



# BEA WebLogic Integration™

## Managing WebLogic Integration Solutions

Version 8.1  
July 2003

# Copyright

Copyright © 2003 BEA Systems, Inc. All Rights Reserved.

## Restricted Rights Legend

This software and documentation is subject to and made available only pursuant to the terms of the BEA Systems License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the software except as specifically allowed in the agreement. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from BEA Systems, Inc.

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the BEA Systems License Agreement and in subparagraph (c)(1) of the Commercial Computer Software-Restricted Rights Clause at FAR 52.227-19; subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, subparagraph (d) of the Commercial Computer Software--Licensing clause at NASA FAR supplement 16-52.227-86; or their equivalent.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA Systems DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

## Trademarks or Service Marks

BEA, Jolt, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Liquid Data for WebLogic, BEA Manager, BEA WebLogic Commerce Server, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Personalization Server, BEA WebLogic Platform, BEA WebLogic Portal, BEA WebLogic Server, BEA WebLogic Workshop and How Business Becomes E-Business are trademarks of BEA Systems, Inc.

All other trademarks are the property of their respective companies.

# Contents

## About This Document

What You Need to Know . . . . .	xiii
dev2dev Product Documentation Web Site . . . . .	xiii
How to Print the Document . . . . .	xiii
Contact Us! . . . . .	xiii
Documentation Conventions . . . . .	xiv

## Introducing the WebLogic Integration Administration Console

Starting the WebLogic Integration Administration Console . . . . .	1-5
--	-----

## Processes Configuration

About Process Configuration . . . . .	2-2
Overview of the Process Configuration Module . . . . .	2-7
Listing and Locating Process Types . . . . .	2-10
Listing and Locating Dynamic Controls . . . . .	2-11
Viewing and Changing Process Details . . . . .	2-11
Viewing an Interactive or Printable Process Type Graph . . . . .	2-16
Managing Process Versions . . . . .	2-18
Adding or Changing Dynamic Client Callback Selectors . . . . .	2-19
Updating Security Policies . . . . .	2-21
Adding or Changing Dynamic Control Selectors . . . . .	2-22
Defining Process Control Properties for a Selector . . . . .	2-23
Defining Service Broker Control Properties for a Selector . . . . .	2-24

Deleting Dynamic Control Selectors . . . . .	2-25
--	------

## Process Instance Monitoring

Overview of the Process Instance Monitoring Module . . . . .	3-2
Browser Requirements for the Interactive Graph . . . . .	3-4
Viewing Instance Statistics by Process Type . . . . .	3-5
Viewing System Health Statistics . . . . .	3-5
Listing and Locating Process Instances . . . . .	3-6
Constructing an Advanced Search . . . . .	3-8
Viewing Process Instance Details . . . . .	3-9
Viewing an Interactive or Printable Process Instance Graph . . . . .	3-12
Suspending, Resuming, Terminating, or Unfreezing Process Instances . . . . .	3-14

## Message Broker

About Message Broker Channels . . . . .	4-2
Overview of the Message Broker Module . . . . .	4-3
Listing and Locating Channels . . . . .	4-4
Viewing Channel Details and Subscriptions . . . . .	4-5
Setting Channel Security Policies . . . . .	4-6
Viewing and Resetting Message Counts . . . . .	4-7

## Event Generators

About the Event Generators . . . . .	5-2
Overview of the Event Generator Module . . . . .	5-4
Creating and Deploying Event Generators . . . . .	5-8
Defining Channel Rules for a File Event Generator . . . . .	5-10
Defining Channel Rules for an Email Event Generator . . . . .	5-12
Defining Channel Rules for a JMS Event Generator . . . . .	5-15
Defining Channel Rules for a Timer Event Generator . . . . .	5-16

Listing and Locating Event Generators . . . . .	5-17
Viewing and Updating Event Generator Channel Rules . . . . .	5-18
Suspending and Resuming Event Generators . . . . .	5-19
Resetting the Counters . . . . .	5-20
Deleting Channel Rules . . . . .	5-21
Deleting Event Generators . . . . .	5-21

## Worklist Administration

Overview of the Worklist Administration Module . . . . .	6-2
Listing and Locating Worklist Tasks . . . . .	6-4
Listing and Locating Substitute Routing Rules . . . . .	6-5
Constructing a Custom Query for Task Instances . . . . .	6-6
Viewing and Changing Task Details . . . . .	6-8
Updating Task State or Deleting Tasks . . . . .	6-11
Updating Task Comment, Owner, or Due Dates from the Summary Page . . . . .	6-13
Adding a Substitute Routing Rule . . . . .	6-15
Changing a Substitute Routing Rule . . . . .	6-16
Deleting a Substitute Routing Rule . . . . .	6-17

## Application Integration

About Application Integration Monitoring and Configuration . . . . .	7-3
Overview of the Application Integration Module . . . . .	7-6
Listing and Locating Application Views . . . . .	7-11
Listing and Locating Adapter Instances. . . . .	7-12
Viewing Application View Instance Statistics. . . . .	7-13
Viewing Adapter Instance Statistics . . . . .	7-14
Viewing Dependent Application Views of Adapter Instances . . . . .	7-15
Viewing and Changing Application View Details. . . . .	7-16

Viewing and Changing Adapter Instance Details . . . . .	7-20
Viewing and Changing Event Connection Properties . . . . .	7-23
Viewing and Changing Service Connection Properties. . . . .	7-24
Viewing and Changing Connection Pool Size Parameters . . . . .	7-24
Viewing and Changing Application View Auto Suspend Settings . . . . .	7-26
Viewing and Changing Environment Variable Values for an Application View . . . . .	7-27
Viewing and Changing WebLogic Server to EIS Principal Mappings . . . . .	7-28
Changing Event Connections for an Application View . . . . .	7-29
Changing Service Connections for an Application View . . . . .	7-30
Changing Event Generation Targets . . . . .	7-31
Changing Application View Container-Managed Sign-On Settings. . . . .	7-33
Updating Security Policies . . . . .	7-34
Suspending or Resuming an Application View or Adapter Instance . . . . .	7-35
Redeploying an Adapter Instance . . . . .	7-36
Resetting the Counters. . . . .	7-37

## Trading Partner Management

About Trading Partner Management . . . . .	8-3
Overview of the Trading Partner Management Module . . . . .	8-4
Configuring Trading Partner Management . . . . .	8-9
Adding Trading Partner Profiles . . . . .	8-13
Adding Certificates to a Trading Partner. . . . .	8-15
Adding Protocol Bindings to a Trading Partner . . . . .	8-19
Adding a Custom Extension to a Trading Partner. . . . .	8-19
Adding Services. . . . .	8-21
Adding Service Profiles to a Service. . . . .	8-22
Defining Trading Partner Profiles . . . . .	8-30
Defining Protocol Bindings. . . . .	8-31

Listing and Locating Trading Partners . . . . .	8-41
Listing and Locating Services . . . . .	8-42
Viewing and Changing Trading Partner Profiles . . . . .	8-43
Viewing and Changing Certificates . . . . .	8-46
Viewing and Changing Bindings . . . . .	8-47
Viewing and Changing a Custom Extension . . . . .	8-59
Viewing and Changing Services . . . . .	8-60
Viewing and Changing Service Profiles . . . . .	8-62
Enabling and Disabling Trading Partner and Service Profiles . . . . .	8-64
Importing Management Data . . . . .	8-67
Exporting Management Data . . . . .	8-68
Deleting Trading Partner Profiles and Services Using Bulk Delete . . . . .	8-70
Deleting Trading Partner Profiles . . . . .	8-71
Deleting Certificates, Bindings, or Custom Extensions. . . . .	8-72
Deleting Services . . . . .	8-74
Deleting Service Profiles from a Service. . . . .	8-74
Viewing Statistics . . . . .	8-75
Monitoring Messages . . . . .	8-76

## System Configuration

About System Administration . . . . .	9-2
Overview of the System Configuration Module . . . . .	9-7
Viewing the Archive and Purge Configuration . . . . .	9-9
Configuring the Archive and Purge Process . . . . .	9-10
Configuring the Archive Datastore . . . . .	9-11
Configuring the Tracking and Archive Defaults . . . . .	9-11
Manually Starting the Archive and Purge Process. . . . .	9-12
Adding Passwords to the Password Store . . . . .	9-13

Listing and Locating Password Aliases . . . . .	9-14
Changing the Password for a Password Alias . . . . .	9-14
Deleting Passwords from the Password Store . . . . .	9-15
Configuring the Server for Application Integration . . . . .	9-15
Configuring the Worklist Task Creation Role. . . . .	9-16

## User Management

About WebLogic Integration Users, Groups, and Roles . . . . .	10-2
Overview of the User Management Module . . . . .	10-9
Adding a User . . . . .	10-11
Adding a Group . . . . .	10-12
Adding a Role . . . . .	10-13
Constructing a Role Statement . . . . .	10-13
Listing and Locating Users . . . . .	10-16
Listing and Locating Groups . . . . .	10-16
Listing and Locating Roles . . . . .	10-17
Viewing and Changing User Properties . . . . .	10-17
Viewing and Changing Group Properties . . . . .	10-19
Viewing and Setting Role Conditions . . . . .	10-20
Deleting Users, Groups, or Roles . . . . .	10-20

