**. For a description of the permission options, see "[Search Security Page](#)" on page A-20. The [Search Preview and Test Page](#) is displayed.
  13. On the [Search Preview and Test Page](#), review how the search form will display for the user. Test it and if necessary, go back and make modifications where necessary. When satisfied with the display and operation, click **Next**. The [Search Summary Page](#) is displayed.
  14. Review the details of the new search and go back in the navigation train to make changes, if necessary. When satisfied with the search, return to the [Search Summary Page](#) and click **Submit**.

## 6.3 Modifying an Existing Search

To modify an existing search, complete these steps:

---



---

**Note:** Unlike documents, definitions cannot be locked while being modified. Consequently, if the same definition is being modified at the same time by different people, only the last changes submitted are saved.

---



---

1. Expand the **Manage Searches** panel in the navigator pane.
2. Click the name of the search you want to change. The [Search Summary Page](#) is displayed.
3. Click **Modify**. The [Search Properties Page](#) for that search is displayed.

---



---

**Note:** If you only have the Grant Access security rights, the [Search Security Page](#) is displayed. The [Search Security Page](#) and the [Search Summary Page](#) are the only two you will have access to.

---



---

4. Navigate to the appropriate page or pages to make the desired modifications using the navigation train. Review the section "[Creating a Search](#)" on page 6-1 for information regarding page options. Once you have made the desired modifications, return to the [Search Summary Page](#).
5. On the [Search Summary Page](#), click **Submit** to enter the changes.



---

---

## Managing Connections

To successfully have all aspects of your business flow communicate with Oracle I/PM, you must define the appropriate connection types. Using the Oracle I/PM user interface, you can create a connection to both an Oracle Content Server repository or a Business Process Execution Language (BPEL) server.

---

---

**Note:** You must ensure that the I/PM support component **IpmRepository** is installed and enabled on the Content Server you are connecting to. For information on enabling Content Server components, see the Oracle Universal Content Management guide *Working With Content Server Components*.

---

---

This section describes the connection configuration options available to an Oracle I/PM administrator and how they are accessed. It contains the following topics:

- ["Creating a Content Server Connection"](#) on page 7-1
- ["Creating a BPEL Connection"](#) on page 7-2

### 7.1 Creating a Content Server Connection

To connect Oracle I/PM to a Content Server document repository, do the following:

1. From the navigator pane, under Manage Connections, click the **Add** icon and select the **Create Content Server Connection**. The [Content Server Connection Basic Information Page](#) is displayed.
2. Enter a name for the connection. The name will display in the Manage Connections panel. This field is required.
3. Enter a brief description of the connection and click **Next**. The [Content Server Connection Content Server Settings Page](#) is displayed.
4. Enter the name of the repository proxy. The repository proxy is a user created in Content Server when Oracle I/PM is installed. The proxy is given rights to Content Server that allows it to fulfill requests to Content Server on behalf of I/PM users who may not have the necessary rights in Content Server to perform the required tasks. For example, a user may have the rights in I/PM to create an application and add metadata fields, but may not have the rights in Content Server to create metadata fields to support the application. When the application is created, the request to Content Server to create the necessary metadata fields is made by the repository proxy. By default, the repository proxy name is `fmwadmin`. This field is required.

5. Optionally, enable SSL to connect to the repository over SSL. Additional steps are required and must be completed prior to enabling this field. See "[Configuring SSL Connection to Content Server Repository](#)" on page 7-2.
6. Specify the hostname or IP address, domain, and port number of the Content Server. For example, enter *contentserver.company.com* in the **Machine** field, and *4444* in the **Server Port** field. These fields are required and must be unique for each connection. You can optionally specify a secondary Content Server as well.
7. Click **Next**. The [Content Server Connection Security Page](#) is displayed.
8. Add any additional users required. To add a user, do the following:
  - a. Click **Add**. The [Add Security Member Page](#) is displayed.
  - b. Select either **Search Groups** or **Search Users**, then click **Search**. A listing of available groups or users is displayed.
  - c. Select the users or groups to be added. You can make multiple selections by holding down the Control or Shift key on your keyboard when making a selection.
  - d. When you have selected all the users or groups you wish to add to the connection, click **Add**. The [Add Security Member Page](#) is closed and the new users or groups are listed on the Connection Security page.
9. Enable the security permissions desired for each user or group and click **Next**. The [Content Server Connection Review Settings Page](#) is displayed.
10. Ensure that settings are correct. If they are not, click **Back** to return to the page you need to modify, or click the link in the navigation train to return directly to the desired page. When satisfied with the settings, return to the Review settings page and click **Submit**.

### 7.1.1 Configuring SSL Connection to Content Server Repository

Before enabling SSL on the [Content Server Connection Content Server Settings Page](#), you must first configure Content Server to accept SSL connections. For information on configuring Content Server to accept SSL connections, see the *Remote Intradoc Client (RIDC) Developer Guide*.

## 7.2 Creating a BPEL Connection

To create a BPEL process, you must first create a connection to a BPEL server. To do this, do the following:

1. From the navigator pane, under Manage Connections, click the **Add** icon and select the **Create BPEL Connection**. The [BPEL Connection Basic Information Page](#) is displayed.
2. Enter a name for the connection. The name will display in the Manage Connections panel. This field is required.
3. Optionally enter a brief description of the connection and click **Next**. The [BPEL Connection Settings Page](#) is displayed.
4. Specify the hostname or IP address, domain, and port number of the BPEL Server. For example, enter *bpelserver.company.com* in the **Machine** field, and *8001* in the **Server Port** field. This field is required.

If the BPEL server is a single instance, it is the hostname or IP of the BPEL machine. If the BPEL server is operating within a cluster, this parameter value can



be a comma-separated list of machine names or IP addresses of servers in the cluster, or it can be the cluster name for the cluster.

If multiple machine names are provided in a comma-separated list, the machines must *all* use the same port (the value supplied by the `port` parameter). If the BPEL managed servers in the cluster need to be defined with different ports, then the cluster-name configuration must be used.

When a cluster name is used, the name must be defined in DNS to resolve to the multiple machines within the cluster. Neither Oracle I/PM nor BPEL defines this behavior. Rather, it is defined by the Oracle WebLogic Server support for JNDI in a cluster.

5. Enable **SSL** if desired. This field is optional. If the SSL option is checked, then the port provided must be the SSL listening port for the server, and T3 communication will actually use T3S, the SSL version of T3. For setting the listening port on the BPEL server, see "[Configuring SSL for the BPEL Server](#)" on page 7-3.
6. Enter the Credential Alias. For example, *basic.credential*. This field is required. The credential alias is an alias, or key, used to look up the user name and password in the Credential Store Framework (CSF), which encrypted them to provide for proper security.  
  
This credential must be created in the CSF before the BPEL connection configuration can be completed. A credential can be created in the CSF in one of two ways: through Fusion Middleware Control or through WLST.
7. Click **Test Connection** to ensure the connection is made. When successful, a list of BPEL composites is displayed.
8. Click **Next**. The [BPEL Connection Security Page](#) is displayed.
9. Add any additional users required. To add a user, do the following:
  - a. Click **Add**. The [Add Security Member Page](#) is displayed.
  - b. Select either **Search Groups** or **Search Users**, then click **Search**. A listing of available groups or users is displayed.
  - c. Select the users or groups to be added. You can make multiple selections by holding down the **Control** or **Shift** key on your keyboard when making a selection.
  - d. When you have selected all the users or groups you wish to add to the connection, click **Add**. The [Add Security Member Page](#) is closed and the new users or groups are listed on the [BPEL Connection Security Page](#).
10. Enable the security permissions desired for each user or group and click **Next**. The [BPEL Connection Review Settings Page](#) is displayed.
11. Ensure that settings are correct. If they are not, click **Back** to return to the page you need to modify, or click the link in the navigation train to return directly to the desired page. When satisfied with the settings, return to the [BPEL Connection Security Page](#) and click **Submit**.

## 7.2.1 Configuring SSL for the BPEL Server

For the Oracle I/PM SSL configuration to work with BPEL, the SSL listening port must be enabled on the BPEL server. This can be done at the time the BPEL server is first installed, through the configuration wizard, or after installation, through the Oracle WebLogic Server Administration Console.

**To configure SSL for the BPEL server:**

1. Log in to the Administration Console for the BPEL managed server domain.
2. From Domain Structure, click **Environment** and then **Servers**.
3. Select the BPEL managed server instance.
4. Check **SSL Listen Port Enabled**.
5. Enter an available port number for **SSL Listen Port**.
6. Click **SAVE**. SSL is enabled on the BPEL managed server.

In the Oracle I/PM connection, the SSL check can be checked and the SSL listen port used for the port parameter. At this point, communication to the server will work properly if both the BPEL managed server and the Oracle I/PM managed server are configured to use the default `DemoTrust` certificates. All Oracle WebLogic Server instances use the same `DemoTrust` self-signed certificates and, therefore, are configured to trust the others by default. Note that this should only be used to test the system in a demonstration or test environment. For security, `DemoTrust` certificates should never be used in production.

---

---

**Note:** These files should be used for test and demonstration purposes only. In a production environment, you should obtain proper and valid certificates and follow appropriate procedures for importing and configuring those certificates to establish identity and trust. When properly signed certificates are used and configured properly, SSL will work properly without special configuration.

---

---

You can also configure SSL for the BPEL server in the Oracle I/PM user interface, using the **Managed Connections** section to create the BPEL connection.

## 7.2.2 Configuring a BPEL Connection CSF Credential

A credential store framework (CSF) credential is a username/password pair that is keyed by an alias and stored inside a named map in the CSF. Because of its integration with Oracle Web Services Manager (OWSM), Oracle I/PM leverages the standard OWSM CSF map named `oracle.wsm.security`.

A credential can be created through Enterprise Manager (EM) or through WebLogic Scripting Tool (WLST).

### Creating a Credential Using EM

To create a credential using EM, do the following:

1. Log in to Enterprise Manager.
2. Click **WebLogic Domain**.
3. Click **Security** and then **Credentials**.
4. Select the `oracle.wsm.security` map. If it does not exist, do the following:
  - a. Select **Create Map**.
  - b. Enter `oracle.wsm.security` in the map field and click **OK**.
  - c. Click **Create Key**. The key is now available for selection.
5. Enter a key name. This is the credential alias used in the BPEL connection configuration.

6. Select **password** as the type.
7. Enter a user name and password.
8. Optionally, enter a description for the credential.
9. Click **OK**.

### **Creating a Credential Using WLST**

To create a credential using WLST, execute the following command:

```
createdCred(map="oracle.wsm.security", key="basic.credential", user="weblogic",  
password="Welcome1")
```

where key is the alias which is used for the credential alias property of a BPEL connection definition in the user interface. In the API, it is used for the `Connection.CONNECTION_BPEL_CSFKEY_KEY` property. The alias, `basic.credential`, is used in the example because it is a standard default name used by OWSM and BPEL. However, the alias can be anything as long as it is unique within the map.



---

---

## Working with BPEL

This section contains the following topics:

- ["Business Process Management"](#) on page 8-1
- ["Business Process Execution Language \(BPEL\)"](#) on page 8-1

### 8.1 Business Process Management

Business Process Management (BPM) technology is a framework for applications that can effectively track and orchestrate business processes. BPM solutions can automatically manage processes and process flow, yet also allow for manual intervention when necessary.

For example, BPM might coordinate the extraction of customer information from a database or manage a new customer information transaction. BPM could generate transactions in multiple related systems or support complete though processing automatically, without human intervention. BPM allows you to automate tasks involving information from multiple systems with rules to define the sequence in which the tasks are performed, as well as responsibilities, conditions and other aspects of the process. BPM not only allows a business process to be executed more efficiently, it also provides the tools to allow you to measure performance and identify opportunities for improvement. A benefit of BPM is that changes can be easily made in processes or flow by adding, removing or updating a process.

To best take advantage of BPM, the software application components of an Oracle process follow a Service-Oriented Architecture (SOA). These components are published as web services for reuse and ease of integration using BPEL.

### 8.2 Business Process Execution Language (BPEL)

Business Process Execution Language (BPEL) is an executable language for specifying interactions with web services. It extends and enables the web services interaction model to support business transactions and human interaction. BPEL is emerging as the clear standard for composing multiple synchronous and asynchronous services into collaborative and transactional process flows. BPEL is to business process management what SQL is to data management.

You can use BPEL to define services that can be used by other applications. You define all aspects of a process, from the definitions of data required to start a process to the available forms for human interaction with a process. These components are bundled into a composite and deployed to an SOA server.

To integrate a BPEL process with I/PM, you must complete the following steps:

1. Ensure that the AgentUser configuration MBean is defined (see ["Configuring the AgentUser and GDFontPath MBeans"](#) on page 3-15).
2. Create a BPEL connection (see ["Creating a BPEL Connection"](#) on page 7-2).
3. Create an application with a BPEL process defined within it (see ["Creating An Application"](#) on page 4-2).
4. Configure BPEL properties, which is part of the process to create an application in the Oracle I/PM user interface (see ["Configuring BPEL Properties"](#) on page 8-2).

## 8.2.1 Configuring BPEL Properties

The BPEL process can be added to an application when the application is created, or by modifying an existing application. Adding a BPEL process begins with the [Application BPEL Configuration Page](#). When you configure an application to use BPEL, you must ensure that a connection to a BPEL server has been created and select the BPEL connection on the [BPEL Server Properties Page](#). The BPEL Server connection must include a name, protocol, server, and port (for example, name=t3://sta00319:7001). Oracle I/PM must authenticate with the server to discover the deployed BPEL components.

Once connected to the server, a list of BPEL components is identified. A BPEL component can provide many different services, so you must identify the service you want to use on the [BPEL Component Properties Page](#). Services can be invoked in multiple ways, so you must also identify the operation used to start a process.

This operation is assumed to be asynchronous; it is a one-way communication into BPEL. Oracle I/PM uses it to initiate a process instance and does not wait for a response. A business process may take hours or days to complete. Once the operation is selected, Oracle I/PM knows which data has to be provided to start the process. This is called the payload.

BPEL uses web services so the payload reflects the data contained in the Web Services Description Language (WSDL) that defines the service. This data is represented as a schema with defined data types. On the [BPEL Payload Properties Page](#), the payload type and a list of allowed values are displayed which are called mapping functions. [BPEL Payload Mapping Functions](#) return a value of a given type: text, number, date, and so on. If the payload value can accept a date, mapping functions that return a date are shown. If a text function cannot properly evaluate to a date, it is excluded from the list of available functions. If the payload value can accept a string, then all mapping functions are allowed since they can all be represented as text.

### 8.2.1.1 BPEL Payload Mapping Functions

The BPEL Payload Properties is used to map IPM application metadata fields to elements within a BPEL process service payload. Predefined mapping functions are associated with simple typed elements in the payload. At runtime, when a document is created and the BPEL agent is triggered to create a BPEL process instance for the document, the mapping function for each element is evaluated to transform metadata from the document into payload element values. The mapping functions that are available may provide the raw metadata of the document, including system properties and application defined field values. A special mapping function named Format Value is also provided, allowing mapping of any value. The format is custom concatenation of constant values as well as values from other mapping functions.

Mapping functions are typically specific to type and must match the schema type of the payload element. This means that numeric, decimal, and date types in the payload may only map be mapped with mapping functions that return these types. String

types in the payload can typically be mapped with any mapping function. Also, the Format Value mapping function can be mapped to any payload element. However, The Format Values return type is technically a string, and care must be taken to ensure that the return value is a valid string representation of the payload schema type.

The following table lists the available specific payload schema types and their compatible mapping functions:

Schema Types	Mapping Function
string, normalizedString, token	All Functions All Field Values
anyType	All Functions All Field Values
anyUri	DocUrl DocUrlRoot Format Value
byte	AppId
unsignedByte	BatchId
integer	DocSize
positiveInteger	Version
negativeInteger	Format Value
long	Number Field Values
unsignedLong	
short	
unsignedShort	
<b>Note:</b> I/PM uses integer bounded types to store numbers. Mapping to schema elements with lower bounds is allowed but may result in errors or loss of data during mapping execution	
time	Create Date
date	Modify Date
dateTime	Volume Date Format Value DateField Values
Boolean	True False Boolean Field Values
All other schema types	Format Value

Format Values for types other than string-based types must return valid string representation of the schema type. Also, there are many other valid payload schema XSD types that may be present in a payload. Format Value is the only mapping function supporting types other than those specifically listed in the table above. As with other Format Value usages, it is up to the application and BPEL process implementer to ensure that the format string returns a compatible type. Because the actual value returned is only known at runtime, I/PM cannot do any validation on such a configuration. It is recommended that payloads use the known types listed in the above table whenever possible.

### 8.2.1.2 Required Payload Element (MinOccurs) Handling

BPEL payload elements annotated with minOccurs are defined as being **required** when mapping I/PM application fields. These elements are designated with a (\*) symbol on the [BPEL Payload Properties Page](#) of the I/PM user interface.

Payload elements with a minOccurs=1 are interpreted as being required and I/PM requires a mapping for them. In this case, required means that the element must be supplied in the payload, but does not need a value. It is possible for a field value mapped to a payload element to be null even when mapped to a minOccurs=1 payload element. In this case, an empty element will be passed. In cases where the BPEL process wants **required** to mean that a value must be supplied, the application field value mapped to the element can be marked as required in the application definition to ensure that it has a value. The BPEL payload mapping does not enforce this.

Payload elements with a minOccurs=0 are interpreted as being optional and need not be supplied in the payload if there is no mapping for the element. This means that providing a mapping is optional as well. If no mapping is provided, the node will not be included in the payload sent to the BPEL server. If a mapping is provided, however, the node will always be included, even if the value returned by the mapping function is empty. In this case, an empty element node is passed.

---



---

**Note:** In the BPEL payload, Oracle I/PM does not support types where the minOccurs or maxOccurs attributes are greater than one.

---



---

### 8.2.1.3 Date Field Format

For mapping functions that map to a payload schema date or time based type (time, date, dateTime), values are encoded to ISO 8601 compliant formats as follows:

Schema Type	Format	Example
time	hh:mm:ss±tz	12:45:15-05:00
date	yyyy-MM-dd	2009-11-09
datetime	yyyy-MM-ddThh:mm:ss±tz	2009-11-09T12:45:15-05:00

As indicated, types that include a time use the positive/negative time zone designator as an offset in hours and minutes (hh:mm).

### 8.2.1.4 Doc Property Functions

Document property functions assign the value of a system property of the document to a payload element. Document Id, Application Name, Create Date, etc.

### 8.2.1.5 Field Value Functions

The Field Value function assigns application field values from a document to a payload element. Although "Field Value" is technically the name of the function, with the name of the field as a parameter, the BPEL Payload Properties page presents each of an application's field definitions as a item in the mapping function selection box listed by the field's name. As with all mapping functions, the field definition type is used to determine whether or not it is compatible with the payload element schema type. Only compatible field values are listed as options next to any particular payload element.



### 8.2.1.6 Format Value Function

Format value is a special mapping function that allows assigning any string value to a payload element. The format value can also embed multiple other mapping function values in the format string value as variables that will be supplied at runtime.

A format value is assigned to a payload item on the BPEL Payload Properties page by selecting Format Value as the mapping function and then clicking the Edit Format Value button that appears next to selection box. On the "Edit Format Value" dialog that appears, the format value is entered at the bottom. A selection list at the top provides available mapping function scan be inserted into the edit box. (Items append to the end of any currently entered text.)

When creating a format value string manually, mapping function variables are encoded in the value using the mapping function name surrounded by square brackets (e.g., "[DocUrl]"). Field Values are coded by include the mapping function (Field Value), a colon, and then the desired field name, all within square brackets.

For an example, suppose that the BPEL process includes a data variable that is expected to contain custom URL. The custom URL must include a customerId, which is available in the metadata of the document, and the document's unique identifier. The root of the URL is hard coded. This example might be coded in a format value as follows:

```
http://example.com/svc.jsp?custId=[Field Value:custId]&docId=[DocId]
```

## 8.2.2 Payload Limitations

In general, the BPEL payload mapping can handle payloads containing nesting of complex types. However, there are a number of standard XSD constructs that it cannot handle. BPEL process service payload definitions containing any of the following cannot be used:

- Hierarchical depth greater than 10
- Choice element types
- List elements with minOccurs greater than 1

Payload definitions containing list like structures with (maxOccurs is greater than 1 or unbounded) with a minOccurs equal 0 or 1 can be used, but only support mapping to a single element in the array.

## 8.2.3 Mapping Secure BPEL Services

When the BPEL Process service has server-side Oracle Web Services Manager (OWSM) policies applied to it, additional parameters need to be supplied in the imaging application's BPEL configuration such that the client-side policy is also used. These additional configuration parameters are provided on the [BPEL Payload Properties Page](#) with the normal BPEL process instance payload mappings. If the service has a OWSM policy applied, Oracle I/PM detects this policy and provides an additional payload mapping section labeled as "". The full set of keys that are possible for all OWSM policies is provided by the OWSM API in the class *oracle.wsm.security.util.SecurityConstants*. Oracle I/PM however filters out the full set and lists only those parameters relevant to the server policy in use. Currently, only parameters are provided for *wss\_username\_token* and *wss11\_username\_token\_with\_message\_protection* policies.

The following parameters are possible:

Parameter	Description	Policies
csf.key	Provides the username and password for the policy.	wss_username_token wss11_username_token_with_message_protection policies
recipient.key.alias	Provides the key store alias for encrypting the sent message.	wss11_username_token_with_message_protection policies

For more information on setting up keystores, CSF keys and aliases for Oracle Web Services Manager, see *Oracle Web Services Manager Administrator's Guide*.

## 8.2.4 Changing WebLogic Server Work Manager Settings

A work manager is a WebLogic server concept for controlling how many threads are assigned to a process. In Oracle I/PM, they are used to control how many threads are assigned to the input and BPEL agents and for increasing or decreasing their load on the system. On a new installation, the BPEL agent is assigned 20 threads. You can reconfigure how many threads WebLogic server (WLS) should provide to the input and BPEL agents by changing the default settings of the WLS work managers BpelMaxThreadConstraint (default 20) to match your system needs.

To update thread settings, complete the following steps from the WLS administration console. For more information about the WebLogic server, see *Weblogic Web Services Reference for Oracle Weblogic Server*.

1. Open the WebLogic Server console and click Deployments.
2. Select the **Imaging** deployment to display the details for Oracle I/PM.
3. Click the **Configuration** tab and then the **Workload** tab to display the Work Manager list.
4. Select the agent you want to adjust, either **BpelAgent**.
5. Select the **Max Threads Constraint**.
6. Update the count to the new maximum thread count and click **Save**.
7. Restart the managed server or servers and the new thread count will be in effect.

## 8.2.5 Using a BPEL Connection CSF Credential

A credential store framework (CSF) credential is a username/password pair that is keyed by an alias and stored inside a named map in the CSF. Because of its integration with Oracle Web Services Manager (OWSM), Oracle I/PM leverages the standard OWSM CSF map named *oracle.wsm.security*.

A credential can be created through Enterprise Manger (EM) or through WebLogic Scripting Tool (WLST). For details, see "[Configuring a BPEL Connection CSF Credential](#)" on page 7-4.

## 8.2.6 BPEL Agent Retry Sequence

If the BPEL agent cannot connect to the BPEL server, there will be three immediate attempts at connection. If all three attempts fail, the message is returned to the JMS queue for deployed process. The BPELInjectorQueue JMS queue is configured for a five minute retry delay. Each subsequent retry attempt to process the message is again manually retried three times. Like the manual retry mechanism, the message is

returned to the queue two times (for three process attempts). After the third message processing attempt fails, the document details are written to a BPEL agent faults table, including the exception message from the last exception received, and the message is not returned to the queue. This provides nine retries over a time period of 10 minutes. Note: If for any reason the attempt to record the document details to the fault table fails, the message is returned to the queue to avoid dropping the request.

## 8.2.7 Configuring the BPEL Faults Table

BPEL agent processing faults that are recorded to the faults table are managed using a set of WebLogic Scripting Tool (WLST) diagnostic commands. To access these commands, you must execute WLST from the Enterprise Content Management \$ORACLE\_HOME/common/bin directory. Also, when connecting to WLST, you must connect to an Oracle I/PM managed server instance, not the admin server. These commands are only available when the Oracle I/PM managed server is online.

The following BPEL diagnostic commands are available using WLST:

- **sumIPMBpelFaults:** Counts processing failures during BPEL agent processing, grouped by choice of date, application ID, or batch ID.
- **clearIPMBpelFaults:** Clears processing failures that occurred during BPEL agent processing.
- **listIPMBpelFaults:** Provides details of processing failures that occurred during BPEL agent processing.
- **repairIPMBpelFaults:** Repairs processing failures that occurred during BPEL agent processing.

Details about use and syntax of these faults can be found in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 8.2.8 Initiating a BPEL Process Instance

Once a user has configured all of the BPEL properties, they are ready to be used to initiate BPEL processes. When a document is uploaded to Oracle I/PM, a message is sent to the BPEL agent indicating new content. The BPEL agent monitors these messages, and when it receives a message that the document's application has been configured to use BPEL, it uses the configuration to build a payload of values for that specific document and then calls the service to initiate a BPEL process.

The BPEL process must be designed in such a way that if a user needs to look at a document from Oracle I/PM, it has the necessary information needed to launch the viewer. This can be accomplished by defining a payload value to hold the viewer URL. It is up to the BPEL designer to create a form that includes a button or link to open the target of the viewer URL property. If the business process must update information in Oracle I/PM, it can do so by using the Oracle I/PM API. For more information about APIs, see *Oracle® Fusion Middleware Developer's Guide for Imaging and Process Management*. The Oracle I/PM API is exposed as a web service which can easily be added to any BPEL process by a process designer. Again, the designer needs to ensure that he or she has collected enough information at the start of the process to communicate updated data for the document. For example, the document ID and application field names would be necessary.



---



---

## Document Storage

Oracle I/PM uses the functionality of an Oracle database to store and retrieve uploaded documents. Documents are stored based on criteria specified in the application in which they reside.

This section contains the following:

- ["Document Storage Overview"](#) on page 9-1

### 9.1 Document Storage Overview

Conceptually, applications represent containers of documents with common characteristics as defined and enforced by the application. A single instance of Oracle Content Server may not be able to handle the multiple applications required by an organization. In order to scale a solution to handle the multiple applications required, multiple Content Server instances can be used. However, an application cannot be divided across multiple Content Server instances. To support multiple Oracle Content Server instances, you must associate each application with its target Content Server instance. To represent this at the Oracle I/PM level, a new object has been added to the public API known as the repository. The repository object is responsible for keeping track of the connection information to each Content Server instance. Each application will be associated with a particular repository. For more information about creating connections to repositories, see ["Managing Connections"](#) on page 7-1.

#### 9.1.1 Oracle Content Server Document Properties

The following table identifies how Oracle I/PM document properties map to Content Server document properties.

Oracle I/PM Document Property	Content Server Property	Comment
Id	dDocName	
Name	dOriginalName	Could also come from dDocTitle but dDocTitle can be changed in Content Server user interface
Properties.ApplicationId	xIPMSYS_APP_ID	Custom metadata field
Properties.ApplicationName	none	Read from Application definition not from Content Server

<b>Oracle I/PM Document Property</b>	<b>Content Server Property</b>	<b>Comment</b>
Properties.BatchId	xIPMSYS_BATCH_ID	Custom metadata field
Properties.CharacterSetName	xIPMSYS_CHARACTERSET	Custom metadata field
Properties.CreateDate	xIPMSYS_CREATE_DATE	dCreateDate is when a revision is checked in. If additional revisions are checked in, the value of dCreateDate tracks the revision. So this should be implemented as a custom metadata field.
Properties.Creator	xIPMSYS_CREATOR	Custom metadata field. dDocAuthor is the user who checks in a revision. If additional revisions are checked in, the value of dDocAuthor tracks the revision. So this should be implemented as a custom metadata field.
Properties.DocUrl	none	Will be computed with imaging code. There is a Content Server IdocScript function to compute the URL in the weblayout directory.
Properties.Language	xIPMSYS_LANG	Customer metadata field
Properties.LastModifiedBy	dDocAuthor of latest revision	
Properties.LastModifiedDate	dCreateDate of latest revision	
Properties.LockedBy	dCheckoutUser	Content server does not have a locking concept other than checking out a document to prevent others from checking it out.
Properties.LockedDate	none	
Properties.MimeType	dFormat	
Properties.RetentionPolicyName	none	
Properties.Size	dFileSize	
Properties.StoragePolicyDate	none	
Properties.StoragePolicyName	none	
Properties.Version	dRevisionID	This distinct from dRefLabel which can be modified by the user.

<b>Oracle I/PM Document Property</b>	<b>Content Server Property</b>	<b>Comment</b>
Properties.VolumeName	none	If a file store provider is configured and used, this could come from the rules.
FieldValues	Custom metadata fields defined by Application	
Permissions.Delete	Delete	Can be determined from IdocScript userHasGroupPrivilege(dSecurityGroup, "D") function (or code that implements the function).
Permissions.Grant	Admin	Can be determined from IdocScript userHasGroupPrivilege(dSecurityGroup, "A") function (or code that implemented the function)
Permissions.Modify Fields	Write	Can be determined from IdocScript userHasGroupPrivilege(dSecurityGroup, "W") function (or code that implements the function)
Permissions.Update	Write	Can be determined from IdocScript userHasGroupPrivilege(dSecurityGroup, "W") function (or code that implements the function)
Permissions.View	Read	Can be determined from IdocScript userHasGroupPrivilege(dSecurityGroup, "R") function (or code that implements the function)
AnnotationPermissions	N/A	Annotation permissions are managed via I/PM Entity Beans.
Revision History	<Versions>	Revision history is provided as part of DOC_INFO service.
Audit History	<Content Tracker>	Auditing history must be obtained by reading the appropriate auditing data via the Content Tracker APIs.





---

---

## Troubleshooting

This appendix contains information about troubleshooting. It includes information about the following topics.

- ["Contacting Support"](#) on page 10-1
- ["UI Slowdown"](#) on page 10-2
- ["Decimal Field Error"](#) on page 10-2
- ["I/PM and Windows Server Prerequisites"](#) on page 10-3
- ["Search Results Not Displaying Seconds When Displaying Time"](#) on page 10-3
- ["NULL Number Fields"](#) on page 10-3
- ["Full-Text Search Fails On Large Documents"](#) on page 10-3
- ["Repository Capacity Errors"](#) on page 10-3
- ["Problems Connecting Multiple I/PM Systems to Single Repository"](#) on page 10-4
- ["Font Errors"](#) on page 10-4
- ["Input Agent and Input File Issues"](#) on page 10-5
- ["Advanced Viewer Transformation Errors"](#) on page 10-6
- ["Problems with TIFF Display in Viewer"](#) on page 10-6
- ["Shared Temp Directory in Linux Causes Display Failure"](#) on page 10-6
- ["Shifting Redaction and Other Annotations"](#) on page 10-6
- ["Logging of ImagingException"](#) on page 10-7
- ["Reviewing Audit History of Deleted Documents"](#) on page 10-7
- ["Deciphering Nested Stack Errors"](#) on page 10-7
- ["500 Internal Server Error When Using OSSO"](#) on page 10-8
- ["Oracle Content Server 10g Provides Incorrect Dates for BPEL"](#) on page 10-8
- ["Doc URL Returned With Invalid IP Address"](#) on page 10-9

### 10.1 Contacting Support

If you purchased Oracle Product Support, you can call Oracle Support Services for assistance. Oracle Support Services include phone assistance, version updates, and access to Oracle service offerings. You have access to phone support 24 hours a day, 7 days a week. In the U.S.A., you can call Product Support at 1-800-223-1711.