## Business Calendar Configuration

About Business Calendars and Business Time Calculations. . . . .	11-2
Overview of the Business Calendar Configuration Module . . . . .	11-4
Adding a Business Calendar . . . . .	11-5
Listing and Locating Business Calendars . . . . .	11-6
Viewing and Changing Business Calendars . . . . .	11-6
Defining a Time Period Rule. . . . .	11-8



Exporting and Importing Business Calendars . . . . .	11-9
Assigning Business Calendars to Users and Groups . . . . .	11-11
Deleting Business Calendars . . . . .	11-12

## TPM Schema

TPM Overview . . . . .	A-1
address Element . . . . .	A-5
authentication Element . . . . .	A-6
client-certificate Element . . . . .	A-9
ebxml-binding Element . . . . .	A-11
encryption-certificate Element . . . . .	A-18
extended-property-set Element . . . . .	A-20
failure-notifier Element . . . . .	A-22
failure-report-administrator Element . . . . .	A-23
reference simpleType . . . . .	A-25
rosettanet-binding Element . . . . .	A-26
rosettanet-service-defaults Element . . . . .	A-33
server-certificate Element . . . . .	A-35
service Element . . . . .	A-37
service-profile Element . . . . .	A-40
signature-certificate Element . . . . .	A-44
signature-transforms Element . . . . .	A-45
trading-partner Element . . . . .	A-47
trading-partner-management Element . . . . .	A-53
transport Element . . . . .	A-56
web-service-binding Element . . . . .	A-59
xpath Element . . . . .	A-60

## Using the Bulk Loader

About Using the Bulk Loader .....	B-1
Schemas .....	B-2
Configuring the Bulk Loader Configuration File .....	B-2
Using the Bulk Loader Command Line Options .....	B-3
Importing and Exporting Management Data .....	B-4
Deleting Management Data .....	B-10

## Production Database

Creating the WebLogic Integration Tables .....	C-1
--	-----

# About This Document

This document provides the information you need to manage solutions built with BEA WebLogic Integration. Specifically, it discusses the following topics:

- [Chapter 1, “Introducing the WebLogic Integration Administration Console,”](#) provides a summary of the administration tasks that can be performed using the WebLogic Integration Administration Console, and instructions for starting the console.
- [Chapter 2, “Processes Configuration,”](#) provides the information you need to use the Process Configuration module of the WebLogic Integration Administration Console to configure business process security and archiving properties, manage process versions, update dynamic callback or control selectors, or view an interactive process graph.
- [Chapter 3, “Process Instance Monitoring,”](#) provides the information you need to use the Process Instance Monitoring module of the WebLogic Integration Administration Console to view summary or detailed process instance status, monitor process progress by viewing an interactive process instance graph, terminate or suspend instances, resume previously suspended instances, or unfreeze frozen instances.
- [Chapter 4, “Message Broker,”](#) provides the information you need to use the Message Broker module of the WebLogic Integration Administration Console to monitor message broker channels, view channel subscribers, and set channel security policies.
- [Chapter 5, “Event Generators,”](#) provides the information you need to use the Event Generator module of the WebLogic Integration Administration Console to create and deploy JMS, Email, File, and Timer event generators, add channel rules to an event generator, and suspend or resume deployed event generators.

- [Chapter 6, “Worklist Administration,”](#) provides the information you need to use the Worklist Administration module of the WebLogic Integration Administration Console to monitor task status, perform queries to determine individual workload, reassign tasks to speed progress, control task routing by creating substitute routing rules, and update task properties or state.
- [Chapter 7, “Application Integration,”](#) provides the information you need to use the Application Integration module of the WebLogic Integration Administration Console to view the adapter instances associated with an application view, view adapter event and service statistics, set application view security policies, and suspend, resume, or redeploy application views and adapter instances.
- [Chapter 8, “Trading Partner Management,”](#) provides the information you need to use the Trading Partner Management module of the WebLogic Integration Administration Console to configure the entities and resources required for your trading partner integration applications and to monitor the messages exchanged.
- [Chapter 9, “System Configuration,”](#) provides the information you need to use the System Configuration module of the WebLogic Integration Administration Console to create, view or change the password aliases in the password store, specify the datastore used to archive tracking data, set the archive and purge schedule, set the default tracking level for worklist tasks and business processes, set the default archiving policy for business processes, and configure the JMS connection factory, repository root, and debug level for application integration.
- [Chapter 10, “User Management,”](#) provides the information you need to use the User Management module of the WebLogic Integration Administration Console to manage the users, groups, and roles defined in the default security realm. Information about the default users, groups, and security roles is also provided.
- [Chapter 11, “Business Calendar Configuration,”](#) provides the information you need to use the Business Calendar Configuration module of the WebLogic Integration Administration Console to create and update business calendars, export and import business calendars, and map calendars to users or groups.
- [Appendix A, “TPM Schema,”](#) provides reference information for the `tpmschema.xsd` used in trading partner integration.
- [Appendix B, “Using the Bulk Loader,”](#) provides the information you need to use the Bulk Loader command line utility to update trading partner management data.
- [Appendix C, “Production Database,”](#) provides information about creating the tables required by WebLogic Integration.

## What You Need to Know

This document is intended mainly for developers and administrators who are familiar with:

- WebLogic Server administration.
- The entities and resources that make up WebLogic Integration applications.

## dev2dev Product Documentation Web Site

BEA product documentation is available on the dev2dev Product Documentation Web site at <http://edocs.bea.com>.

## How to Print the Document

You can print a copy of this document from a Web browser, one file at a time, by using the File→Print option on your Web browser.

A PDF version of this document is available on the WebLogic Integration documentation Home page on the dev2dev Web site (and also on the documentation CD). You can open the PDF in Adobe Acrobat Reader and print the entire document (or a portion of it) in book format. To access the PDFs, open the WebLogic Integration documentation Home page, click the PDF files button and select the document you want to print.

If you do not have the Adobe Acrobat Reader, you can get it for free from the Adobe Web site at <http://www.adobe.com/>.

## Contact Us!

Your feedback on the BEA WebLogic Integration documentation is important to us. Send us e-mail at **docsupport@bea.com** if you have questions or comments. Your comments will be reviewed directly by the BEA professionals who create and update the WebLogic Integration documentation.

In your e-mail message, please indicate that you are using the documentation for the BEA WebLogic Integration 5.0 release.

If you have any questions about this version of BEA WebLogic Integration, or if you have problems installing and running BEA WebLogic Integration, contact BEA Customer Support through BEA WebSupport at **www.bea.com**. You can also contact Customer Support by using the contact information provided on the Customer Support Card, which is included in the product package.

When contacting Customer Support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your machine type and authorization codes
- The name and version of the product you are using
- A description of the problem and the content of pertinent error messages

# Documentation Conventions

The following documentation conventions are used throughout this document.

Convention	Item
<b>boldface text</b>	Indicates terms defined in the glossary.
Ctrl+Tab	Indicates that you must press two or more keys simultaneously.
<i>italics</i>	Indicates emphasis or book titles.
monospace text	<div>Indicates code samples, commands and their options, data structures and their members, data types, directories, and file names and their extensions. Monospace text also indicates text that you must enter from the keyboard.</div> <div><i>Examples:</i></div> <div>#include &lt;iostream.h&gt; void main ( ) the pointer psz chmod u+w * \tux\data\ap .doc tux.doc BITMAP float</div>
<b>monospace boldface text</b>	<div>Identifies significant words in code.</div> <div><i>Example:</i></div> <div>void <b>commit</b> ( )</div>

Convention	Item
<i>monospace</i> <i>italic</i> <i>text</i>	Identifies variables in code. <i>Example:</i> String <i>expr</i>
UPPERCASE TEXT	Indicates device names, environment variables, and logical operators. <i>Examples:</i> LPT1 SIGNON OR
{ }	Indicates a set of choices in a syntax line. The braces themselves should never be typed.
[ ]	Indicates optional items in a syntax line. The brackets themselves should never be typed. <i>Example:</i> buildobjclient [-v] [-o name ] [-f <i>file-list</i> ...] [-l <i>file-list</i> ]...
	Separates mutually exclusive choices in a syntax line. The symbol itself should never be typed.
...	Indicates one of the following in a command line: <ul style="list-style-type: none"> <li>• That an argument can be repeated several times in a command line</li> <li>• That the statement omits additional optional arguments</li> <li>• That you can enter additional parameters, values, or other information</li> </ul> The ellipsis itself should never be typed. <i>Example:</i> buildobjclient [-v] [-o name ] [-f <i>file-list</i> ...] [-l <i>file-list</i> ]...
.	Indicates the omission of items from a code example or from a syntax line. The vertical ellipsis itself should never be typed.