Make sure you have your CSI (Customer Support Identifier) number ready when you call. Keep the CSI number for your records because it is your key to Oracle Support Services. The Oracle Store sends the CSI number to you in an e-mail alert when it processes your order. If you do not have your CSI number and you are in the U.S.A., you can look up your CSI number by accessing the online Order Tracker, which provides detailed order information. Go to the Oracle Store and click Order Tracker, above the top navigation bar.

For Oracle Support Services locations outside the U.S.A., call your local support center for information on how to access support. To find the local support center in your country, visit the Support Web Center at <http://www.oracle.com/support>.

The Support Web Center has information about Oracle Support Services, such as these topics:

- Contact Information
- Instructions for Accessing Electronic Services
- Helpful Web Sites
- Support Resources
- Oracle Support Portfolio
- Oracle Support Service News

With Oracle Product Support, you have round-the-clock access to My Oracle Support (formerly Oracle MetaLink), Oracle Support Services premier Web support offering. My Oracle Support offers you access to installation assistance, product documentation, and a technical solution knowledge base.

It has technical forums, where you can post questions about your Oracle products and receive answers from Oracle Technical Support Analysts and other Oracle users. The questions and answers remain posted for the benefit of all users.

My Oracle Support options include:

- Technical Assistance Request (TAR) access
- Patch Downloads
- Bug Database Query Access
- Product Life-Cycle Information

You can access My Oracle Support at <http://metalink.oracle.com>.

## 10.2 UI Slowdown

If you are experiencing long delays in the UI, turn on the LogDetailedTimes MBean to collect entries that you can review to determine where the slowdown is occurring. When not experiencing slowdowns, turn off LogDetailedTimes because it floods the log with entries that are really only useful for troubleshooting slowdowns.

## 10.3 Decimal Field Error

Oracle I/PM supports 15 digits of precision centered around the decimal separator. Note the min/max values are not inclusive. Some examples:

Scale of 2:

- Value must be less than 10,000,000,000,000.00

- Value must be greater than -10,000,000,000,000.00

Scale of 5:

- Value must be less than 10,000,000,000.00000
- Value must be greater than -10,000,000,000.00000

## 10.4 I/PM and Windows Server Prerequisites

Oracle I/PM uses OutsideIn Technology which requires the Visual C++ libraries included in the Visual C++ Redistributable Package available from Microsoft. There are three versions of this package (x86, x64, and IA64) for each corresponding version of Windows. These can be downloaded from [www.microsoft.com/downloads](http://www.microsoft.com/downloads), by searching on the site for the packages `vc redistrib_x86.exe`, `vc redistrib_x64.exe`, or `vc redistrib_IA64.exe`. The required version of each of these downloads is the Microsoft Visual C++ 2005 SP1 Redistributable Package. The redistributable module that OutsideIn requires is `msvcr80.dll`.

## 10.5 Search Results Not Displaying Seconds When Displaying Time

By default, the Oracle Content Server repository is not set to return seconds to Oracle I/PM when returning time information for display in a search results table. If you require seconds to be displayed in a search results table date and time field, you must configure the Content Server repository to return seconds when returning time information to Oracle I/PM using the SystemProperties applet. In order to run the SystemProperties applet, you must first temporarily disable JpsUserProvider. To configure Content Server to return seconds, see ["Configuring Display of Seconds in Search Results"](#) on page 3-15.

## 10.6 NULL Number Fields

When a search is executed on an application with a number field that returns hits with documents with nothing entered in a number field, either a 0 or a -1 appears in the field. When an application containing documents is modified to have a number field, the search returns -1 for those documents.

When a document is uploaded and the number field is left blank, the search returns 0. If a search is executed with the number field as a condition, they are treated as empty fields and when viewed in Oracle Content Server, the fields are empty.

The null number field issue is a result of Oracle Content Server functionality.

## 10.7 Full-Text Search Fails On Large Documents

By default, the maximum document size that will be indexed is 10MB. This is changed by setting the `MaxIndexableFileSize` configuration variable in the Content Server repository. The default is `MaxIndexableFileSize=10485760`. If larger documents require full-text indexing, the value of `MaxIndexableFileSize` should be increased.

## 10.8 Repository Capacity Errors

A Oracle Content Server repository can get full to the point of reducing Oracle I/PM efficiency at which time it will not accept any new applications. However, you may continue to upload documents to existing applications in that repository.

A Oracle Content Server repository is considered full if any of the following are true:

- The number of security groups exceeds the value of the environment variable `IpmMaxGroupLimit`.
- The number of roles assigned permission to security groups exceeds the value of the environment variable `IpmMaxGroupRoleLimit`.
- The number of metadata fields exceeds the value of the environment variable `IpmMaxMetadataFields`.
- The Content Server configuration setting `IpmRepositoryForceFull=True`  
Setting `IpmRepositoryForceFull` equal to `True` allows you to configure Content Server to identify itself as full to I/PM in order to prevent additional applications from being created. This does not prevent documents from being uploaded.

To get additional space for applications, do one of the following:

- Install an additional Oracle Content Server repository and set it as a proxy to the main content server. For information on how to configure a proxy server, see the Oracle Universal Content Management *Managing System Settings and Processes* guide.
- Increase the values of the `IpmMaxGroupRoleLimit` and `IpmMaxMetadataFields` environment variables by editing the `config.cfg` file directly or by using the Oracle Content Server administrative server. For more information about changing Oracle Content Server environment variables, see the Oracle Universal Content Management guide *Managing System Settings and Processes*.

You can also change these environment variable values in the `config.cfg` file for your Content Server Repository. For more information, see the Oracle Universal Content Management *Managing System Settings and Processes* and *Getting Started with Content Server* guides.

## 10.9 Problems Connecting Multiple I/PM Systems to Single Repository

When two or more I/PM systems are using the same Content Server repository, the `AgentUser` must be configured with the same user. If `AgentUser` is configured with different repository users for each I/PM system, each I/PM system competes with what `AgentUser` should be within the repository.

## 10.10 Font Errors

Documents with text content require the fonts necessary to render the document to be available to the `OutsideIn` rendering engine, which uses TrueType fonts. Fonts are not provided by Oracle. If the font used in a document is not available to `OutsideIn`, then a suitable substitute will be used. Font substitutions can cause a document to be unreadable, create incorrect text formatting, or cause shifting of data or repagination on text documents, including potentially exposing redacted content.

To ensure that proper fonts are used when rendering documents, the administrator should install them to the client and server system. The server MBean `GdFontPath` should be set to the directory where the fonts are installed. When using the advanced viewer mode on Linux systems, the fonts can be installed and the environment variable `GDFONTPATH` set to that directory. If the environment variable is not found, the user will be prompted for that path the first time the advanced viewer mode is used. In cases where an attempt to download a document as a TIFF before the path is set, and error may occur that prevents downloading the TIFF rendition.

For more information, see ["Configuring the AgentUser and GdFontPath MBeans"](#) on page 3-15.

## 10.11 Input Agent and Input File Issues

The following issues involve input agents or input files.

### 10.11.1 Input Agent Will Not Detect and Process Input Files

If the input agent will not pick up input files, try the following steps to determine a solution.

1. Check the settings of the following Oracle I/PM MBeans:
  - **AgentUser:** This must be set to a valid user in the security store for the agents to operate. Content Server and I/PM must be restarted if the AgentUser changes. Note that if multiple I/PM systems connect to one Content Server repository, the same AgentUser should be configured for each I/PM system.
  - **CheckInterval:** Make sure this is set to a reasonable amount of time for your environment (for example, maybe 1 minute for test systems or 30 minutes for production systems that do not need to get data right away) and ensure that enough time has expired for at least one polling interval to have occurred.
  - **InputDirectories:** Examine the list of directories and ensure that they are the correct directories where the input files are stored.
2. Ensure that the input file has Read/Write permissions for WebLogic Server.
3. Check the permissions on the input directory paths and make sure they are accessible to the user that is running the WLS managed server.
4. Look at the input object in the user interface and make sure the input that is supposed to be processing is marked online and that the input file mask matches the files that are in the directory.
5. If the input agent is still not running then examine the log files to see if an error was encountered that is preventing the agent from functioning.

### 10.11.2 Auto-detect Not Determining Character Set

Auto-detect does not work if the provided sample file is not large enough to get an accurate determination of the character set. If the sample file is too small, disable **Auto-detect input file character set** and manually select the character set.

### 10.11.3 Input File Entries Have Errors

For the steps below, refer to the following directory structure:

```
Input
- Errors
- Failed
  - YYYY-MM-DD
- Processed
  - YYYY-MM-DD
- Samples
- Stage
```

If some or all of the entries in the input file have errors, try the following steps to determine a solution.

1. Look at the Errors directory in which the input file was placed and see if an error file was created. If an error file exists, then open it and examine the last column of the file to determine the specific error.

2. Examine the input file and verify that the path to the image file is accessible to the user that is running the Oracle I/PM managed server and that the user has permissions to the path and image files.
3. Copy one of the failing input files to the samples directory and load it into the input definition editor UI. Verify that the mappings are correct and that one of the columns has not shifted.
4. Finally, look at the Oracle I/PM log file and examine the errors that are listed for the individual lines to determine the exact cause of the problems.

Once you have determined the cause of the error and are able to correct it, copy the corrected input file back into the input directory. For additional information, see ["Checking Results and Error Files"](#) on page 5-8.

#### 10.11.4 Dates and Times Shifting on Content Ingested Using Input Agent

Dates and times specified in the input file are subject to current Daylight Savings Time rules, and not the DST rules in effect for the specified date. This can cause the timestamp of the document to shift forward or back up to two hours. If the timestamp shifts forward or back across midnight, the date used for the document input may also shift.

### 10.12 Advanced Viewer Transformation Errors

In cases where the advanced viewer applet experiences transformation errors, the first response is to delete temporary files on the user's workstation. Doing so will remove the distribution of OutsideIn files which will cause a new deployment next time the applet is used.

#### 10.13 Problems with TIFF Display in Viewer

The Advanced Viewer mode renders Group 6 and Group 7 TIFFs, while the Basic Viewer mode supports Group 7 but not Group 6 TIFFs. Group 7 TIFFs must conform to the TIFF standard for JPEG compression. Color images should use YCbCr for photometric interpretation or the image will be treated as a grayscale image. YCbCr is the standard color for JPEG images.

#### 10.14 Shared Temp Directory in Linux Causes Display Failure

When using Oracle I/PM in a multi-user Linux environment, ensure that individual temp directories are set up for each user. Using a temp directory shared among several users can cause the Advance Viewer to delete temp files for one user that are necessary for another, causing a problem with documents not displaying. Ensure that each user has a temp directory created and configured as recommended by the operating system documentation.

#### 10.15 Shifting Redaction and Other Annotations

Annotations are placed based on coordinates, and in some circumstances, content underneath the annotation may shift. This can be a particular problem when a redaction annotation shifts, potential exposing sensitive information. For example, if a document contains text data and the font used in a document is not available to the OutsideIn rendering engine, then a suitable substitute will be used. Font substitutions can cause a document to be unreadable, create incorrect text formatting, or cause

shifting of data and repagination on text documents, including potentially exposing redacted content.

If annotations become misaligned and expose text they originally covered, ensure that a consistent set of fonts is being used across the servers and clients. For information on font errors, see "[Font Errors](#)" on page 10-4.

## 10.16 Logging of ImagingException

By default, not all exceptions caught within I/PM are logged. In the event that all exceptions need to be monitored, the following steps will help identify all exceptions thrown.

By default, not all exceptions caught within I/PM are logged. I/PM exception handlers do not inherit a log level from a parent logger (oracle.imaging.service). To get exceptions from the core I/PM services, you must explicitly set the logger named *oracle.imaging.service.exceptions*.

To enable some degree of flexibility, it uses the following log levels:

- ERROR 1(SEVERE): Logs SYSTEM and DATABASE ImagingExceptions
- NOTIFICATION(INFO): Logs SYSTEM, DATABASE, and SECURITY ImagingExceptions
- TRACE(FINE): Logs SYSTEM, DATABASE, SECURITY, and USAGE ImagingExceptions

For example, all ImagingExceptions would be logged at throw time by setting oracle.imaging.service.exceptions to TRACE:32.

## 10.17 Reviewing Audit History of Deleted Documents

If documents are deleted from I/PM, administrators can view the entry for the delete action in the Content Server DocumentHistory table. This is the only place for administrators to view audit entries for deleted documents.

## 10.18 Deciphering Nested Stack Errors

A nested stack error, also called a nested exception, is basically an error that has been wrapped by another error, which is standard with Java and other languages to help provide more context to the issue. You can usually find the nested exception by locating the *caused by* string in the stack trace as shown in bold in the following example. If there is not enough information provided by the Oracle I/PM error, look deeper into the error message to see if other components are involved. Oracle I/PM uses nested stack errors to display repository related problems, BPEL issues, or problems caused by other components. After you locate the possible initial error, check the diagnostic logs for more troubleshooting information.

In the following example, the TCM-00787 error is occurring because the default provider within the Oracle Content Server repository was corrupted and reset (see boldface text).

```
[2009-06-11T09:56:21.720-07:00] [ipm_server1] [ERROR] []
[oracle.imaging.ui.backing.application.LifecycleState] [tid:
[ACTIVE].ExecuteThread: '4' for queue: 'weblogic.kernel.Default (self-tuning)']
[userId: weblogic] [ecid:
0000I7GFuQ9F8DT6uBj8EH1AC2Ut0000WK,0] [APP: imaging#11.1.1.1.0] IPM UI Exception[[
oracle.imaging.ImagingException: TCM-00787: A repository error has occurred.
```

```

Contact your system administrator for assistance.
    stackTraceId: 9-1244739381674
    faultType: SYSTEM
    faultDetails:
        ErrorCode = oracle.stellent.ridc.protocol.ServiceException,
ErrorMessage = File
'/app/stellent/content/10gR3/proxy1/data/providers/defaultfilestore/provider.hda'
does not exist.
    at
oracle.imaging.repository.ucm.UcmErrors.convertRepositoryError(UcmErrors.java:108)
    at
oracle.imaging.repository.ucm.UcmLifecycleOperationImpl.getStorageRules(UcmLifecyc
leOperationImpl.java:58)
...
<...snip...>
    at
weblogic.servlet.internal.ServletRequestImpl.run(ServletRequestImpl.java:1428)
at weblogic.work.ExecuteThread.execute(ExecuteThread.java:201)  at
weblogic.work.ExecuteThread.run(ExecuteThread.java:173)
Caused by: oracle.stellent.ridc.protocol.ServiceException: File
'/app/stellent/content/10gR3/proxy1/data/providers/defaultfilestore/provider.hda'
does not exist.
    at
oracle.stellent.ridc.protocol.ServiceResponse.getResponseAsBinder(ServiceResponse.
java:116)
    at
oracle.stellent.ridc.protocol.ServiceResponse.getResponseAsBinder(ServiceResponse.
java:92)
    at
oracle.imaging.repository.ucm.UcmResponse.<init>(UcmResponse.java:61)
    at
oracle.imaging.repository.ucm.UcmRequest.makeOneServiceCall(UcmRequest.java:310)
    at
oracle.imaging.repository.ucm.UcmRequest.makeServiceCallWithRetries(UcmRequest.jav
a:228)
    at
oracle.imaging.repository.ucm.UcmRequest.makeServiceCall(UcmRequest.java:210)
    at
oracle.imaging.repository.ucm.UcmLifecycleOperationImpl.getStorageRules(UcmLifecyc
leOperationImpl.java:53)
... 234 more

```

## 10.19 500 Internal Server Error When Using OSSO

When using Oracle Single Sign On, POST requests to WebLogic Server will return an internal server error when the Oracle I/PM session has expired. Refreshing the page returns to the I/PM log in page for reauthentication to start a new session.