About This Document



# Introducing the WebLogic Integration Administration Console

The WebLogic Integration Administration Console allows you to manage and monitor the entities and resources required for your WebLogic Integration applications. The following table lists the available modules and summarizes the tasks associated with each.

Module	Associated Tasks
Process Configuration	<a href="#">Listing and Locating Process Types</a> <a href="#">Listing and Locating Dynamic Controls</a> <a href="#">Viewing and Changing Process Details</a> <a href="#">Viewing an Interactive or Printable Process Type Graph</a> <a href="#">Managing Process Versions</a> <a href="#">Adding or Changing Dynamic Client Callback Selectors</a> <a href="#">Updating Security Policies</a> <a href="#">Adding or Changing Dynamic Control Selectors</a> <a href="#">Defining Process Control Properties for a Selector</a> <a href="#">Defining Service Broker Control Properties for a Selector</a> <a href="#">Deleting Dynamic Control Selectors</a>
Process Instance Monitoring	<a href="#">Viewing Instance Statistics by Process Type</a> <a href="#">Viewing System Health Statistics</a> <a href="#">Listing and Locating Process Instances</a> <a href="#">Constructing an Advanced Search</a> <a href="#">Viewing Process Instance Details</a> <a href="#">Viewing an Interactive or Printable Process Instance Graph</a> <a href="#">Suspending, Resuming, Terminating, or Unfreezing Process Instances</a>

Module	Associated Tasks
Message Broker	<a href="#">Listing and Locating Channels</a> <a href="#">Viewing Channel Details and Subscriptions</a> <a href="#">Setting Channel Security Policies</a> <a href="#">Viewing and Resetting Message Counts</a>
Event Generators	<a href="#">Listing and Locating Event Generators</a> <a href="#">Creating and Deploying Event Generators</a> <a href="#">Defining Channel Rules for a File Event Generator</a> <a href="#">Defining Channel Rules for an Email Event Generator</a> <a href="#">Defining Channel Rules for a JMS Event Generator</a> <a href="#">Defining Channel Rules for a Timer Event Generator</a> <a href="#">Listing and Locating Event Generators</a> <a href="#">Viewing and Updating Event Generator Channel Rules</a> <a href="#">Suspending and Resuming Event Generators</a> <a href="#">Resetting the Counters</a> <a href="#">Deleting Channel Rules</a> <a href="#">Deleting Event Generators</a>
Worklist Administration	<a href="#">Overview of the Worklist Administration Module</a> <a href="#">Listing and Locating Worklist Tasks</a> <a href="#">Listing and Locating Substitute Routing Rules</a> <a href="#">Constructing a Custom Query for Task Instances</a> <a href="#">Viewing and Changing Task Details</a> <a href="#">Updating Task State or Deleting Tasks</a> <a href="#">Updating Task Comment, Owner, or Due Dates from the Summary Page</a> <a href="#">Adding a Substitute Routing Rule</a> <a href="#">Changing a Substitute Routing Rule</a> <a href="#">Deleting a Substitute Routing Rule</a>

<b>Module</b>	<b>Associated Tasks</b>
Application Integration	<a href="#">Listing and Locating Application Views</a> <a href="#">Listing and Locating Adapter Instances</a> <a href="#">Viewing Application View Instance Statistics</a> <a href="#">Viewing Adapter Instance Statistics</a> <a href="#">Viewing Dependent Application Views of Adapter Instances</a> <a href="#">Viewing and Changing Application View Details</a> <a href="#">Viewing and Changing Adapter Instance Details</a> <a href="#">Viewing and Changing Event Connection Properties</a> <a href="#">Viewing and Changing Service Connection Properties</a> <a href="#">Viewing and Changing Connection Pool Size Parameters</a> <a href="#">Viewing and Changing Application View Auto Suspend Settings</a> <a href="#">Viewing and Changing Environment Variable Values for an Application View</a> <a href="#">Viewing and Changing WebLogic Server to EIS Principal Mappings</a> <a href="#">Changing Event Connections for an Application View</a> <a href="#">Changing Service Connections for an Application View</a> <a href="#">Changing Event Generation Targets</a> <a href="#">Changing Application View Container-Managed Sign-On Settings</a> <a href="#">Updating Security Policies</a> <a href="#">Suspending or Resuming an Application View or Adapter Instance</a> <a href="#">Redeploying an Adapter Instance</a> <a href="#">Resetting the Counters</a>

Module	Associated Tasks
Trading Partner Management	<a href="#">Configuring Trading Partner Management</a> <a href="#">Adding Trading Partner Profiles</a> <a href="#">Adding Certificates to a Trading Partner</a> <a href="#">Adding Protocol Bindings to a Trading Partner</a> <a href="#">Adding a Custom Extension to a Trading Partner</a> <a href="#">Adding Services</a> <a href="#">Adding Service Profiles to a Service</a> <a href="#">Defining Trading Partner Profiles</a> <a href="#">Defining Protocol Bindings</a> <a href="#">Listing and Locating Trading Partners</a> <a href="#">Listing and Locating Services</a> <a href="#">Viewing and Changing Trading Partner Profiles</a> <a href="#">Viewing and Changing Certificates</a> <a href="#">Viewing and Changing Bindings</a> <a href="#">Viewing and Changing a Custom Extension</a> <a href="#">Viewing and Changing Services</a> <a href="#">Viewing and Changing Service Profiles</a> <a href="#">Enabling and Disabling Trading Partner and Service Profiles</a> <a href="#">Importing Management Data</a> <a href="#">Exporting Management Data</a> <a href="#">Deleting Trading Partner Profiles and Services Using Bulk Delete</a> <a href="#">Deleting Trading Partner Profiles</a> <a href="#">Deleting Certificates, Bindings, or Custom Extensions</a> <a href="#">Deleting Services</a> <a href="#">Deleting Service Profiles from a Service</a> <a href="#">Viewing Statistics</a> <a href="#">Monitoring Messages</a>
System Configuration	<a href="#">Viewing the Archive and Purge Configuration</a> <a href="#">Configuring the Archive and Purge Process</a> <a href="#">Configuring the Archive Datastore</a> <a href="#">Configuring the Tracking and Archive Defaults</a> <a href="#">Manually Starting the Archive and Purge Process</a> <a href="#">Adding Passwords to the Password Store</a> <a href="#">Listing and Locating Password Aliases</a> <a href="#">Changing the Password for a Password Alias</a> <a href="#">Deleting Passwords from the Password Store</a> <a href="#">Configuring the Server for Application Integration</a> <a href="#">Configuring the Server for Application Integration</a>

Module	Associated Tasks
User Management	<a href="#">Adding a User</a> <a href="#">Adding a Group</a> <a href="#">Adding a Role</a> <a href="#">Listing and Locating Users</a> <a href="#">Listing and Locating Groups</a> <a href="#">Listing and Locating Roles</a> <a href="#">Viewing and Changing User Properties</a> <a href="#">Viewing and Changing Group Properties</a> <a href="#">Viewing and Setting Role Conditions</a> <a href="#">Deleting Users, Groups, or Roles</a>
Business Calendar Configuration	<a href="#">Adding a Business Calendar</a> <a href="#">Listing and Locating Business Calendars</a> <a href="#">Viewing and Changing Business Calendars</a> <a href="#">Defining a Time Period Rule</a> <a href="#">Exporting and Importing Business Calendars</a> <a href="#">Assigning Business Calendars to Users and Groups</a> <a href="#">Deleting Business Calendars</a>

## Starting the WebLogic Integration Administration Console

Access to the WebLogic Integration Administration Console is password protected.

### To start the console:

1. Open the following URL in your web browser:

`http://adminserver:port/wliconsole`

Here, *adminserver* is the host name or IP address of the WebLogic Server administrative server, and *port* is the server listening port.

2. Enter the username and password when prompted.



**Note:** The user must be a member of the Administrators, IntegrationAdministrators, IntegrationOperators, or IntegrationMonitors group. See [“Default Groups, Roles, and Security Policies” on page 10-3](#). If this is the sample integration domain, the default login is:


**username:** weblogic


**password:** weblogic

The WebLogic Integration Administration Console home page is displayed.

The home page provides access to each of the management modules. To return to the home page at any time during the session:

- Click the  icon in the upper right corner of the page.
- Click  in the module navigation bar.

If the console is idle for a period of time, the user is automatically logged off. To manually log out and return the Login page, select the Logout  icon.

To access the online help at any time, select the Help  icon.

# Processes Configuration

This section provides the information you need to use the *Process Configuration* module of the WebLogic Integration Administration Console to:

- View process type information and locate specific processes for configuration.
- View or update process type properties, such as the display name, tracking level, and archiving policy.
- View or update the security policies for a process.
- Configure the activation time for a newly deployed process version, or rollback to a previous version.
- View an interactive or printable process type graph.
- View or update the selectors used to dynamically set control attributes for a Process or Service Broker control.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to make changes to the configuration for a process or dynamic control. IntegrationOperators cannot modify process security policies. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About Process Configuration](#)
- [Overview of the Process Configuration Module](#)
- [Listing and Locating Process Types](#)

- [Listing and Locating Dynamic Controls](#)
- [Viewing and Changing Process Details](#)
- [Viewing an Interactive or Printable Process Type Graph](#)
- [Adding or Changing Dynamic Control Selectors](#)
- [Adding or Changing Dynamic Client Callback Selectors](#)
- [Updating Security Policies](#)
- [Adding or Changing Dynamic Control Selectors](#)
- [Defining Process Control Properties for a Selector](#)
- [Defining Service Broker Control Properties for a Selector](#)
- [Deleting Dynamic Control Selectors](#)

## About Process Configuration

The following sections provide background information related to business process administration:

- [Managing Process Tracking Data](#)
- [Process Security Policies](#)
- [Service Level Agreements](#)
- [Dynamic Controls](#)

## Managing Process Tracking Data

The data generated as process instances execute is initially stored in the runtime database. The monitoring information provided in the console is based on this data. In order to optimize performance, it is important to keep the amount of tracking data stored in the runtime database to a minimum. This is accomplished by:

- Capturing only the necessary data.
- Archiving the data to an offline database if required for later analysis.
- Purging the data from the runtime database when it is no longer needed for monitoring from the console.



A combination of system and process properties control the management of tracking data. The following table provides a summary of each property and its related configuration tasks. To learn how to carry out the configuration task, see the referenced topic.

Property	Configuration Task	Task Type and Reference
Tracking Level	Set the system default tracking level.	System Configuration. See <a href="#">“Configuring the Tracking and Archive Defaults”</a> on page 9-11.
	Set or verify the tracking level for each process. The administrator can set the level for a process to: <ul style="list-style-type: none"> <li>• System <b>Default</b></li> <li>• <b>Full</b>, <b>Node</b>, <b>Minimum</b>, or <b>None</b> (setting overrides the system default tracking level)</li> </ul>	Process Configuration. See <a href="#">“Viewing and Changing Process Details”</a> on page 2-11.
Archive and Purge Configuration	Configure the archive and purge process to do one of the following: <ul style="list-style-type: none"> <li>• Copy data to an offline database, then purge it from the runtime database (archive and purge).</li> <li>• Purge the data from the runtime database without copy (purge only).</li> </ul>	System Configuration. See <a href="#">“Configuring the Archive and Purge Process”</a> on page 9-10.
	Set the regular intervals at which the archive and purge process runs.	
	Enable or disable the archiver process. (When the archiver process is disabled, the archive and purge process is configured for purge only.)	
Purge Delay	Set the amount of time after completion or termination before the instance data is subject to purge by the archive and purge process.	System Configuration. See <a href="#">“Configuring the Archive and Purge Process”</a> on page 9-10.

Property	Configuration Task	Task Type and Reference
Archive Policy	Set or verify the archive policy for each process: <ul style="list-style-type: none"><li>• <b>On</b> indicates that the instance data is archived if the archiver is enabled. If the archiver is disabled, no processes are archived, regardless of the policy set.</li><li>• <b>Off</b> indicates that the instance data is not subject to archive even if the archiver is enabled (that is, the data is only purged).</li><li>• <b>Default</b> indicates that the system default archive policy (described below) is used.</li></ul>	Process Configuration. See <a href="#">“Viewing and Changing Process Details” on page 2-11</a>
	Set the system default archive policy to <b>On</b> or <b>Off</b> .	System Configuration. See <a href="#">“Configuring the Tracking and Archive Defaults” on page 9-11</a> .

To learn more, see the following topics:

- [“Process Tracking Data” on page 9-2](#).
- [“Archiving and Purging Tracking Data” on page 9-4](#)

## Process Security Policies

To ensure process security, the administrator can configure the following security policies for a process:

- *Execution policy for process operations*  
The execution policy specifies whether the operations in the process are run as the *start user* or the *caller’s ID*:
  - If start user is specified, each operation assumes the identity of the user that started the process.
  - If caller’s ID is specified, the operation after the call in assumes the identity of that interrupting call.

In addition, the administrator configures whether or not a single principal is required. If a single principal is required, then all incoming client requests must come from the same user.

Execution policy controls the identity used to access external or backend resources. It allows the administrator to specify whether a process accesses an external system as the invoking application or as an application that called into the process later. For example, suppose a process listens for a message on a channel and then waits for a client request. The administrator can set the execution policy to use the identity from the client request when the process subsequently accesses SAP.

- *Process authorization policy*

The role(s) authorized to invoke the process methods (client requests). All methods in the process inherit the role(s) specified in the process authorization policy.

**Note:** If the process authorization policy is not defined, everyone is authorized.

- *Method authorization policy*

The role(s) authorized to invoke the process methods (client requests). All methods inherit the role(s) specified in the process authorization policy. Additional roles can be added to the authorization policy for the method.

- *Callback authorization policy*

The roles authorized to invoke the process callback.

**Note:** If the callback authorization policy is not defined, everyone is authorized.

To learn how to set the security policies, see [“Updating Security Policies” on page 2-21](#).


## Service Level Agreements


A service level agreement (SLA) specifies a performance target for a process. It is typically an internal or external commitment that a process will be executed within a specified period of time.

To assist you in achieving the SLA for a process, the WebLogic Integration Administration Console allows you to set the following thresholds:

- SLA threshold, which represents the commitment applicable to the process type (number of seconds, minutes, hours, or days).
- SLA warning threshold, which is a percent of the total SLA.

Process status relative to these thresholds is tracked for each process instance as follows:

- When the elapsed time for a process instance reaches the warning threshold, a warning  is displayed on the Process Instance Summary and Detail pages. The amount of time remaining until the SLA threshold will be reached is also displayed.

- When the elapsed time exceeds the SLA set, a red flag  is displayed. The amount of time the SLA threshold has been exceeded is also displayed.

This ability to set SLA thresholds allows you to easily identify processes that do not execute within the target time frame. You can then make the changes necessary to meet agreements between suppliers and customers, or to achieve your own performance goals. To learn how to set the SLA for a process, see [“Viewing and Changing Process Details” on page 2-11](#).

## Process Versions

When developers need to modify a deployed process, they must create a new process version and then release it into production along with older versions. To learn more about creating and deploying new versions, see the following topics in *Building Integration Applications* in the WebLogic Workshop help:

- [Versioning a Business Process](#)
- [Building and Deploying WebLogic Integration Applications](#)

When multiple versions are deployed, the system determines which version to use when creating new instances. The administrator controls the release of a process version by:

- Enabling or disabling a version.
- Setting the activation time for a version.

When creating a new instance, the system selects the version with the most recent activation time from among the enabled versions. (A disabled version is not available for selection.)

When an administrator activates a process by setting its activation time, instances currently running are not affected. Only instances that are created after the new version becomes active are created based on the new version.

If a newly activated version experiences problems, a rollback is easily accomplished by doing one of the following:

- Updating the activation time on the prior version.
- Disabling the problem version. In this case, the enabled version with the most recent activation date becomes the active version.

To learn more about how to enable or disable a version, or to configure the activation time, see [“Adding or Changing Dynamic Control Selectors” on page 2-22](#).

## Dynamic Controls

Dynamic controls, which currently include the Service Broker and Process controls, provide the means to dynamically set control attributes through a combination of look-up rules and look-up values. This process is known as *dynamic binding*. In dynamic binding, the process developer specifies look-up rules, and the administrator defines the look-up values. This design pattern allows control attributes to be reconfigured for a running application, without redeployment.

The look-up or *selector* values are stored in the `DynamicProperties.xml` file, which is located in the `wliconfig` subdirectory of the domain root. You can manage the values stored in the `DynamicProperties.xml` file from the View Dynamic Control Properties page of the Process Configuration module.

Dynamic binding changes made in the WebLogic Integration Administration Console override both configuration changes made in the Workshop development environment and static annotations.

To learn more about the dynamic controls, see the following topics in *Building Integration Applications* in the WebLogic Workshop help:

- [Process Control](#)
- [Service Broker Control](#)
- [Using Dynamic Binding](#)

## Overview of the Process Configuration Module

The following table lists the pages you can access from the Process Configuration module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
<b>Process Types</b>		
Process Property Summary	View a list of process types. display name, public URI, state (stateful or stateless), tracking level, archive policy, and SLA are displayed.	<a href="#">“Listing and Locating Process Types” on page 2-10</a>
	Access the Process Type Details page.	