## 10.20 Oracle Content Server 10g Provides Incorrect Dates for BPEL

When using Content Server 10g, the BPEL payload is populated with the incorrect date when the date is less than 1969 or greater than 2068. As a workaround, it is recommended that if you are using dates that fall outside the range of 1969-2068, use four digit years for the date. You can set this using the Content Server System Properties utility.



## 10.21 Doc URL Returned With Invalid IP Address

Users that are getting a host name or IP address that they don't expect for the document URL probably need to configure the Listener Address in their WLS server. This can be done either by setting listen-address in config.xml for the WLS server, or by using the WLS console. To use the console, expand Environment and click Servers in the Domain Structure window. In the Servers Configuration tab, click on the desired server name. Set Listen Address on this page. Restart WLS. For more information about WLS configuration, see *Oracle Fusion Middleware Administrator's Guide*.



---

---

## User Interface

This Appendix contains information about the interface used with Imaging and Process Management (Oracle I/PM).








The following pages are shown in this section:

- ["Icons"](#) on page A-2
- ["Navigator Pane"](#) on page A-3
- ["Navigation Train"](#) on page A-4
- ["Upload Document Page"](#) on page A-4
- ["Update Document Page"](#) on page A-6
- ["Export Definitions: Export Comments Page"](#) on page A-7
- ["Export Definitions: Applications Page"](#) on page A-7
- ["Export Definitions: Searches Page"](#) on page A-8
- ["Export Definitions: Inputs Page"](#) on page A-9
- ["Export Definitions: Summary Page"](#) on page A-9
- ["Import Definitions: File Location Page"](#) on page A-10
- ["Import Definitions: Select Imports Page"](#) on page A-11
- ["Import Definitions: Validate Imports Page"](#) on page A-12
- ["Search Properties Page"](#) on page A-15
- ["Search Results Formatting Page"](#) on page A-16
- ["Search Conditions Page"](#) on page A-17
- ["Search Parameters Page"](#) on page A-19
- ["Search Security Page"](#) on page A-20
- ["Add Security Member Page"](#) on page A-20
- ["Search Preview and Test Page"](#) on page A-21
- ["Search Summary Page"](#) on page A-22
- ["Application General Properties Page"](#) on page A-24
- ["Application Field Definitions Page"](#) on page A-25
- ["Application Security Page"](#) on page A-26
- ["Application Document Security Page"](#) on page A-27

- ["Application BPEL Configuration Page"](#) on page A-28
- ["BPEL Component Properties Page"](#) on page A-29
- ["BPEL Payload Properties Page"](#) on page A-30
- ["Edit Format Value Page"](#) on page A-31
- ["Application Review Settings Page"](#) on page A-32
- ["Input Basic Information Page"](#) on page A-33
- ["Input Identify and Parse File Parameters Page"](#) on page A-34
- ["Input Field Mapping Page"](#) on page A-35
- ["Define Date Format Page"](#) on page A-36
- ["Input Security Page"](#) on page A-38
- ["Input Review Settings Page"](#) on page A-39
- ["Content Server Connection Basic Information Page"](#) on page A-40
- ["Content Server Connection Content Server Settings Page"](#) on page A-41
- ["Content Server Connection Security Page"](#) on page A-42
- ["Content Server Connection Review Settings Page"](#) on page A-43
- ["BPEL Connection Basic Information Page"](#) on page A-44
- ["BPEL Connection Settings Page"](#) on page A-45
- ["BPEL Connection Security Page"](#) on page A-46
- ["BPEL Connection Review Settings Page"](#) on page A-47
- ["Manage Security"](#) on page A-48

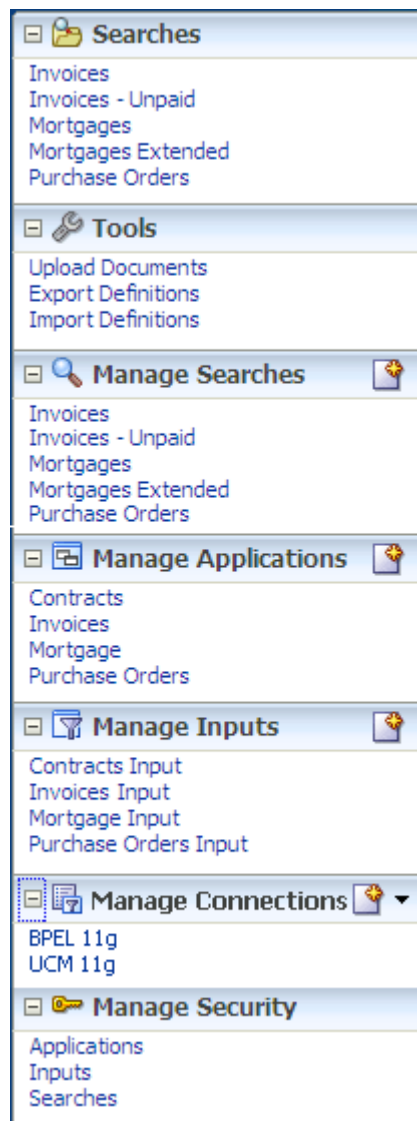
## A.1 Icons

The following icons are used throughout the Oracle I/PM interface without explicit identification. In some cases, as in the pencil icon, the exact use is determined by the context it is in. You can place your cursor over an icon to view identifying text about it.

Name	Icon	Description
Collapse or Restore Pane		Click to expose or hide a pane.
Show or Hide this Panel		Click to expose or hide a panel.
Create		Click to create a new item. Items may be searches, application, or other.
Close Current		Click to close a current tab or window.
More Options		Click to expand a hidden menu.
Expand Horizontally		Click to expand an item horizontally.
Edit, Modify, or Update		Click to edit, update, or modify a value or document.

## A.2 Navigator Pane

The navigator pane displays the top-level navigation panels used to access the main features of Oracle I/PM.



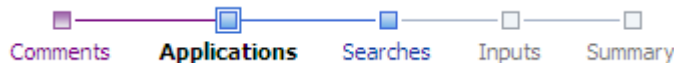
The following table describes the options available on the page.

Panel	Description
Searches	Lists all searches to which you have rights. Clicking on a search name displays the search form in the content region. The search form is used to enter criteria to find documents in Oracle I/PM.

Panel	Description
Tools	<p>Contains the following options:</p> <ul style="list-style-type: none"> <li>▪ <b>Upload Documents:</b> Displays the <a href="#">Upload Document Page</a> used to add documents to the repository.</li> <li>▪ <b>Export Definitions:</b> Displays the <a href="#">Export Definitions: Export Comments Page</a> used to export application, input and search definitions.</li> <li>▪ <b>Import Definitions:</b> Displays the <a href="#">Import Definitions: File Location Page</a> used to import application, input and search definitions.</li> </ul>
Manage Searches	<p>Lists all searches to which you have at least Modify or Grant Access rights. Click the expand icon to view the Create New Search icon. Click this icon to open the <a href="#">Search Properties Page</a> to create a new search.</p>
Manage Applications	<p>Lists all created applications to which you have at least Modify or Grant Access rights. Click the expand icon to view the Create Application icon. Click this icon to open the <a href="#">Application General Properties Page</a> to create a new application.</p>
Manage Inputs	<p>Lists all created inputs to which you have at least Modify or Grant Access rights. Click the expand icon to view the Create Input icon. Click this icon to open the <a href="#">Input Basic Information Page</a> to create a new input.</p>
Manage Connections	<p>Lists all created connection to which you have at least Modify or Grant Access rights. Click the expand icon to view the Create New Connection menu icon. Click this icon to open a menu and select <b>Create Content Server Connection</b> to display the <a href="#">Content Server Connection Basic Information Page</a> or select <b>Create BPEL Connection</b> to display the <a href="#">BPEL Connection Basic Information Page</a>.</p>
Manage Security	<p>Used to grant security rights to applications, inputs, and searches.</p>

### A.3 Navigation Train

The Navigation Train is displayed on all pages in Oracle I/PM that are used within a procedure such as creating searches, applications, and inputs. The current step of the procedure is in **Bold** and has a double box icon above the step name. Click **Next** when the required information has been entered to proceed to the next page. Click **Back** to visit a previous page or access steps directly by clicking the step name or icon in the navigation train. Steps displayed in gray have not yet been completed in a sequential process, such as creating an application, and cannot be navigated to until each preceding step is completed. Once all steps have been completed, all steps in the navigation train are enabled and can be used to jump from one step to another non-sequentially.



### A.4 Upload Document Page

Access the Upload Document page by clicking **Upload Document** in the **Tools** panel in the [Navigator Pane](#).

---

**Note:** When uploading a document, be aware of the file size. File size limitations are primarily a factor when retrieving a document for viewing. System architecture, hardware limitations, network load and other factors can influence document retrieval times and cause the viewer to time out. Oracle I/PM has been optimized to store tiff image files of sizes to 200KB. If the documents you need to upload and view are larger than to 200KB, test the performance of with those files in the specific network architecture you are planning to use while simulating peak network load.

---

The following table describes the elements available on the page.

Element	Description
Open Viewer	Displays the Viewer next to the Upload Document page, replacing the Document Image field and Browse button. Use the Viewer to navigate to a document and to review and annotate a document before uploading. This is useful when you need to view the document to see the associated metadata to be entered, such as an invoice number or title, if you need to see the document to determine what application should be used, or if you want to annotate a document when uploading. Note that you must select an application and enter the associated metadata values before completing the upload.
Upload	Submits the document and metadata to Oracle I/PM based on the selected application. When the document has been successfully uploaded, you will see a confirmation message. Clicking the confirmation message opens the uploaded document in the viewer.
Reset	Resets the page and allows for another document to be uploaded. Click this to clear inaccurate information before submitting the document or to clear the information and confirmation of a successfully submitted document so you can upload another one.
Close	Closes the Upload Document page and returns to the Welcome page or an open search tab if one or more searches have been run.

Element	Description
Select An Application	Select an application in which to upload the document. This is a required field. Once an application is selected, metadata fields specific to the application are displayed. Application-specific metadata fields are determined when the application is defined and will likely be different for each application.
Document Image field and Browse button	Enter the path to the image being uploaded, or click <b>Browse</b> to select the file. This is a required field. This field is replaced with the Viewer if Open Viewer is clicked, and the viewer is used to navigate and select the file to upload.  Note that if using your keyboard rather than your mouse to select the Browse button, use the Space bar to execute the Browse button function and open the dialog box. The Enter key does not execute the Browse button function.

## A.5 Update Document Page

Use the Update Document function to update or add a new version of an existing document. Depending on the application configuration and repository, you can replace the existing document, create a new version, or update one or more application fields of the existing document.

From within a search results list, select a document and click **Update** in the Search Results toolbar. The Update Document window opens and displays the Original File Name, Document ID, and its application. To add a new version of the existing document, enter the path and name of the file, or click **Browse** to select it, and click **Update**. To update specific fields in the existing document, make your changes to the fields displayed and click **Update**. Upon successful update, you will see a confirmation message.

It is recommended that you lock a document prior to updating it in order to prevent others from updating the document at the same time. You can easily lock a document from a search results listing using the contextual menu or search results toolbar. If a document is locked before being updated, the Keep Lock check box is displayed at the bottom of the Update document page. Select to keep the document locked after it is updated. If you did not have it locked before clicking Update, the Lock Document check box will appear. Select to lock the document after it is updated.

The screenshot shows the 'Update Document' window. At the top right is an 'Update' button. Below the title, the document details are displayed:

- Document ID: 3.IPM\_017684
- Original Filename: ipm\_017684.tiff
- Application Name: Invoices
- Amount: 1538025649.02
- Vendor: Bowman Electronics
- Receive Date: 3/3/2009 12:00 AM
- Purchase Order: 108278
- Invoice Number: 601387

At the bottom left, there is a checkbox labeled 'Keep Lock'.



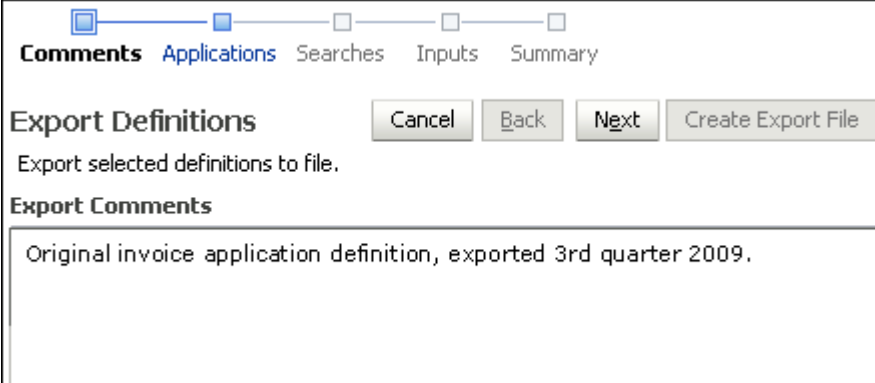
The following table describes the elements available on the page.

Element	Description
Update	Submits the document and metadata to Oracle I/PM based on the selected application. When the document has been successfully updated, you will see a confirmation message. If you receive a system error message, review the log files to determine its cause.
File name field and Browse button	Type the name of the new file or click <b>Browse</b> to select it. Note that if using your keyboard rather than your mouse to select the Browse button, use the Space bar to execute the Browse button function and open the dialog box. The Enter key does not execute the Browse button function.
Application fields	Information fields vary by application. Change the information in an existing document by updating one or more of the application fields.
Keep Lock or Lock Document	If document is locked, select Keep Lock to remain locked after being updated. If document is not locked, select Lock Document to lock document after being updated.

## A.6 Export Definitions: Export Comments Page

Application, input, and search definitions can be exported to a transportable file format (XML) for import and use in other systems. Enter a short description and other pertinent information in the Comments field about the export file.

Access the Export Definitions Comments page by clicking **Export Definitions** in the Tools panel in the navigator pane.



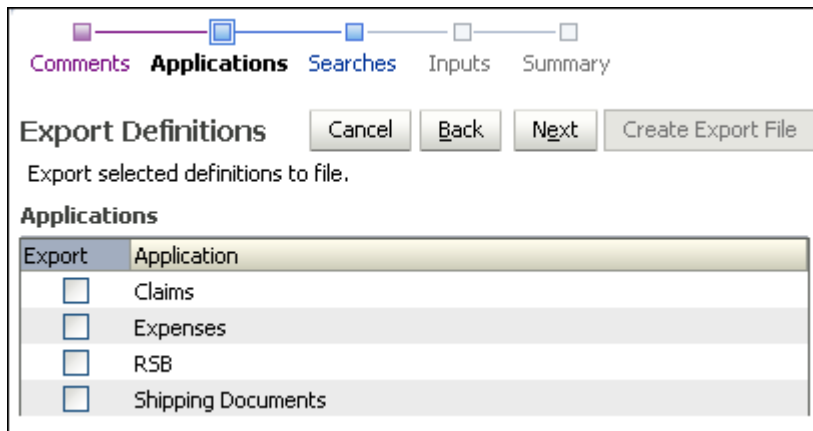
The following table describes the elements available on the page.

Element	Description
Cancel	Cancels the export procedure and returns to Oracle I/PM welcome page.
Next	Continues to next step.
Export Comments field	Type the description or other pertinent information for the definitions file being created.

## A.7 Export Definitions: Applications Page

Select the applications to be included in the export definitions file by enabling the check box in the **Export** column next to the application name.

Access the Export Applications page by clicking **Next** on the Export Comments page.