Page	Associated Tasks	Topics
Process Type Details	View process properties. Identifying information (such as service URI and application name), configurable properties (display name, tracking level, archiving policy, SLA), dynamic client callback properties, execution and authorization policies, variables, and active version are displayed.	<a href="#">“Viewing and Changing Process Details” on page 2-11</a>
	Access an interactive or printable graph of the process.	<a href="#">“Viewing an Interactive or Printable Process Type Graph” on page 2-16</a>
	Access one of the following pages to update settings: Edit Process Properties Edit Process Versioning Add New Client Callback Properties Edit Client Callback Properties Edit Process Execution Policy Edit Process Authorization Policy Edit Method Authorization Policy Edit Call Back Authorization Policy	
Edit Process Properties	Update service URI, display name, SLA, SLA warning threshold, tracking level, and archiving policy for the selected process type.	<a href="#">“Viewing and Changing Process Details” on page 2-11</a>
Edit Process Versioning	Enable, disable, or set the activation date and time for the selected version.	<a href="#">“Adding or Changing Dynamic Control Selectors” on page 2-22</a>
Add New Client Callback Properties	Add a selector value and properties which can be used to dynamically configure the callback to the client.	<a href="#">“Adding or Changing Dynamic Client Callback Selectors” on page 2-19</a>
Edit Client Callback Properties	Edit the properties which can be used to dynamically configure the callback to the client.	<a href="#">“Adding or Changing Dynamic Client Callback Selectors” on page 2-19</a>
Edit Process Execution Policy	Specify the <b>run as</b> identity for the process operations, and whether or not a single principal is required.	<a href="#">“Updating Security Policies” on page 2-21</a> <a href="#">“Process Security Policies” on page 2-4</a>

Page	Associated Tasks	Topics
Edit Process Authorization Policy	Set the minimum authorized roles for the methods (client requests) in the process.	<a href="#">“Updating Security Policies” on page 2-21</a> <a href="#">“Process Security Policies” on page 2-4</a>
Edit Process Method Authorization Policy	Set additional authorized roles for the selected method. (Minimum authorized roles for all methods are set by the process authorization policy.)	<a href="#">“Updating Security Policies” on page 2-21</a> <a href="#">“Process Security Policies” on page 2-4</a>
Edit Call Back Authorization Policy	Set the authorized roles for the selected callback.	<a href="#">“Updating Security Policies” on page 2-21</a> <a href="#">“Process Security Policies” on page 2-4</a>
<b>Dynamic Controls</b>		
View Dynamic Control Properties	View a list of dynamic controls. Control name, type, and selector value are displayed.	<a href="#">“Listing and Locating Dynamic Controls” on page 2-11</a>
	Delete a selector from the control.	<a href="#">“Deleting Dynamic Control Selectors” on page 2-25</a>
	Access the Add New or Edit page for the control to define properties for a new selector, or edit properties for an existing selector.	<a href="#">“Adding or Changing Dynamic Control Selectors” on page 2-22</a>
Add New Process Control Selector	Define the properties for a new selector.	<a href="#">“Defining Process Control Properties for a Selector” on page 2-23</a>
Edit Process Control Selector	Update the properties for an existing selector.	<a href="#">“Defining Process Control Properties for a Selector” on page 2-23</a>

Page	Associated Tasks	Topics
Add New Service Broker Control Selector	Define the properties for a new selector.	<a href="#">“Defining Service Broker Control Properties for a Selector” on page 2-24</a>
Edit Service Broker Control Selector	Update the properties for an existing selector.	<a href="#">“Defining Service Broker Control Properties for a Selector” on page 2-24</a>

## Listing and Locating Process Types





The Process Property Summary page displays the following information for each deployed process type. For a more detailed description of the properties, see [“Viewing and Changing Process Details” on page 2-11](#).

**Note:** The process types are listed alphabetically by display name.

Property	Description
Display name	<p>Display name assigned to the process. The name is a link to the Process Type Details page.</p> <p><b>Note:</b> If more than one version of the process is deployed, it is customary to append the version number to the display name, but this convention is not enforced.</p>
Public URI	The process URI. If there are multiple versions deployed, this is the version group URI (that is, the version number is not appended).
State	The process type ( <b>Stateful</b> or <b>Stateless</b> ).
Tracking Level	The tracking level set for the process.
Archive Policy	The archive policy set for tracking data.
SLA	Service level agreement set for the process.









**To list and locate process types:**

1. From the home page, select the **Process Configuration** module.
2. Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Listing and Locating Dynamic Controls

The View Dynamic Control Properties page displays the dynamic controls (Process and Service Broker controls) associated with deployed processes. For each control, the selector values for any dynamic bindings are displayed.

**To list and locate dynamic controls:**

1. From the home page, select the **Process Configuration** module.
2. From the left panel, select **View Dynamic Controls**.
3. To locate a specific control, do one of the following:
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Viewing and Changing Process Details

The Process Type Details page allows you to view or change process properties.

**To view and change process details:**

1. Locate the process. See [“Listing and Locating Process Types” on page 2-10](#).
2. Click the process name to display the Process Type Details page.



3. To update configurable properties, do the following:
  - a. In the Configurable Properties section, click **Configure Parameters** to display the Edit Process Properties page.
  - b. Set the properties as required. The properties are described in the table that follows this procedure.
  - c. Click **Submit** to update the properties and return to the Process Type Details page.
4. To enable, disable, or activate a version, see [“Adding or Changing Dynamic Control Selectors” on page 2-22](#).
5. To update the security policies, see [“Updating Security Policies” on page 2-21](#).

The following table summarizes the information displayed on the Process Type Details page.

**Note:** When the server is started in iterative development mode (`iterativeDevFlag=true`), updates to the configurable properties are overridden when the process is redeployed through an application build or process redeploy.

Property	Description	Administrator Can Set (Yes/No)
Service URI	The process URI. If there are multiple versions of the process, a version number is appended	No
Application Name	The name of the application.	No
Stateful/Stateless	The process type ( <b>Stateful</b> or <b>Stateless</b> .) To learn more about how stateful and stateless processes are created, see <a href="#">Building Stateless and Stateful Business Processes</a> in <i>Building Integration Applications</i> in the WebLogic Workshop Help.	No
Description	User-friendly description of the process.	No
Version Group URI	The URI for the group.	No
Process Graph	Links to an interactive or printable view of the process. See <a href="#">“Viewing an Interactive or Printable Process Type Graph” on page 2-16</a> .	No

Property	Description	Administrator Can Set (Yes/No)
<b>Configurable Properties</b>		
Display name	<p>Display name assigned to the process.</p> <p><b>Note:</b> If more than one version of the process is deployed, it is customary to append the version number to the display name, but this convention is not enforced.</p>	Yes
Tracking Level	<p>The tracking level set for the process. The following types of events can be tracked:</p> <p><i>Global events</i> Events such as start process, end process, suspend, and resume.</p> <p><i>Node transitions</i> Events generated by each executed node (a start node event and an end or abort node event).</p> <p><i>Data</i> Data logged as a result of invoking of <code>JpdContext.trackData()</code>.</p> <hr/> <p><b>Full</b>      Global events, node transitions, and data are tracked.</p> <hr/> <p><b>Node</b>      Global events and node transitions are tracked.</p> <hr/> <p><b>Minimum</b>      Global events, such as start process, end process, suspend, and resume, are tracked.</p> <hr/> <p><b>Default</b>      Tracking level is set to the current system-wide setting (Full, Node, Minimum, or None). See <a href="#">“Configuring the Tracking and Archive Defaults” on page 9-11</a>.</p> <hr/> <p><b>None</b>      No events or data are tracked.</p>	Yes
Archive Policy	<p>The archive policy set for tracking data.</p> <hr/> <p><b>On</b>      Archiving is enabled for this process.</p> <hr/> <p><b>Off</b>      Archiving is disabled for this process.</p> <hr/> <p><b>Default</b>      Process archive policy is set to the system default archive policy. See <a href="#">“Archiving and Purging Tracking Data” on page 9-4</a>.</p>	Yes

Property	Description	Administrator Can Set (Yes/No)
SLA	<p>Service level agreements (SLA) expressed as the number of seconds, minutes, hours, or days. When this threshold has been reached, a red flag  is displayed for the process instance.</p> <p>For processes without an SLA, NA is displayed. To remove an SLA setting, enter 0 in the SLA field on the Edit Process Properties page.</p> <p>To learn more about the SLA, see <a href="#">“Service Level Agreements” on page 2-5</a>.</p>	Yes
SLA Warning Threshold	<p>A percent of the total SLA time. When this threshold has been reached, a warning flag  is displayed for the process instance.</p>	Yes

Property	Description	Administrator Can Set (Yes/No)
<b>Dynamic Client Callback Properties</b>		
Selector table	If the process includes a Client Response node for which a lookup property has been specified, this table lists the selector values configured by the administrator. If no values are listed, none have yet been added.	Yes
Selector name	The selector name used to look up the selector properties.	
Edit	A link to the Edit Client Callback Properties page for the selector.	
Delete	A control used to delete the selector.	
<b>Version Group</b>		
Version Group URI	The URI for the group.	No
Default Service URI	The URI for the process type.	No
Current Active	The process in the group that is currently active.	No
Version group table	Entry for each deployed version in the version group.	No
Display Name	Display name assigned to the process version.	No
Service URI	The URI for the process version.	No
Enabled	Indicates whether the process is enabled ( <b>true</b> ) or disabled ( <b>false</b> ).	Yes
Activation Date	Date and time the process version became, or is to become, active.	Yes
Configure	Link to the Edit Process Versioning page, from which you can enable, disable, or update the activation time for the process version. See <a href="#">“Adding or Changing Dynamic Control Selectors”</a> on page 2-22.	