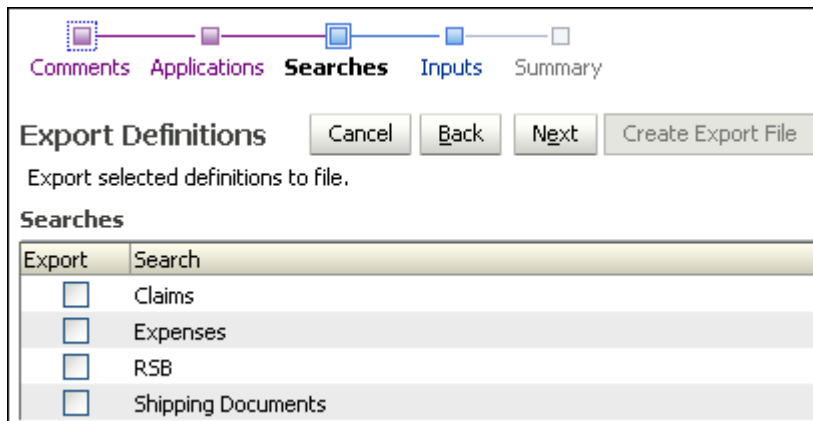
The following table describes the elements available on the page.

Element	Description
Export	Select to export the application on that line.
Application	Name of the application to include in the Export Definitions file.

## A.8 Export Definitions: Searches Page

Select the searches you want to export by selecting the field in the Export column next to the search name.

Access the Export Definitions Searches page by clicking **Next** on the Export Definitions Applications page or by clicking searches in the [Navigation Train](#).



The following table describes the elements available on the page.

Element	Description
Export	Select to export the search on that line.
Search	Name of the search to include in the Export Definitions file.

## A.9 Export Definitions: Inputs Page

Choose the input definitions to export by selecting the field in the Export column next to the input name.

Access the Export Definitions Inputs Page by clicking **Next** on the Import Definitions Searches page or by clicking on Inputs in the [Navigation Train](#).

Comments Applications Searches **Inputs** Summary

Export Definitions

Export selected definitions to file.

**Inputs**

Export	Input
<input checked="" type="checkbox"/>	Invoices
<input checked="" type="checkbox"/>	Purchase Orders
<input type="checkbox"/>	Shipping

The following table describes the elements available on the page.

Element	Description
Export	Select to export the input on that line.
Input	Name of the input to include in the Export Definitions file.

## A.10 Export Definitions: Summary Page

Review your selected definitions and make any necessary changes. Then click **Create Export File**. A File Download window displays where you indicate whether you want to open, save or cancel the new Export Definitions File.

Access the Export Definitions Summary Page by clicking **Next** on the Export Definitions Inputs page or by clicking Summary in the [Navigation Train](#).

**Export Definitions**

Export selected definitions to file.

**Export Comments**

For server 1

**Applications**

Export	Application
<input type="checkbox"/>	Claims
<input type="checkbox"/>	Invoices

**Searches**

Export	Search
<input checked="" type="checkbox"/>	Claims
<input checked="" type="checkbox"/>	Expenses
<input type="checkbox"/>	HR Claims
<input type="checkbox"/>	Invoices

**Inputs**

Export	Input
<input checked="" type="checkbox"/>	Invoices
<input checked="" type="checkbox"/>	Purchase Orders
<input type="checkbox"/>	Shipping

The following table describes the elements available on the page.

Element	Description
Summary sections	Displays a summary of the selections made in each of the Export Definitions pages.

## A.11 Import Definitions: File Location Page

Access the Import Definitions Select File page by clicking **Import Definitions** on the Tools panel in the [Navigator Pane](#).

**Select File**

Select the file containing the exported definitions.

Select File

**File Properties**

File Date 12/2/2009 9:28 AM

File Comments

The following table describes the elements available on the page.

Element	Description
Select File field	Click <b>Browse</b> to locate and select the file that contains the definitions to import or type the file name in the field.  Note that if using your keyboard rather than your mouse to select the Browse button, use the Space bar to execute the Browse button function and open the dialog box. The Enter key does not execute the Browse button function.
File Properties section	After a file is selected, displays the date of file creation and associated comments.

## A.12 Import Definitions: Select Imports Page

Choose the applications, inputs, and searches to be imported by selecting the field in the Import column next to the application, input or search name.

Access the Import Definitions Select Definitions page by clicking **Next** on the [Import Definitions: File Location Page](#).

**Select Imports**      Cancel    Back    Next    Submit

Select the definitions to import.

**Applications**

Action	Application	Repository
<input type="checkbox"/> Overwrite	Invoices	tcmlcluster-4 UCM
Inbound Invoice Documents to be paid		
<input type="checkbox"/> Overwrite	Purchase Orders	tcmlcluster-4 UCM
Purchase Orders to be processed		
<input type="checkbox"/> Overwrite	Shipping Documents	tcmlcluster-4 UCM

**Inputs**

Action	Input
<input type="checkbox"/> Add	Invoices NY Server
<input type="checkbox"/> Overwrite	Purchase Orders
<input type="checkbox"/> Input Is Online	Shipping

**Searches**

Action	Search
<input type="checkbox"/> Add	Invoices Past Due
<input type="checkbox"/> Overwrite	Purchase Orders
<input type="checkbox"/> Overwrite	Shipping Documents

The following table describes the elements available on the page.

Element	Description
Action	<p>Select the specific definitions to import for applications, inputs, and searches by selecting the field under the Action heading. Options are:</p> <ul style="list-style-type: none"> <li>▪ <b>Add:</b> If the object you are importing the definition of does not exist on the system you are importing to, then the action taken is to add the imported definition file and create the object.</li> <li>▪ <b>Overwrite:</b> If the object you are importing the definition of exists on the system you are importing to, then the action taken is to overwrite the existing definition file with the imported definition file.</li> </ul> <p>Note that you must take existing input definitions offline before you can import a definition to overwrite the existing input. You take an input definition offline and online by clicking <b>Toggle Online</b> on the Input Summary page, accessed by clicking the input name in the Manage Inputs panel.</p>
Applications, Inputs, Searches Sections	<p>Each application, input, or search is listed under the appropriate heading.</p>
Repository	<p>When there are multiple Oracle Content Server repositories, use the Repository picklist to select the repository to which the imported definition should be applied.</p>

## A.13 Import Definitions: Validate Imports Page

After all selections are made on this page, click **Submit**. The definitions being imported reference multiple system-specific items, such as security groups, storage devices, and repository connections. All of these items are referenced by name. As long as items are named correctly between the two systems, importing definitions will be successful with no additional adjustment. By the time the Validate Imports page is displayed, I/PM has validated each of these system-specific items to determine if the definitions can imported as provided. If the definitions are valid, the Successful Validation icon (a check mark) will display in the Status column. If not valid, the Validation Failed icon will display. If a failure occurs, click the expand button to see details. Change options or verify that users and groups exist on the target system and click **Submit** again. If you receive a system error message, review log files to determine the problem.

Access the Import Definitions Select File page by clicking **Next** on the [Import Definitions: Select Imports Page](#).

The following table describes the elements available on the page.

Element	Description
Submit	Click <b>Submit</b> to import the selected application, input, and search definitions.
Status	A Successful Validation icon or Failed Validation icon is displayed indicating whether or not to proceed with importing the definition or definitions.
Action	Specifies the action being taken with the import. Options are: <ul style="list-style-type: none"> <li>▪ <b>Add:</b> If the object you are importing the definition of does not exist on the system you are importing to, then the action taken is to add the imported definition file and create the object.</li> <li>▪ <b>Overwrite:</b> If the object you are importing the definition of exists on the system you are importing to, then the action taken is to overwrite the existing definition file with the imported definition file.</li> </ul>
Application	Name of application from which definitions are being imported.

Element	Description
Security	<p>Select from the following security options:</p> <ul style="list-style-type: none"> <li>■ <b>Use Imported:</b> Select this option to use the security information defined in the export file.</li> <li>■ <b>Current User:</b> Select this option to allow only the current user permission to modify which groups and users will be granted permission to the definition. This will allow the definition to be imported and this user will then be able to modify later which groups and users will be granted permissions to the definition.</li> <li>■ <b>Valid Entries Only:</b> Select this option for Oracle I/PM to check the security information in the export file and only pass entries that are valid for the target system. For example, if the file specifies user UserX but the target system does not recognize that user name, then UserX will not be configured in the target system.</li> <li>■ <b>Choose New:</b> Select this option to allow the user to select a user or group to be the only one with security to the definition. Similar to the Current User option, this selected user or group will be able to later modify which groups and users will be granted permissions to the definition. The user or group is selected by choosing the name from the popup dialog window that is launched when you click the Edit icon next to the Choose New picklist. When a user or group is selected, the Security and Document Security picklist is populated with the new user or group name.</li> <li>■ <b>Use Existing:</b> Select this option to use the existing definition security, ignoring the configuration in the imported definition. This option is available only for definitions that already exist on the system.</li> </ul>
Document Security	<p>Select from the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Use Imported:</b> Select this option to use the security information defined in the export file.</li> <li>■ <b>Valid Entries Only:</b> Oracle I/PM checks the security information in the export file and only passes entries that are valid for the target system. For example, if the file specifies group GroupY but the target system does not recognize that group name, then GroupY will not be configured in the target system.</li> <li>■ <b>Choose New:</b> Select this option to allow the user to select a group to be the only group with security to the definition. The selected group will be able to later modify which groups will be granted permissions to the definition. The group is selected by choosing the name from the popup dialog window that is launched when you click the Edit icon next to the Choose New picklist. When a group is selected, the Security and Document Security picklist is populated with the new group name.</li> <li>■ <b>Use Existing:</b> Select this option to use the existing definition security, ignoring the configuration in the imported definition. This option is available only for definitions that already exist on the system.</li> </ul>



Element	Description
Storage Policy	<p>Select from the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Use Imported:</b> Select this option to use the Storage Policy options defined in the export file.</li> <li>■ <b>Clear:</b> Select this option to clear out the Storage Policy options and use the system default.</li> <li>■ <b>Use Existing:</b> Select this option to use the existing Storage Policy settings, ignoring the configuration in the imported definition. This option is available only for applications that already exist on the system.</li> <li>■ <i>Additional Choices:</i> If there are specific storage options defined in your system, such as Network Attached Storage, they are appended to the list in the Storage Policy field.</li> </ul>
BPEL (Business Process Execution Language)	<p>Select from one of the following options:</p> <ul style="list-style-type: none"> <li>■ <b>Clear:</b> Select this option to remove all BPEL configurations for the application.</li> <li>■ <b>Use Existing:</b> Select this option to use the existing BPEL settings, ignoring the configuration in the imported definition. This option is available only for applications that already exist on the system.</li> <li>■ <i>Additional Choices:</i> BPEL connections defined for the target system are listed here. Different systems may connect to the same BPEL server but have different names for the connection. Because the input file being imported specifies the BPEL connection name of the original system, selecting the name of the target system BPEL connection ensures proper field mapping between the two.</li> </ul>
Document Upload	<p><b>Use Existing:</b> Select this option to use the existing definition document upload, ignoring the configuration in the imported definition. This option is available only for definitions that already exist on the system.</p>

## A.14 Search Properties Page

Use the Create Search Properties page to start creating a search that will be used more than once. If the Accounting department often searches for all Invoices during a specific year, create a search that specifies Invoices between the desired dates, such as January 1, 2008 and December 31, 2008.

Access this page by clicking the Create New Search icon on the Manage Searches panel in the [Navigator Pane](#). Expand the Manage Searches panel to view the Create New Search icon.

The following table describes the elements available on the page.

Element	Description
Search Name	Enter a descriptive name for the search. This search name will be displayed to users under the searches panel of the navigator pane and must be unique to I/PM.
Description	Enter a description of the new search. The description is displayed when the cursor hovers over the search name in the navigator pane. The field contains a maximum of 2000 characters.
Instructions	Enter helpful information about what criteria is being searched for and how a user should use the search. These instructions are available on the search form and also appear on the Search Tab display. If no instructions are defined, the Instructions section is not displayed on the search form. The field contains a maximum of 2000 characters.
Maximum Search Results	Select the maximum number of rows per application a search will return before stopping. The search can span multiple applications, which are selected on the <a href="#">Search Results Formatting Page</a> . The default is zero which means that the search will use the maximum results value set on the server.

## A.15 Search Results Formatting Page

The Create Search Results Formatting page is used to format how search results are displayed. Searches can be limited to one application or span multiple applications. For example, you can create a single search that returns purchase orders from a Purchase Order application and invoices from an Invoice application.

Access the Create Search Results Formatting page by clicking **Next** on the Create Search Properties page or by clicking Results Formatting on the [Navigation Train](#).

**New Search: Results Formatting** Cancel Back Next Submit

Select a source application or applications that you wish to return images from. Then select the fields in this application you wish to display to the user when their results are returned.

Source Application	Acct Nbr	Scan Date	Company Name
Customer Service	Acct Nbr	Scan Date	Company Name
Invoices	Invoice Numb	Invoice Date	Amount

The following table describes the elements available on the page.

Element	Description
Source Application	Specifies the application to be searched. The application selected determines the criteria fields available. Only applications to which you have View security rights are listed.
Field Columns	The second and subsequent columns represent the columns of metadata fields from the searched applications that will appear in the search results. Selecting a search field populates the column header with the name and enables the next column.
Column Options Icon	Clicking the Column Options icon in the column header displays the following options: <ul style="list-style-type: none"> <li>■ <b>Modify Column Name:</b> Allows you to rename the column header.</li> <li>■ <b>Move Column Left:</b> Moves the column one space to the left.</li> <li>■ <b>Move Column Right:</b> Moves the column one space to the right.</li> <li>■ <b>Delete Column:</b> Displays a dialog window asking you to confirm deleting the column.</li> </ul>
Remove Application Icon	Clicking the Remove Application Icon next to the Source Application displays a dialog window asking for confirmation to remove the application from the search.

## A.16 Search Conditions Page

Specify the conditions to be applied to each document in the searched applications to determine if they should be shown in the search results. Each condition contains three parts: the application's metadata field, the operator used for the comparison and the data value to be used. These conditions for each application can be grouped using parentheses and combined using the conjunction operators (and/or) to form complex conditions.

Access the Create Search Conditions page by clicking **Next** on the Create Search Results Formatting page or by clicking **Conditions** in the [Navigation Train](#).

The following table describes the elements available on the page.

Element	Description
	Moves the selected condition up one row.
	Moves the selected condition down one row.
	Displays a dialog window requesting confirmation to remove the selected condition.
(	Opening parenthesis for beginning conditional grouping.
Field	Selects the application field to be used in the condition.
Operator	Selects the operator used for the search. Available operators depend on the data type of the application selected.
Value	A search condition value is the value that the selected Field is being compared to. This value can be one of the following: <ul style="list-style-type: none"> <li>▪ <b>Static Value:</b> This is a value that does not change. The selected field is compared directly to this value. For example, Text_Field1 = "Hello".</li> <li>▪ <b>Relative Date:</b> This value represents a number of days from the current day. The value can be positive or negative. When the search is executed, the value is calculated from the current day. For example, Relative Date +7 is one week from today.</li> <li>▪ <b>Logged in UserID:</b> This value represents the userid of the user executing the search. The user's textual userid is used when the search is executed.</li> <li>▪ <b>Parameter Value &lt;name&gt;:</b> This value represents a value that is to be provided by the user when they execute the search.</li> </ul>
Modify Value Icon	Displays a dialog window with options for modifying value types.
)	Closing parenthesis for ending conditional grouping.
Conjunction	Logical operator for grouping together the smaller condition elements. <ul style="list-style-type: none"> <li>▪ <b>And:</b> Both search conditions must be met for the document to be returned.</li> <li>▪ <b>Or:</b> Either condition must be met for the document to be returned.</li> </ul>

## A.17 Search Parameters Page

Specify the parameters for conditions used in a search. Default values can be set, and parameters can be required or set to read only. The Create Search Parameters page is accessed by clicking **Next** on the [Search Conditions Page](#) or by clicking Parameters on the [Navigation Train](#).

Parameter Name	Prompt Text	Operator Text	Default Value	Picklist	Required	Read Only
Purchase Order(1)	Purchase Order	=		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
↑	Move the parameter up in the list. The ordering in this list corresponds to the presentation the user will see on the Search Form page.
↓	Move the parameter down in the list. The ordering in this list corresponds to the presentation the user will see on the Search Form page.
Parameter Name	Specifies the parameter name.
Prompt Text	Specifies what is listed on the Search Form page to prompt the user.
Edit Operator Properties Icon	Clicking displays the Operator Properties dialog window for making additional operator options available to a user when searching.
Modify Default Value Icon	Displays a dialog window for specifying a default value for the parameter. The value you enter will be of the same data type as the parameter. Defaults for date and text data types also provide the option to select relative date and current logged in user. <ul style="list-style-type: none"> <li>■ <b>Text Value:</b> Value will validate using textual rules.</li> <li>■ <b>Date Value:</b> Value will be validated using regional date settings.</li> <li>■ <b>Number Value:</b> Value will be validated as a whole number.</li> <li>■ <b>Decimal Value:</b> Value will be validated as a number.</li> <li>■ <b>Relative Date:</b> Value will be calculated as the number of days from today and the date value from that day displayed. The value will then be validated as a date.</li> <li>■ <b>Logged in UserID:</b> The current user's userid will be placed into the value and validated as text.</li> </ul>
Picklist	Enable to allow users to choose from defined parameter values.
Required	Enable to require users to enter a parameter when using this search.
Read Only	Enable to prevent a user from modifying a parameter.

## A.18 Search Security Page

Use the Security page to define who has rights to view, modify, delete and grant access to the search being created.

The Search Security page is accessed by clicking **Next** on the [Search Parameters Page](#) or by clicking Security on the [Navigation Train](#).

	Display Name	View	Modify	Delete	Grant Access
	weblogic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	David	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Robert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.
User/Group Icon	Displays a single person for a user and multiple persons for a group.
Display Name	The name of the user or group.
View	Enabled by default. Grants the user or group the right to view and execute this search.
Modify	Enable to grant the user or group the right to modify all aspects of this search except for granting security rights.
Delete	Enable to grant the user or group the right to delete this search.
Grant Access	Enable to grant a user or group the right to grant security rights to others for this search. If this is the only security level granted, the user can modify only the security information for this search.

## A.19 Add Security Member Page

Use the Add Security Member page to add users and groups to an application, search, or input security. Access this page by clicking **Add** on the [Search Security Page](#), the [Application Security Page](#), [Application Document Security Page](#), or by clicking **Applications** on the [Input Security Page](#).

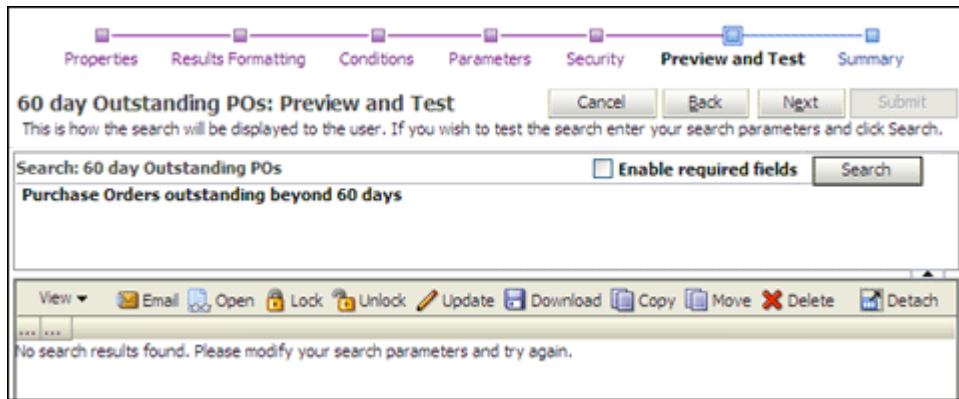
The following table describes the elements available on the page.

Element	Description
Search Menu	Select Search Users to search for users by their login identifier; select Search Groups to search for groups by group name.
Search Field	Enter the name of a user or group to find. Criteria is not case-sensitive. The asterisk (*) can be used as a wildcard. For example, you can enter *group to find UserGroup and AdminGroup, but would need to enter *group* to find AdminGroups. Click Search without entering any criteria to return the entire listing of either users or groups.
Search	Click Search to submit search criteria.
Results Listing	Displays the returned results.
Add	Click Add to close the dialog and return the selected user(s) or group(s) to originating security configuration page.
Cancel	Cancels the procedure and closes the Add Security Member page.

## A.20 Search Preview and Test Page

From this page, you can test the search you just created to ensure it is working and displaying properly before deploying it.

Access the Create Search Preview and Test page by clicking **Next** on the [Search Security Page](#).



The following table describes the elements available on the page.

Element	Description
Enable Required Fields	By default, the search parameters marked as required are not enforced in this search test page so as not to hinder progressing through the search definition process. Enable and provide the required search parameters to more accurately reproduce the Search Form operation.
Search	Runs the test search. Once run, the results are displayed in the lower section as they will display on a search results page. Go back to any previous page to alter any elements of the search that are not producing the desired results. Navigate backwards by clicking the back button, or skipping directly to it using the <a href="#">Navigation Train</a> .
Search Result Toolbar	The Search Results Toolbar is displayed above the search results area and provides options for manipulating returned documents. Functionality is documented in the User's Guide for Oracle IPM and in the help system on a search results page.

## A.21 Search Summary Page

Review the details of the search you just created on the Create Search Summary page. Go back to previous pages to make changes by clicking the Back button or by clicking the name of the page on the [Navigation Train](#).

Access this page by clicking **Next** on the [Search Preview and Test Page](#).



[Properties](#)
[Results Formatting](#)
[Conditions](#)
[Parameters](#)
[Security](#)
[Preview and Test](#)
**Review Settings**

Create Search: Review Settings

Source Application	Description	Department	Version	
Office Docs	Description	Department	Version	

▣ Conditions

**Application: Office Docs**

(	Field	Operator	Value	)	Conjunction
	Description	Begins With	Parameter - Description		Or
	Department	=	Parameter - Accounting		

▣ Parameters

Parameter Name	Prompt Text	Operator Text	Default Value	Picklist	Required	Read Only
Description	Description	Begins With				
Accounting	Department	=		✓		

▣ Security

Type	Security Member	View	Modify	Delete	Grant Access
	ipmadmin	✓	✓	✓	✓

▣ Audit History

Date	Type	User Name

The following table describes the elements available on the page.

Element	Description
Properties Section	Lists the search name and other criteria defined on the <a href="#">Search Properties Page</a> .
Results Formatting Section	Displays the information defined on the <a href="#">Search Results Formatting Page</a> .
Conditions Section	Displays information defined on the <a href="#">Search Conditions Page</a> .
Parameters Section	Displays information defined on the <a href="#">Search Parameters Page</a> .
Security Section	Displays information defined on the <a href="#">Search Security Page</a> .
Audit History Section	Once a search is created, the audit history section displays a list of all actions performed on a search. It is blank on the summary page of a search being created.

## A.22 Application General Properties Page

**Note:** The user creating an application must also have View permission to the repository connection being used.

Applications define a set of common metadata and access to a group of documents. On this page, provide general properties information about the application being created.

Access the Create Application General Properties page by clicking the Create Application icon on the Application panel in the navigator pane.

The following table describes the elements available on the page.

Element	Description
Application Name	Enter a descriptive name for the application. The application name is displayed to users on the Upload Document page and to system administrators when creating inputs and searches. This field is required and must be unique.
Description	Enter a description for the application.
Repository	Oracle I/PM can leverage multiple instances of Oracle Content Server to store documents. This field specifies which Content Server repository instance will contain this application and its documents. The choices for this field are the I/PM repository connections to which the user has access. Once the application is created, the repository cannot be changed. This field is required.
Full-Text Search	Disable to index metadata only. Enable to index metadata and the full-text of any documents with text information. Images of documents do not contain text information, and so cannot be full-text indexed. For example, a Microsoft Word has text that can be indexed, but a TIFF image of a Microsoft Word document does not, and so cannot be indexed.

## A.23 Application Field Definitions Page

Specify the fields and their definitions that will appear in the new application.

Access the Create Application Field Definitions page by clicking **Next** on the [Application General Properties Page](#) or by clicking Field Definitions in the [Navigation Train](#).

The following table describes the elements available on the page.

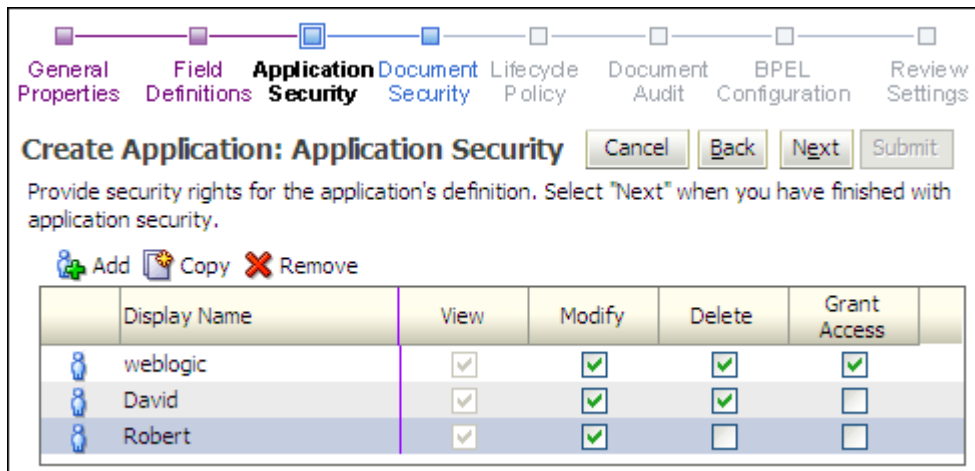
Element	Description
Add	Adds a new field to the application.
Remove	Removes a selected field from the application.
Name	Specifies the name of the field. This name must be unique. There is a restriction that when adding or modifying an application you cannot delete an existing field and re-add it with the same name. If this happens, click <b>Cancel</b> and start again.
Type	Specifies the type of information to be input. Options include: <ul style="list-style-type: none"> <li>■ <b>Text:</b> Fields of this type accept text consisting of all character types. The maximum number of characters to be allowed is defined in the Length element</li> <li>■ <b>Number:</b> Fields of this type accept integer values of up to 10 digits from approximately -2 billion to +2 billion.</li> <li>■ <b>Decimal:</b> Fields of this type accept decimal values up to 15 digits of precision. The scale, or number of decimal places, is specified in the Scale element.</li> <li>■ <b>Date:</b> Fields of this type accept date values.</li> </ul> Note that once a field type has been selected when the field is added, it cannot be changed.
Length	Specifies the maximum number of text characters allowed in the associated text field. The system supports up to 200 characters. This applies only to the Text data type.
Scale	Specifies the number (1-15) of decimal places. This applies only to Decimal data type.
Required	Fields marked required must always have a value. No document can be added to the application without providing a value for this field.

Element	Description
Indexed	Fields marked as Indexed cause the repository to create database level indexes to accelerate searching.
Default Value	Specifies a value to be recommended to the user as a default when uploading a document. Clicking the pencil icon displays a form in which to enter the value. If a default value is to be assigned from a picklist, you must define the picklist first. If you assign a default value from a picklist and then clear the value from the picklist, it also clears the default value.
Picklist	Click the <b>Add Picklist</b> icon to display the Picklist window where you can enter values for the new picklist. Click the <b>Edit Picklist</b> icon to edit an existing list. Click the <b>Remove Picklist</b> icon to remove the picklist.

## A.24 Application Security Page

Specify the users and groups that will be able to view, modify, or delete the application or grant access to others.

Access the Create Application: Application Security page by clicking **Next** on the [Application Field Definitions Page](#) or by clicking on Application Security in the [Navigation Train](#).



The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.
User/Group Icon	Displays a single person for a user and multiple persons for a group.
Display Name	The name of the user or group.
View	Enabled by default. Grants the user or group the right to view and upload into this application.

Element	Description
Modify	Enable to grant the user or group the right to modify all aspects of this application except for granting security rights.
Delete	Enable to grant the user or group the right to delete this application.
Grant Access	Enable to grant a user or group the right to grant security rights to others for this application. If this is the only security level granted, the user can modify only the security information for this application.

## A.25 Application Document Security Page

Application Document Security applies to groups but not users. Select the field in the appropriate column to grant a group that aspect of document security.

Access the Create Application Document Security page by clicking **Next** on the [Application Security Page](#) or by clicking Document Security in the [Navigation Train](#).

	Display Name	View	Write	Delete	Grant Access	Lock Admin	Annotate Standard	Annotate Restricted	Annotate Hidden
	Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Managers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Directors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.
User/Group Icon	Displays a single person for a user and multiple persons for a group.
Display Name	The name of the user or group.
View	Enabled by default. Grants the user or group the right to view documents in this application.
Modify	Enable to grant the user or group the right to modify all aspects of documents in this application except for granting security rights.
Delete	Enable to grant the user or group the right to delete documents in this application.

Element	Description
Lock Admin	Grants the selected group the right to unlock documents locked by users other than themselves within this application.
Annotate Standard	Grants a group the right to create and manipulate annotations classified as standard by the annotator
Annotate Restricted	Grants a group the right to create and manipulate annotations classified as restricted by the annotator.
Annotate Hidden	Grants a group the right to create and manipulate annotations classified as hidden by the annotator.

## A.26 Application Storage Policy Page

On this page, specify the location of storage for the documents in this application.

**WARNING:** Changing the Storage Policy in an existing application affects future documents only. Existing documents maintain the Storage Policy that was in place at the time they were uploaded.

Access the Create Application Storage Policy page by clicking **Next** on the [Application Document Security Page](#) or by clicking Storage Policy in the [Navigation Train](#).

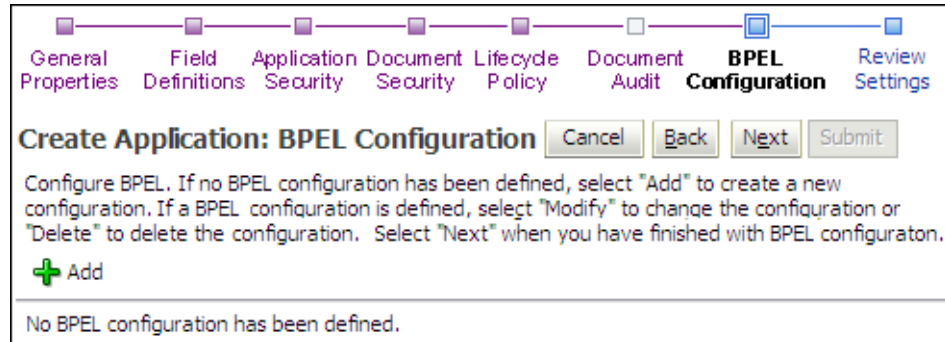
The following table describes the elements available on the page.

Element	Description
Document Storage Volume	Specify where documents will be stored. This may be a file system or a database, depending on how the Content Server repository is configured. Note that volume status is not indicated here.
Supporting Content Storage Volume	Specify where annotations and supporting content will be stored. This may be a file system or a database, depending on how the Content Server repository is configured. Note that volume status is not indicated here.

## A.27 Application BPEL Configuration Page

BPEL enables your organization to automate its business processes by orchestrating services within the process flow. Click add to create a BPEL process to define an integration to an existing BPEL process. A new instance of this process will be created each time a document is created within this application.