Property	Description	Administrator Can Set (Yes/No)
<b>Security Policies</b>		
Execution Policy	Run As	The identity the operations in the process assume while executing. Options are <b>caller's identity</b> or <b>start user</b> .
	Single Principal Required	<b>Yes</b> or <b>No</b> . If set to <b>Yes</b> , all incoming client requests must come from the same user.
Process Authorization Policy	Roles authorized to invoke process methods.	Yes
Method Authorization Policy	Additional roles authorized to invoke the method. (The roles specified for Process Authorization Policy are inherited by the method.)	Yes
Callback Authorization Policy	Roles authorized to invoke the callback.	Yes
<b>Variables</b>		
Variables	Name and declared type for each variable defined	No

## Viewing an Interactive or Printable Process Type Graph

The Process Type Details page allows you to view an interactive or printable graph of the deployed process type. The graphical view represents your business process and its interactions with clients and resources, such as databases, JMS queues, file systems.

If there are running instances, you can access an interactive or printable graph of any instance from the Process Instance Detail page. See [“Viewing an Interactive or Printable Process Instance Graph” on page 3-12](#).

**Note:** The interactive process graph requires Adobe SVG Viewer Version 3.0. To learn more, see [“Browser Requirements for the Interactive Graph” on page 3-4](#). The printable graph requires a PDF viewer such as Adobe Acrobat.

**To view a printable graph for a process type:**

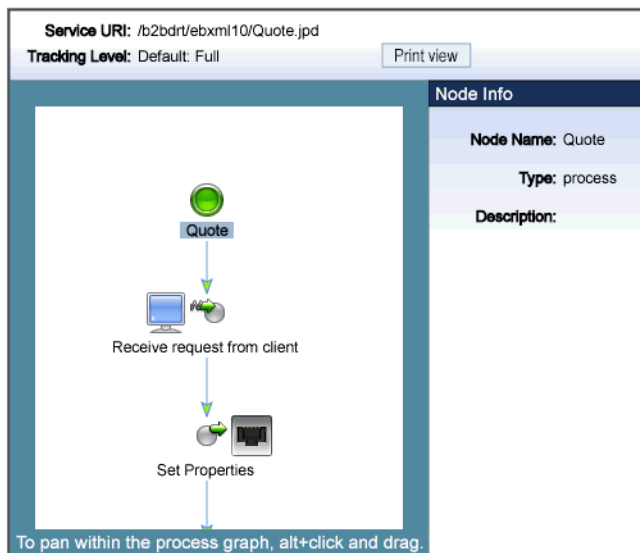
1. Locate the process to view. See [“Listing and Locating Process Types”](#) on page 2-10.
2. Click the process name to display the Process Type Details page.
3. Click **Printable View**.

The process graph is displayed as a PDF document.




**To view the interactive graph for a process type:**

1. Verify that your browser meets the requirements. See [“Browser Requirements for the Interactive Graph”](#) on page 3-4.
2. Locate the process to view. See [“Listing and Locating Process Types”](#) on page 2-10.
3. Click the process name to display the Process Type Details page.
4. Click **Interactive View**.

The Adobe SVG Viewer displays the interactive view as shown in the following figure.



5. Do any of the following:
  - To display the name, type, and description for a node, click the node image.

- To scroll the view, press and hold down the **Alt** key. The cursor changes to a hand  tool. Click and drag to scroll the process graph vertically or horizontally.
- To zoom in, press and hold down the **Ctrl** key. The cursor changes to a zoom in  tool. Click to zoom in.
- To zoom out, press and hold down the **Ctrl+Shift** keys. The cursor changes to a zoom out  tool. Click to zoom out.
- To change to a printable view, click **Print View**. The process graph is displayed as a PDF document.

## Managing Process Versions

The Process Type Details page allows you to enable, disable, or set the activation time for the versions in a process group.

### To enable, disable, or activate a version:

1. Locate the process to view. See [“Listing and Locating Process Types” on page 2-10](#).
2. Click the process name to display the Process Type Details page.

In the Version Group section, the current status of each version is displayed in the version table.

3. In the version table, click the **Configure** link for the version.
4. Do one or more of the following:
  - To set the activation time, select the month, date, and time from the **Activation Date** drop-down lists.
  - To disable the version, uncheck the **Enabled** check box.
  - To enable the version, check the **Enabled** check box.
5. Do one of the following:
  - To save the changes, click **Submit**.

The Process Type Details page is displayed. The version table reflects the changes.
  - To reset to the last saved values, click **Reset**.
  - To disregard changes and return to the Process Type Details page, click **Cancel**.



**Note:** There should always be one active version. If no version is available (that is, all versions are disabled) when the process is invoked, an error is logged.

## Adding or Changing Dynamic Client Callback Selectors

If a process includes a Client Response node for which a lookup property has been specified, the Process Details page includes a Dynamic Client Callback Properties section. This section allows you to define the selector values and properties required to dynamically configure the callback to the client.

To learn more about specifying a lookup property for a Client Response node, see [Sending Messages to Clients](#) in *Building Integration Applications* in the WebLogic Workshop help.

### To add or change a dynamic client callback selector:

1. Locate the process. See [“Listing and Locating Process Types” on page 2-10](#).
2. Click the process name to display the Process Type Details page.
3. In the Dynamic Client Callback Properties section, do one of the following:
  - a. To add a new selector, click the **Add a new callback property** link to display the Add New Client Callback Properties page.
  - b. To edit a selector, click the **Edit** link to the right of the selector value to display the Edit Client Callback Properties.
4. Set the properties as required. For a description of the available properties, see the table at the end of this procedure.
5. Click **Submit**.

The Process Type Details page is displayed. If you added a new selector, the value is displayed.

The following table summarizes the settings available on the Add New Client Callback Properties and Edit Client Callback Properties pages.

Setting	Description	Required/ Optional
In the <b>Selector Value</b> field, enter the look up key.	The value used to select and dynamically set control attributes at runtime.  <b>Note:</b> This field cannot be edited on the Edit Client Callback Properties page.	Required
Select the <b>No Dynamic Authentication, Basic Authentication, or Certificate Based Authentication</b> option button.	Type of authentication.	Optional
In the <b>User Name</b> field, enter the user name.	If <b>Basic Authentication</b> is selected, the required user name.	Required if <b>Basic Authentication</b> is selected.
In the <b>Password Alias</b> field, enter the password alias.	The password alias used to look up the user password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	
In the <b>Client Certificate Alias</b> field, enter the certificate alias.	Certificate alias for <b>Certificate Based Authentication</b> .	Required if <b>Certificate Based Authentication</b> is selected.
In the <b>Client Certificate Password Alias</b> field, enter the password alias.	Password alias to look up the certificate password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	
In the <b>Keystore Location</b> field, enter the keystore location.	The keystore location.	Required if <b>Certificate Based Authorization</b> is selected.
In the <b>Keystore Password Alias</b> field, enter the password alias.	The password alias used to look up the keystore password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	
In the <b>Keystore Type</b> field, enter the keystore type.	The keystore type.	

**To delete a dynamic client callback selector:**

1. Locate the process. See [“Listing and Locating Process Types” on page 2-10](#).
2. Click the process name to display the Process Type Details page.
3. In the Dynamic Client Callback Properties section, click the **Delete** link to the right of the selector value.

## Updating Security Policies

The Process Type Details page allows you to set the security policies for the process or its methods and callbacks.

**To set security policies:**


1. Locate the process to view. See [“Listing and Locating Process Types” on page 2-10](#).
2. Click the process name to display the Process Type Details page.
3. To configure the execution policy for the process:
  - a. Click **Configure Execution Policy**.
  - b. From the **Run as** drop-down list, select **caller’s identity** or **start user**.
  - c. Check or uncheck the **Single Principal Required** check box.
  - d. Click Submit to update the properties and return to the Process Type Details page.
4. To configure the authorization policies, do one or more of the following:
  - To configure the authorization policy for the process methods, click **Configure Process Authorization Policy**.
 

**Note:** If the process authorization policy is not defined, everyone is authorized.
  - To configure the authorization policy for a method, click the **Configure** link for the method.
 


**Note:** All methods in the process inherit the roles assigned in the process authorization policy. These roles cannot be removed.
  - To configure the authorization policy for a callback, click the **Configure** link for the callback.

5. Add or remove role assignments as follows:

To add roles:

- a. From the **Available Roles** list, select the required roles. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)
- b. Click the  icon to move the selected roles to the **Current Roles** list.

To remove roles:

- a. From the **Current Roles** list, select the roles to remove. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)
  - b. Click the  icon to move the selected roles to the **Available Roles** list.
6. Do one of the following:
- To update the policy, click **Submit**.  
The Process Type Details page is displayed and reflects the changes.
  - To reset to the last saved values, click **Reset**.
  - To disregard changes and return to the Process Type Details page, click **Cancel**.

## Adding or Changing Dynamic Control Selectors

The View Dynamic Controls Properties page allows you to add new or update existing selectors.

### To add or change a selector:

1. Locate the dynamic control to update. See [“Listing and Locating Dynamic Controls” on page 2-11](#).
2. Do one of the following:
  - a. Select the **Add Selector** link
  - b. Select the **Edit** link to the right of the selector value to be updated.
3. Set the properties as required. For a description of the available properties, see the topic applicable to type of dynamic control.
  - [“Defining Process Control Properties for a Selector” on page 2-23](#)
  - [“Defining Service Broker Control Properties for a Selector” on page 2-24](#)

4. Do one of the following:

- To update, click **Submit**.

The View Dynamic Controls Properties page is displayed. If you added a new selector, the value is displayed.

- To reset to the last saved values, click **Reset**.
- To disregard changes and return to the View Dynamic Controls Properties page, click **Cancel**.

## Defining Process Control Properties for a Selector

The Add New Process Control Selector and Edit Process Control Selector pages allow you to set the selector value, target URI, user name, and password alias. The following table summarizes the available settings.

Setting	Description	Required/ Optional
In the <b>Selector Value</b> field, enter the look up key.	The value used to select and dynamically set control attributes at runtime.  <b>Note:</b> This field cannot be edited on the Edit Process Control Selector page.	Required to Add
In the <b>Target URI</b> field, enter the URI for the target process.	The URI for the target process associated with this look up key.	Optional
In the <b>User Name</b> field, enter the user name.	The user name (if required) used to invoke the target process.	Optional
In the <b>Password Alias</b> field, enter the password alias.	The password alias used to look up the user password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	Optional

## Defining Service Broker Control Properties for a Selector

The Add New Service Broker Control Selector and Edit Service Broker Selector pages allow you to set the selector value and associated properties. The following table summarizes the available settings.

Setting	Description	Required/ Optional
In the <b>Selector Value</b> field, enter the look up key.	The value used to select and dynamically set control attributes at runtime.  <b>Note:</b> This field cannot be edited on the Edit Service Broker Selector page.	Required
In the <b>End Point</b> field, enter the URI for the target service.	The URI for the service end point associated with this look up key.	Optional
From the <b>Protocol</b> drop-down list, select the protocol.	Protocol to use when making the call. Valid values are <b>http-soap</b> <b>http-xml</b> <b>jms-soap</b> <b>jms-xml</b> <b>form-get</b> <b>form-post</b>  The default is <b>http-soap</b> .	Optional
Select the <b>No Dynamic Authentication, Basic Authentication, or Certificate Based Authorization</b> option button.	Type of authentication.  If client certificates are required, select <b>Certificate Based Authorization</b> and enter values in the <b>Keystore Location</b> , <b>Keystore Password Alias</b> , and <b>Keystore Type</b> fields.	Optional
In the <b>User Name</b> field, enter the user name.	The user name (if required) used to invoke the target process.	Required if <b>Basic Authentication</b>
In the <b>Password Alias</b> field, enter the password alias.	The password alias used to look up the user password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	is selected.

Setting	Description	Required/ Optional
In the <b>Client Certificate Alias</b> field, enter the certificate alias.	Certificate alias if the remote service requires SSL with two-way authentication or a digital signature.	Required if <b>Certificate Based Authorization</b> is selected.
In the <b>Client Certificate Password Alias</b> field, enter the password alias.	Password alias to look up the certificate password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	
In the <b>Keystore Location</b> field, enter the keystore location.	The keystore location.	Required if <b>Certificate Based Authorization</b> is selected.
In the <b>Keystore Password Alias</b> field, enter the password alias.	The password alias used to look up the keystore password in the password store. See <a href="#">“Password Aliases and the Password Store”</a> on page 9-6.	
In the <b>Keystore Type</b> field, enter the keystore type.	The keystore type.	

## Deleting Dynamic Control Selectors

The View Dynamic Controls Properties page allows you to delete selectors.

### To delete a selector:

1. Locate the dynamic control to update. See [“Listing and Locating Dynamic Controls”](#) on page 2-11.
2. Click the **Delete** link to the left of the selector value to be deleted.

The selector is deleted from the list.





# Process Instance Monitoring

This section provides the information you need to use the *Process Instance Monitoring* module of the WebLogic Integration Administration Console to:

- View summary statistics that reflect system health.
- View the summary or detailed status for selected instances.
- View an interactive or printable process instance graph.
- Terminate or suspend instances, resume previously suspended instances, or unfreeze frozen instances.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to make changes to process status. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The information displayed in the Process Monitoring module is based on the tracking data stored in the runtime database. A combination of system-level and process-level properties control the capture and archiving of data. To learn more about how tracking data is managed, see [“Managing Process Tracking Data” on page 2-2](#).

The following topics are provided:

- [Overview of the Process Instance Monitoring Module](#)
- [Browser Requirements for the Interactive Graph](#)
- [Viewing Instance Statistics by Process Type](#)

- [Viewing System Health Statistics](#)
- [Listing and Locating Process Instances](#)
- [Constructing an Advanced Search](#)
- [Viewing Process Instance Details](#)
- [Viewing an Interactive or Printable Process Instance Graph](#)
- [Suspending, Resuming, Terminating, or Unfreezing Process Instances](#)

## Overview of the Process Instance Monitoring Module

The following table lists the pages you can access from the Process Instance Monitoring module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
Process Instance Statistics	For each process type, the average elapsed time and a count of the number of instances in each state (running, suspended, aborted, frozen, terminated, completed, and above SLA) are displayed.	<a href="#">“Viewing Instance Statistics by Process Type” on page 3-5</a>
	Filter the list by URI or display name. Use ? to match any single character or * to match zero or more characters.	

Page	Associated Tasks	Topics
Process Instance Summary	View a list of process instances. Instance ID, display name, process label, start time, elapse time, status (running, completed, frozen, aborted, suspended), and SLA status are displayed.	<a href="#">“Listing and Locating Process Instances” on page 3-6</a>
	Filter the list by process status (for example, running, frozen, or over SLA), instance ID, or process label.	
	Access the Process Instance Details page for a selected process.	
	Set the number of instances to display per page.	
	Suspend, Resume, Terminate, or Unfreeze process instances.	<a href="#">“Suspending, Resuming, Terminating, or Unfreezing Process Instances” on page 3-14</a>
Advanced Search	Construct an advanced search using process properties such as status, begin time, elapsed time, completed time, or SLA.	<a href="#">“Constructing an Advanced Search” on page 3-8</a>
System Health	View general indicators of system health and performance trends by process type, including the process types that are taking the longest to execute, those that have not completed within SLA thresholds, and those that are failing to complete.	<a href="#">“Viewing System Health Statistics” on page 3-5</a>
Process Instance Details	View process instance properties, including variable values for the running instance, worklist tasks created by or associated with the process, and business messages associated with the process.	<a href="#">“Viewing Process Instance Details” on page 3-9</a>
	Suspend, Resume, Terminate, or Unfreeze the process instance.	<a href="#">“Suspending, Resuming, Terminating, or Unfreezing Process Instances” on page 3-14</a>
	Access an interactive or printable process graph.	<a href="#">“Viewing an Interactive or Printable Process Instance Graph” on page 3-12</a>

# Browser Requirements for the Interactive Graph

The interactive process graph requires Adobe SVG Viewer Version 3.0. You can download the viewer from the Adobe Web site (<http://www.adobe.com/svg/viewer/install/main.html>).

This viewer is not available for some configurations that WebLogic Platform 8.1 supports. The following table provides viewer availability by browser and operating system. Detailed information about the operating systems and browsers WebLogic Platform supports is provided at the following URL:

[http://edocs.bea.com/platform/docs81/support/supp\\_plat.html](http://edocs.bea.com/platform/docs81/support/supp_plat.html)

Browser	Operating System	Adobe SVG Viewer 3.0 Availability
Microsoft Internet Explorer 6.x	Windows	Viewer is available from Adobe.
Netscape 7.0x	Windows	Requires a workaround. See “ <a href="#">Using Adobe SVG Viewer with Netscape 7.0 on Windows.</a> ”
	Solaris	3.0 beta 1 version of viewer available from <a href="http://www.adobe.com/svg/viewer/install/old.html">http://www.adobe.com/svg/viewer/install/old.html</a>
	Linux	3.0 beta 1 version of viewer available from <a href="http://www.adobe.com/svg/viewer/install/old.html">http://www.adobe.com/svg/viewer/install/old.html</a>
	HP-UX	Viewer is not available from Adobe.
	AIX	Viewer is not available from Adobe.
Mozilla 1.x	Linux	Viewer is not available from Adobe.

## Using Adobe SVG Viewer with Netscape 7.0 on Windows

Before viewing an interactive process graph in Netscape 7.0 on Windows, you must install Version 3.0 of the Adobe SVG Viewer as described in the following procedure.

### To install the Adobe SVG Viewer with Netscape 7.0:







1. Download version 3.0 of the viewer.
2. Close Netscape.
3. Install the viewer.

4. Copy `NPSVG3.dll` from the viewer installation directory to your Netscape Plugins folder. For example, copy the file from `C:\WINNT\system32\Adobe\SVG Viewer 3.0` to `C:\Program Files\Netscape\Netscape\Plugins`.