Access the Create Application BPEL (Business Process Execution Language) Configuration General Properties page by clicking **Next** on the [Application Storage Policy Page](#).



The following table describes the elements available on the page.

Element	Description
Add	Click to add a new BPEL configuration.
Modify	Click to modify an existing BPEL configuration.
Remove	Remove the configuration from the application.

## A.28 BPEL Server Properties Page

On this page select the BPEL connection to the BPEL server hosting the desired process. Connection, User name, and Password are required values.

Access this page by clicking Add or Modify on the Application BPEL Configuration Page. Access the Create Application BPEL Server Properties page by clicking **Next** on the [Application BPEL Configuration Page](#) or clicking Modify on an existing Application BPEL Configuration Server Properties page.



The following table describes the elements available on the page.

Element	Description
Connection	Select the BPEL connection to the BPEL server hosting the desired process. This is a required value.

## A.29 BPEL Component Properties Page

Select from the Composite, Service, and Operation fields to identify the BPEL process you want to initiate.

Access the Create Application BPEL Component Properties page by clicking **Next** on the [Application BPEL Configuration Page](#) or clicking **Modify** on an existing Application BPEL Configuration Component Properties page.

The screenshot shows a navigation breadcrumb at the top: BPEL Configuration > General Properties > **Component Properties** > Payload Properties > BPEL Configuration. Below the breadcrumb are four buttons: Cancel, Back, Next, and Finished. The main heading is "Invoices: BPEL Configuration" followed by a sub-heading "Component Properties". The instructions state: "Configure a BPEL component that will be invoked when new documents are added to the application. Select 'Next' when you have finished with BPEL component configuration." The form contains three required fields, each with an asterisk and a dropdown menu:
 

- \* Composite: Payment (1.2)
- \* Service: payment\_entry\_ep
- \* Operation: process

The following table describes the elements available on the page.

Element	Description
Composite	Select the name and version of a deployed BPEL composite. This is a required value.
Service	Select the name of a service associated with the selected composite. This is a required value.
Operation	Select the name of an operation associated with the selected service. This is a required value.

### A.30 BPEL Payload Properties Page

The BPEL Payload Properties page defines which application field values will be transferred to the new process instance when it is created. Access the Create Application BPEL Payload Properties page by clicking **Next** on the Create Application Component Properties page or clicking **Modify** on an existing Application BPEL Configuration Payload Properties page. When you have completed the changes, click **Finished**.




**Invoices: BPEL Configuration** Cancel Back Next Finish

Configure payload values when a BPEL component is invoked. Select "Finish" when you have finished with payload configuration and return to the application definition.

**Payload Properties**

\* Indicates a required value

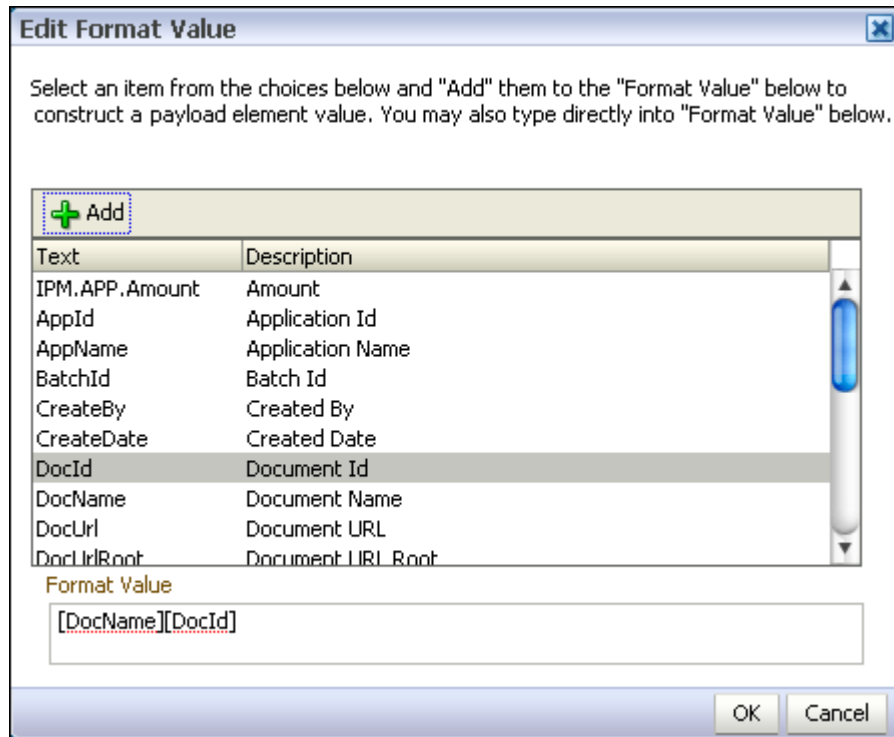
Payload Element	Type	Mapped Value
*process	complex	
*InvoiceId	int	Format Value 
*ReceivedDate	date	Receive Date
*PurchaseOrderId	int	Purchase Order
*Amount	decimal	Amount
*DocumentURL	string	Document URL
*VendorName	string	Vendor

The following table describes the elements available on the page.

Element	Description
Payload Element	Select the application field to provide a value for the BPEL field.
Type	This column lists the data type for the BPEL process field. This data type is used to limit the list of possible application fields to compatible data types.
Mapped Value, Function	Select the application field to provide a value for the BPEL field. Available fields are dependent on the application. The Format Value option allows a user to define a string expression. This expression can include a constant value (1.23) or a function (AppId) or a combination of both. Selecting the Format Value option displays an icon to launch the <a href="#">Edit Format Value Page</a> to facilitate creating custom URLs or concatenation of values.

### A.30.1 Edit Format Value Page

This page is accessed from the [BPEL Payload Properties Page](#). Selecting the **Format Value** option from the Mapped Value column displays an icon which when clicked launches the Edit Format Value page. This page enables you to construct a value from parts of text and application fields. For example, you would use this page to construct custom URLs or to concatenate multiple values together into a single value.



## A.31 Application Review Settings Page

The Create Application Review Settings page allows you to check the settings defined in the application prior to creating the application. Access the Create Application Review Settings page by clicking **Next** on the Create Application BPEL Payload Properties page. To make any changes to the settings prior to submitting them, click **Back** or the appropriate link in the navigation train to return to the necessary page. When you are satisfied with the Application settings, click **Submit**.

[General Properties](#)
[Field Definitions](#)
[Application Security](#)
[Document Security](#)
[Lifecycle Policy](#)
[BPEL Configuration](#)
[Review Settings](#)

**Invoices: Review Settings**

Review the following application settings. Select "Submit" if ok, or select "Back" to make changes. The "Submit" button is only enabled when there are changes.

**General Properties**

Application Name: Invoices  
Description: Inbound Invoice Documents to be paid  
Repository: UCM 11g  
Document Upload Option: Metadata only search, version documents

**Field Definitions**

Type	Name	Length	Scale	Required	Indexed	Default Value	Picklist
123	Invoice Number				✓		
	Receive Date				✓		
Abc	Vendor	80			✓		
8.9	Amount		2		✓		
123	Purchase Order				✓		

**Application Security**

Type	Security Member	View	Modify	Delete	Grant Access
	Clerk	✓			
	Yoda	✓	✓	✓	✓
	Administrators	✓	✓	✓	✓
	Manager	✓	✓	✓	✓

**Document Security**

Type	Security Member	View	Write	Delete	Grant Access	Lock Admin	Annotate Standard	Annotate Restricted	Annotate Hidden
	Administrators	✓	✓	✓	✓	✓	✓	✓	✓
	Manager	✓							
	Clerk	✓	✓	✓	✓	✓	✓	✓	✓
	Chumps	✓	✓	✓	✓	✓	✓	✓	✓

**Lifecycle Policy**

**Document Storage**  
Volume: File default

**Supporting Content Storage**  
Volume: File default

**BPEL Configuration**  
BPEL injection enabled.

**Server Properties**  
Connection: 13:BPEL 11g

**Component Properties**  
Composite: InvoicePayment!1.7  
Service: payment\_entry\_ep  
Operation: process

**Payload Properties**

Payload Id	Mapped Value
process.Amount	FieldValue Amount
process.PurchaseOrderId	FieldValue Purchase Order
process.DocumentURL	DocUrl
process.VendorName	FieldValue Vendor
process.InvoiceId	FieldValue Invoice Number
process.ReceivedDate	FieldValue Receive Date

## A.32 Input Basic Information Page

An input is a configuration that maps an input file to an application when documents are uploaded in the background by the Input Agent.

Access the Create Input Basic Information page by clicking the Create Input icon on the Manage Inputs panel of the navigation pane.

The following table describes the elements available on the page.

Element	Description
Name	The name of the input.
Description	A brief description of the input.
Online	Select this field when you want the input agent to start its search for work. You can leave this field unselected until after you test the file.
Auto-detect input file character set	When enabled, the input file character set of the application is automatically detected. When this field is not selected, you can manually specify the input file character set and override the default character set of the application used in the input.
Sample File	A path to a sample text file that illustrates the content of an input for this input definition. <a href="#">Input Identify and Parse File Parameters Page</a> and will be used when mapping columns in the file to application fields.
Upload	Click to upload a sample file on a local or shared drive to the samples directory on the server.
Browse	Click to select from a list of sample files in the samples directory of the server.

### A.33 Input Identify and Parse File Parameters Page

Specify the input mask, delimiter used to separate data, and the application to which the input file is being mapped. The contents of the sample input file is displayed in the Sample Data section of the page for reference.

The input mask supports regular expressions in addition to the \* or ? characters for masks. For example, specifying an input mask of `abc* | * .def` pulls all files starting with `abc` or ending in `.def`. Specifying an input mask of `[abc] try .1st` pulls files `atry .1st`, `btry .1st`, and `ctry .1st`, but not `dtry .1st`.

---

**WARNING:** Each input's mask should resolve to a unique set of input files that do not overlap the masks of other inputs. Input Agent only processes an input file for one input and will not restage a file to be processed again for a different input definition. The order in which inputs are processed is random so it is unknown as to which input will pick up a shared input file.

---

Access the Create Input Review Sample File page by clicking **Next** on the [Input Basic Information Page](#).

The following table describes the elements available on the page.

Element	Description
Input Mask	This is the filter that the input agent uses to locate files for the input.
Delimiter	Specify the character that indicates the boundary between independent regions of data.
Application	Select the application to be mapped to the input file.
Sample Data	Displays contents of uploaded sample file.

## A.34 Input Field Mapping Page

This page facilitates mapping of the columns of data from input files into the correct fields of the target application. Access the Create Input Field Mapping page by clicking **Next** on the [Input Identify and Parse File Parameters Page](#).

Application Fields	Input Column	Sample Data	Use Application Default	Date Format
File Path	<input checked="" type="checkbox"/> Column 1			+ ✎ ✕
File Language	<input checked="" type="checkbox"/> [ ]			+ ✎ ✕
File Character Set	<input checked="" type="checkbox"/> [ ]			+ ✎ ✕
Amount	<input checked="" type="checkbox"/> Column 2	scratch		+ ✎ ✕
Vendor	<input checked="" type="checkbox"/> Column 3	tmjones		+ ✎ ✕
Purchase Order	<input checked="" type="checkbox"/> Column 4	Oracle		+ ✎ ✕
Receive Date	<input checked="" type="checkbox"/> Column 5	Middleware		+ ✎ ✕
Invoice Number	<input checked="" type="checkbox"/> Column 6	user_projects		+ ✎ ✕

The following table describes the elements available on the page.

Element	Description
Application Fields column	List of field names that are specific to the selected application.
Input Column	A green check mark in the radio button indicates that the mapping is good. A red X indicates that the mapping will not work and you must specify a different column. The picklist lets you choose the column in the input file that will be mapped to the specified data in the application.
Sample Data	After you select a column, the corresponding data from the sample input file will be displayed in the Sample Data column. Click the Show Previous Line or Show Next Line icon to see more data from the sample file.
Use Application Default	Enable to use the default value specified in the application if this value is blank in the input file. The check box is only displayed if the application defines a default value.
Date Format	Click the Add or Edit icons to access the date mask editing dialog. This dialog allows you to create a custom date mask for deciphering nonstandard date values in the input file. Click the Delete icon to remove the custom date mask.

### A.34.1 Define Date Format Page

The Define Date Format Page is displayed when clicking the **Add a Date Format** or **Edit a Date Format** icon in the Date Format column of the [Input Field Mapping Page](#). Use the Define Date Format page to specify how the date is displayed. If no date format is specified, the default is to the format of the input agent server locale.

**Define Date Format**

**+ Add**

**Format Values**

- Era
- Year (4 digit)
- Year (2 digit)
- Month (number in year)
- Month (abbreviated month name)
- Month (full month name)
- Day**
- Hour (24 hour)
- Hour (12 hour)
- Minute
- Second
- / separator
- separator
- \_ separator
- : separator
- . separator
- space

**Format Value**

MMM - dd

**Sample Date**

Dec - 05

**OK**

The following table describes the elements available on the page.

Element	Description
Add	Click to add the selected format value to the to the Format Value field. Once added, an example is displayed in the Sample Date section.

Element	Description
Format Values	<p>Select format values to add to the Format Value field to determine how a date will be displayed. Only one value can be selected at a time. Values are displayed in the order they are added to the Format Value field. Format value options are:</p> <ul style="list-style-type: none"> <li>■ <b>Era:</b> GG - Sample: AD</li> <li>■ <b>Year (4 digit):</b> yyyy - Sample: 2010</li> <li>■ <b>Year (2 digit):</b> yy - Sample: 10</li> <li>■ <b>Month (number in year):</b> MM - Sample: 01</li> <li>■ <b>Month (abbreviated month name):</b> MMM - Sample: Jan</li> <li>■ <b>Month (full month name):</b> MMMM - Sample: January</li> <li>■ <b>Day:</b> dd - Sample: 01</li> <li>■ <b>Hour (24 hour):</b> HH - Sample: 17</li> <li>■ <b>Hour (12 hour):</b> hh - Sample: 05</li> <li>■ <b>Minute:</b> mm - Sample: 16</li> <li>■ <b>Second:</b> ss - Sample: 59</li> <li>■ <b>/ separator:</b> Separates values with a forward slash</li> <li>■ <b>- separator:</b> Separates values with a dash</li> <li>■ <b>_ separator:</b> Separates values with an underscore</li> <li>■ <b>: separator:</b> Separates values with a colon</li> <li>■ <b>. separator:</b> Separates values with a period</li> <li>■ <b>space:</b> Adds a space to the string</li> </ul> <p>For example, if the Format Value field were populated with <i>yyMMMdd - HH:mm:ss</i>, the Sample Date would display <i>10Jan01 - 15:16:59</i> for a date and time of January 10th, 2010 at 5:16 and 59 seconds PM, based on the following Format Values being added in the following order:</p> <ol style="list-style-type: none"> <li>1. Year (2 digit)</li> <li>2. Month (abbreviated month name)</li> <li>3. Day</li> <li>4. space</li> <li>5. - separator</li> <li>6. space</li> <li>7. Hour (24 hour)</li> <li>8. : separator</li> <li>9. Minute</li> <li>10. : separator</li> <li>11. Second</li> </ol>

## A.35 Input Security Page

The Create Input: Security page is accessed by clicking **Next** on the [Input Field Mapping Page](#).



Display Name	View	Modify	Delete	Grant Access
weblogic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.

## A.36 Input Review Settings Page

The Create Input Commit Definition page allows you to check the settings defined in the input wizard prior to creating the input. To make any changes to the settings prior to submitting them, click **Back** or the appropriate link in the navigation train to return to the desired page. When you are satisfied with the input settings, click **Submit**.

The Create Input Commit Definition page is accessed by clicking **Next** on the [Input Security Page](#).

Basic Information | Edit Input File Settings | Map File to Application | Security | **Review Settings**

**Create Input: Input Summary** Cancel Back Next Submit

The following is a summary of the information you entered. Please review this content and click commit to create the input.



**Basic Information**

Name: Invoices  
 Description: Shipping Invoices  
 Priority: 0  
 Online:   
 Auto-detect input file character set:

**Field Mapping**

Application: Invoices  
 Input Mapping:  
 File Path: Column 1  
 File Language:  
 File Character Set:  
 Amount: Column 2  
 Vendor: Column 3  
 Purchase Order: Column 4  
 Receive Date: Column 5  
 Invoice Number: Column 6  
 Input Mask: Invoice20090317140639756000.txt  
 Delimiter: /

**Security**

Security Member	View	Modify	Delete	Grant Access
 weblogic	✓	✓	✓	✓
 Administrators	✓	✓	✓	

### A.37 Content Server Connection Basic Information Page

Create and modify connections to a Content Server repository server by expanding the Manage Connections panel in the [Navigator Pane](#). Click the **Create New Connection** icon or click an existing connection and click **Modify** to display the Connection Basic Information page.

The following table describes the elements available on the page.

Element	Description
Name	A name for the repository to which you are connecting.
Description	A brief description of the connection.
Connection Type	Identifies the type of connection. The type of connection cannot be changed once it is defined.

## A.38 Content Server Connection Content Server Settings Page

Specify the details of the Content Server repository to connect to on the Content Server Settings page. It is accessed by clicking **Next** on the [Content Server Connection Basic Information Page](#) when creating a new connection, or directly using the navigation train on any repository connection page for an existing connection.

The following table describes the elements available on the page.

Element	Description
Repository Proxy	Name of the repository proxy. The repository proxy is a user created in Content Server when Oracle I/PM is installed. The proxy is given rights to Content Server that allows it to fulfill requests to Content Server on behalf of I/PM users who may not have the necessary rights in Content Server to perform the required tasks. For example, a user may have the rights in I/PM to create an application and add metadata fields, but may not have the rights in Content Server to create metadata fields to support the application. When the application is created, the request to Content Server to create the necessary metadata fields is made by the repository proxy. By default, the repository proxy name is fmwadmin. This field is required.
SSL	Enable connection using Secure Socket Layer (SSL). Additional steps must be taken to configure SSL on Content Server and ensure proper credentials. For detailed information, see the full <i>Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management</i> .
Machine Name	Specifies the host name or names used for the connection. If the BPEL server is a single instance, it is the name or IP of the server. If the server is operating within a cluster, this parameter value can be a comma-separated list of machine names or IP addresses of servers in the cluster, or it can be the cluster name for the cluster. The default and most common value is "localhost" which connects I/PM to the Content Server sharing the computer.
Server Port	Specifies the Content Server's remote API (RIDC) connection port. If the SSL option is checked, then the port provided must be the SSL listening port for the server.
Secondaries	In clustered configurations it is necessary to provide the connection information to each of the Content Servers in the cluster. The Machine Name and Server Port values are the same as described above.

## A.39 Content Server Connection Security Page

Specify the connection definition security on Connection security page. It is accessed by clicking **Next** on the [Content Server Connection Content Server Settings Page](#) when creating a new connection, or directly using the navigation train on any connection page for an existing connection.

Basic Information Content Server Settings **Security** Review Settings

UCM 11g: Connection Security Cancel Back Next Submit

Provide security rights for the connection's definition. Select "Next" when you have finished with connection security.

Type	Security Member	View	Modify	Delete	Grant Access
	Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	ipmadmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Clerk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.
User/Group Icon	Displays a single person for a user and multiple persons for a group.
Display Name	The name of the user or group.
View	Enabled by default. Grants the user or group the right to view this connection.
Modify	Enable to grant the user or group the right to modify all aspects of this connection except for granting security rights.
Delete	Enable to grant the user or group the right to delete this connection.
Grant Access	Enable to grant a user or group the right to grant security rights to others for this connection. If this is the only security level granted, the user can modify only the security information for this connection.

## A.40 Content Server Connection Review Settings Page

Review connection settings prior to submitting the connection on the Review Settings page. Access the Review Settings by clicking **Next** on the [Content Server Connection Security Page](#) when creating a new connection, or directly in the navigation train on any connection page when modifying an existing connection.

If settings need to be changed, navigate to the connection page to make the changes either by clicking **Back** or by clicking the needed page in the navigation page. Once you are satisfied with your settings, click **Submit**.

Basic Information
Content Server Settings
Security
Review Settings

**Server: Review Settings**               

Review the following connection settings. Select "Submit" if ok, or select "Back" to make changes. The "Submit" button is only enabled when there are changes.

**Basic Information**

Name: Server

Description:

Connection Type: Content Server Repository

**Connection Settings**





Repository Proxy: fmwadmin

SSL: false

Primary	
Machine	Server Port
tcmcluster-4.us.oracle.com	4444

Secondaries	
Machine	Server Port
No Machines Defined	

**Security**

Type	Security Member	View	Modify	Delete	Grant Access
	Manager	✓			
	ipmadmin	✓	✓	✓	✓
	Clerk	✓			
	Yoda	✓			✓

## A.41 BPEL Connection Basic Information Page

Create and modify connections to a BPEL server by expanding the Manage Connections panel in the [Navigator Pane](#). Click the **Create New Connection** icon or click an existing connection and click **Modify** to display the BPEL Connection Basic Information page.

The following table describes the elements available on the page.

Element	Description
Name	Provide a unique name for this connection.
Description	A brief description of the connection.
Connection Type	Identifies the type of connection.

## A.42 BPEL Connection Settings Page

Specify the details of the BPEL server to connect to on the BPEL Connection Settings page. It is accessed by clicking **Next** on the [BPEL Connection Basic Information Page](#) when creating a new connection, or directly using the navigation train on any Content Server connection page for an existing BPEL connection.

The following table describes the elements available on the page.

Element	Description
Provider	<p>Specifies the host name or names used for the connection. If the BPEL server is a single instance, it is the name or IP of the BPEL machine. If the BPEL server is operating within a cluster, this parameter value can be a comma-separated list of machine names or IP addresses of servers in the cluster, or it can be the cluster name for the cluster.</p> <p>If multiple machine names are provided in a comma-separated list, the machines must <i>all</i> use the same port (the value supplied by the <code>port</code> parameter). If the BPEL managed servers in the cluster need to be defined with different ports, then the cluster-name configuration must be used.</p> <p>When a cluster name is used, the name must be defined in DNS to resolve to the multiple machines within the cluster. Neither Oracle I/PM nor BPEL defines this behavior. Rather, it is defined by the Oracle WebLogic Server support for JNDI in a cluster.</p>
Port	Specifies the configured listening port for the target BPEL server. If the SSL option is checked, then the port provided must be the SSL listening port for the server.
SSL	Enable connection using Secure Socket Layer (SSL).
Credential Alias	<p>Provides the alias for username and password credentials encrypted in the credential store. These credentials are used when making the remote connection to the BPEL server and must reference a username and password with appropriate permissions in the BPEL system, not I/PM.</p> <p>This credential must be created in the credential store before the BPEL connection configuration can be completed. A credential can be created in the credential store in one of two ways: through Fusion Middleware Control or through WLST.</p>
Test Connection	Click to test if connection settings are configured correctly. A dialog box is displayed indicating whether or not the connection test was successful. If successful, the available composites deployed on the BPEL server are also displayed in a list at the bottom.

## A.43 BPEL Connection Security Page

Specify the connection definition security on Connection security page. It is accessed by clicking **Next** on the [BPEL Connection Settings Page](#) when creating a new connection, or directly using the navigation train on any connection page for an existing connection.



Basic Information Content Server Settings **Security** Review Settings

UCM 11g: Connection Security

Provide security rights for the connection's definition. Select "Next" when you have finished with connection security.

Type	Security Member	View	Modify	Delete	Grant Access
	Manager	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	ipmadmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Clerk	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes the elements available on the page.

Element	Description
Add	Displays the <a href="#">Add Security Member Page</a> from which you can search for and select users or predefined security groups.
Copy	Selecting a user or group from the existing list and clicking <b>Copy</b> displays the <a href="#">Add Security Member Page</a> and copies the permissions of the selected user or group to the next user or group added.
Remove	Removes the selected user or group from the list.
User/Group Icon	Displays a single person for a user and multiple persons for a group.
Display Name	The name of the user or group.
View	Enabled by default. Grants the user or group the right to view this connection.
Modify	Enable to grant the user or group the right to modify all aspects of this connection except for granting security rights.
Delete	Enable to grant the user or group the right to delete this connection.
Grant Access	Enable to grant a user or group the right to grant security rights to others for this connection. If this is the only security level granted, the user can modify only the security information for this connection.

## A.44 BPEL Connection Review Settings Page

Review connection settings prior to submitting the connection on the Review Settings page. Access the Review Settings by clicking **Next** on the [BPEL Connection Security Page](#) when creating a new connection, or directly in the navigation train on any BPEL connection page when modifying an existing connection.

If settings need to be changed, navigate to the connection page to make the changes either by clicking **Back** or by clicking the needed page in the navigation page. Once you are satisfied with your settings, click **Submit**.

Basic Information BPEL Settings Security **Review Settings**

**tcmcluster-1 BPEL: Review Settings**

Review the following connection settings. Select "Submit" if ok, or select "Back" to make changes. The "Submit" button is only enabled when there are changes.

**Basic Information**

Name tcmcluster-1 BPEL  
Description  
Connection Type BPEL Connection

**Connection Settings**

Credential Alias basic.credential  
Machine tcmcluster-1.us.oracle.com  
Port 8001  
SSL false

**Security**

Type	Security Member	View	Modify	Delete	Grant Access
	ipmadmin	✓	✓	✓	✓
	Administrators	✓	✓	✓	✓

## A.45 Manage Security

Create and modify the top level security settings for applications, inputs, searches, and connections by selecting the appropriate category in the Manage Security panel in the navigator pane.

Access the Manage Security pages by clicking the expand icon on the Manage Security panel in the navigator pane.

**Inputs Security**

Define the Input create and administrative rights.

Add Copy Remove

Type	Security Member	Create	Administrator
	Yoda	✓	✓
	ipmadmin	✓	✓

The following table describes the elements available on the page.

Element	Description
Create	Select to assign Create permission to a user which allows the user to create an application, input, search, or connection.
Administrator	Select to assign a user permission to view, create, modify, and delete an application, input, search, or connection.

---

---

# Index

## A

---

- administrative account, 1-3
  - default, 1-3
  - password, 1-3
- advanced viewer
  - default, 3-11
- annotation
  - annotate hidden, 2-9
  - annotate restricted, 2-8
  - annotate standard, 2-8
- Annotations
  - Redaction
    - shifting problem, 10-6
- Application, 1-2
  - application security, 4-5
  - BPEL configuration, 8-2
  - creating, 3-8, 4-1, 4-2
  - defining application fields, 4-4
  - document security, 4-5
  - general properties, 4-3
  - permission, 2-4
- Application server, 1-8
- asctl, 1-8

## B

---

- Batch uploading, 5-1
- BPEL
  - creating process, 8-7
  - WLS
    - thread settings, 5-8, 8-6
- Business logic, 1-6

## C

---

- Configuration
  - overview, 3-1
  - post-installation, 3-2
- configuration
  - repository options, 3-2
- Connections
  - configuration of, 7-1
- Content Server (see Oracle Content Server), 1-8
- Content Server file store provider, 3-3
- ContentTracker, 3-4

## D

---

- Document
  - indexing, 4-2

## E

---

- Enterprise Manager
  - System MBean Browser, 3-14
- Exception, 10-7

## F

---

- File size limits, 3-9, A-5
- Font
  - errors, 10-4
- Fonts
  - GDFontPath MBean, 3-14
  - TrueType, 3-14
- fonts
  - setting variables, 3-14
  - TTF font files, 3-10
- full, 10-3
- Fullness, 3-2
- fullness, 10-3

## G

---

- GDFontPath MBean, 3-14

## H

---

- Help
  - troubleshooting, 10-1

## I

---

- images
  - quality, 3-11
  - TIFF
    - compression algorithm, 3-11
- Imaging and Process Management
  - architecture, 1-4
  - business logic, 1-6
- Indexing, 4-2
- Input agent, 5-1
  - error files, 5-8

- input file mask, 5-2
- permissions, 5-2
- processing order, 5-6
- troubleshooting, 10-5

Input definition

- creating, 5-4

Input file

- commands
  - Locale, 5-3
  - New, 5-4
- entries error, 10-5, 10-6
- example, 5-2
- troubleshooting, 10-5

Input file mask

- warning, 5-2

## J

---

- Java API, 1-5
- Java Management Beans (see MBeans), 3-9
- JMX (see MBeans), 3-9
- JOC IdleTime, 3-10

## L

---

Logging

- levels, 10-7

logging

- MBean, 3-11

## M

---

MBean

- Enterprise Manager MBean browser, 3-14

MBeans

- AgentUser, 3-10
- and WLST, 3-12
- CacheAgeLimit, 3-10
- CacheLocation, 3-10
- CheckInterval, 3-10
- command line configuration, 3-9
- DefaultColorSet, 3-10
- DefaultSecurityGroup, 3-10
- GDFontPath, 3-10
- InputDirectories, 3-11
- JpegImageQuality, 3-11
- list of, 3-9
- LogDetailedTimes, 3-11
- MaxSearchResults, 3-11
- SampleDirectory, 3-11
- TiffCompressionType, 3-11
- UseAdvancedAsDefaultViewerMode, 3-11

Middleware Administration Server, 1-8

## O

---

- OC4J, 1-8
- Oracle Content Server, 1-8, 10-3
  - fullness, 3-2
  - optional components, 3-4
  - repository capacity, 3-2, 10-3

- Oracle Web Services Manager (see OWSM), 7-4, 8-6
- OracleTextSearch, 3-4
- Outside In Technology, 4-2
- OWSM
  - credential, 7-4, 8-6

## P

---

page cache, 3-10

Permission

- application, 2-4

permission

- annotation
  - annotate hidden, 2-9
  - annotate restricted, 2-8
  - annotate standard, 2-8
- document access
  - create, 2-8
  - delete, 2-8
  - grant access, 2-8
  - lock, 2-8
  - view, 2-8

Process flow

- BPEL, 8-1

## R

---

Redaction

- shifting problem, 10-6

Repository

- configuration, 7-1
- Content Server file store provider, 3-3
- fullness, 3-2

repository

- fullness, 10-3

Repository capacity, 3-2

repository capacity, 10-3

## S

---

Security

- login, 2-1
- system permissions, 2-1

security

- MBean
  - DefaultSecurityGroup, 3-10

Skin

- default, 3-10

Storage, 3-1

## T

---

Thread settings, 5-8, 8-6

Transactions

- BPEL, 8-1

Troubleshooting, 10-1

- decimal field error, 10-2
- font errors, 10-4
- input agent, 10-5
- input file, 10-5
- input file entries errors, 10-5, 10-6

- I/PM and windows server prerequisites, 10-3
- logging of ImagingException
  - Exceptions
    - logging**, 10-7
  - nested stack errors, 10-7
  - NULL number fields, 10-3
  - repository capacity errors, 10-3
  - shifting redaction annotations, 10-6
  - UI slowdown, 10-2
- TrueType fonts, 3-14

## **U**

---

- Upload file size limit, 3-9, A-5
- Uploading
  - batch, 5-1

## **V**

---

- viewer
  - advanced
    - MBean, 3-11
  - basic
    - MBean, 3-11

## **W**

---

- Web services
  - BPEL, 8-1
  - Java API, 1-5
- WebCenter Suite, 1-8
- Weblogic Server Scripting Tool (see WLST), 3-12
- WLST
  - and MBeans, 3-12