## Viewing Instance Statistics by Process Type

The Process Instance Statistics page lists the display name and average elapsed time for each process type. It also provides a count of the number of instances in each state (running, suspended, aborted, frozen, terminated, completed, and SLA exceeded). The counts are based on tracking data stored in the runtime database and do not include process data that has been purged.

### To view the process instance statistics:

1. From the home page, select the **Process Instance Monitoring** module.
2. To locate a specific process, do one of the following:
  - Filter by display name or URI. Enter the search target, then click **URI or Name**. The processes matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.
3. To view additional information about the instances of a selected type, select the process display name. To view additional information about the instances of a selected type that are in a specific state, select the number. The Process Instance Summary page displays only those instances that match the selection. See [“Listing and Locating Process Instances” on page 3-6](#).

## Viewing System Health Statistics

The System Health page provides a overview of system health. The following indicators are displayed:

- *Highest Average Elapsed Time Since Last Purge*  
Process types with the highest average elapsed time are displayed.
- *Worst SLA Performance Since Last Purge*  
Process types with the worst SLA performance are displayed.

- *Lowest Success Rate Since Last Purge*

Process types with the highest rate of aborted, terminated, or frozen instances are displayed.

For each of the above:

- If any of the instances started in the last 24 hours, the process is also displayed in the **Last 24 Hours** column.
- If any of the process types have running instances, the process is displayed in the **Active instances** column.

Each process name displayed on the page is a link to the Process Instance Summary page for the process type.

**To view the system health statistics:**



1. From the home page, select the **Process Instance Monitoring** module.
2. From the left panel, select **System Health**.

## Listing and Locating Process Instances

The Process Instance Summary page displays the following information for each process instance. For a more detailed description of the properties, see [“Viewing Process Instance Details” on page 3-9](#).

**Note:** The process instances are sorted by start time, most recent first.

Property	Description
ID	Process Instance ID. This is a link to the Process Instance Detail page. See <a href="#">“Viewing Process Instance Details” on page 3-9</a> .
Display name	Display name assigned to the process. If more than one version of the process is deployed, the version number is appended.
Process Label	Label for the process instance. The label is generated for each instance and typically reflects a value specific to the instance. For example, an order number, customer number, DUNS number, or some other value of use in auditing. To learn more about how the process label is set, see the <a href="#">JpdContext Interface</a> in <i>Building Integration Applications</i> in the WebLogic Workshop help.
Start Time	Time this instance started.

Property	Description
Elapsed Time	Time elapsed since instance start.
Status	The current state of the instance (Running, Completed, Suspended, Terminated, Frozen, Aborted).
SLA status	<p>If service level agreements are set, this field displays the current status:</p> <ul style="list-style-type: none"> <li>• If the elapsed time exceeds the SLA warning threshold, a warning  is displayed. The warning is followed by the time remaining until the SLA threshold is reached.</li> <li>• If the elapsed time exceeds the SLA, a red flag  is displayed. The red flag is followed by the time elapsed since the SLA was reached.</li> </ul>

### To list and locate process types:

1. From the home page, select the **Process Instance Monitoring** module.
2. In the left panel, click **View All**.

**Note:** By default, 50 entries are displayed on the page. To set this to a new value, enter the number of entries then click **Page Size**.

3. To locate a specific process, do one of the following:
  - Select a default filter from the **Go** drop-down list. The following options are available:





[All Instances](#)  
[Running Instances](#)  
[Aborted Instances](#)  
[Suspended Instances](#)  
[Frozen Instances](#)  
[Completed Instances](#)  
[Terminated Instances](#)  
[Instances Over SLA](#)  
[Instances Over SLA Warning](#)

- Filter by instance ID. Enter the required instance ID, then click **Instance ID**. The instance identified is displayed.

**Note:** Only the exact match is displayed. Do not use wildcards.

- Filter by Process Label. Enter the search target, then click **Process Label**. Instances with a label that contains the search target are displayed.

**Note:** This is a containment query. Do not use wildcards.

- Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.
- Use the advanced search page. See [“Constructing an Advanced Search” on page 3-8](#).

# Constructing an Advanced Search

The Advanced Search page allows you to construct a complex process instance search. The following table summarizes the available search criteria.

Setting	Description
From the <b>Service URI</b> drop-down list, select the Service URI.	Select from a list of the process types deployed. The default is <b>Any</b> .
From the <b>Status</b> drop-down list, select a the status.	Specify the process status ( <b>Any</b> , <b>Running</b> , <b>Completed</b> , <b>Terminated</b> , <b>Suspended</b> , <b>Aborted</b> , <b>Frozen</b> )
From the <b>Started Between</b> drop-down lists, select the target range.	Specify the target time period. The search returns process instances started during the period that also match the other specified criteria.
From the <b>Completed Between</b> drop-down lists, select the target range.	Specify the target time period. The search returns process instances that completed, terminated, aborted, or froze during the specified period that also match the other specified criteria.
From the <b>Elapsed Time Between</b> drop-down lists, select the target range.	Specify the low and high elapsed time in seconds, minutes, hours, or days. The search returns the process instances with an elapsed time within the range that also match the other specified criteria.
Select the appropriate <b>SLA Status</b> option button.	Specify one of the following options: <b>Any</b> <b>Exceeded SLA</b> <b>Exceeded SLA or SLA Warning Threshold</b> <b>Exceeded SLA Warning Threshold, but not SLA</b>



Setting	Description
In the <b>Label Contains</b> field, enter the target search string.	Specify a search target. The search returns processes instances with a label that contains the search target that also match the other specified criteria.  <b>Note:</b> This is a containment query. Do not use wildcards.
From the <b>Display First</b> drop-down list, select the number of matching process instances to retrieve.	Specify the number of process instances to be returned in the results set.

## Viewing Process Instance Details

The Process Instance Detail page allows you to:

- View process properties.
- View an interactive or printable process graph.
- Suspend, Resume, Terminate, or Unfreeze a process.

### To view process instance details:

1. Locate the process. See [“Listing and Locating Process Instances” on page 3-6](#).
2. Click the process ID to display the Process Instance Details page.
3. To view an interactive or printable process graph, click **Graphical View** or **Printable Graph**.

**Note:** Your browser must meet certain requirements to view the interactive graph. See [“Browser Requirements for the Interactive Graph” on page 3-4](#). To learn more about the interactive process view, see [“Viewing an Interactive or Printable Process Instance Graph” on page 3-12](#).

The following table summarizes the information displayed on the Process Instance Detail page.

Property	Description
Instance ID	Process instance ID.
Service URI	The process URI. If there are multiple versions of the process, a version number is appended.

Property	Description
Status	Current status of the process.
	<b>Running</b> The process is running.
	<b>Completed</b> The process finished.
	<b>Suspended</b> The process was suspended.
	<b>Terminated</b> The process was terminated.
	<b>Aborted</b> The process threw an unhandled exception. Aborted processes can only be terminated.
	<b>Frozen</b> The process failed but can be unfrozen. When a process is unfrozen, it resumes from the point where it failed. See <a href="#">“Suspending, Resuming, Terminating, or Unfreezing Process Instances” on page 3-14.</a>  Processes can be designed to freeze, rather than abort, by setting freeze on failure to true. To learn more see “Setting the Business Process Properties” in <a href="#">Designing Your Application in Building Integration Applications.</a>
Start Time	Time this instance started.
Exception	Exception content for a aborted or frozen instance.
Elapsed Time	Time elapsed since instance start.
Completion Time	Completion date and time for a completed process.
Termination Time	Termination date and time for a process that has been terminated.
SLA Status	<p>If no service level agreements are set, Not Applicable is displayed.</p> <p>If service level agreements are set, this field displays the current status:</p> <ul style="list-style-type: none"> <li>• If the elapsed time does not exceed the SLA, Not exceeded is displayed.</li> <li>• If the elapsed time exceeds the SLA Warning threshold, the time remaining until the SLA threshold is reached is displayed.</li> <li>• If the elapsed time exceeds the SLA, the time elapsed time since the SLA was reached is displayed.</li> </ul> <p>To learn more about the SLA, see <a href="#">“Service Level Agreements” on page 2-5.</a></p>

Property	Description
Pending Activities	<p>Pending <code>controlReceive</code> or <code>clientRequest</code> methods.</p> <p>For example:</p> <ul style="list-style-type: none"> <li><code>waitClientRequest[conditionalWaitClientRequest]</code> is displayed when the instance is waiting for the following:  <code>&lt;clientRequest name="conditionalWaitClientRequest" method="waitClientRequest" /&gt;</code></li> <li><code>t1_onTimeout</code> is displayed when the instance is waiting for the following:  <code>&lt;controlReceive method="t1_onTimeout" /&gt;</code></li> </ul>
Process Label	<p>Label for the process instance. The label is generated for each instance and typically reflects a value specific to the instance. For example, an order number, customer number, DUNS number, or some other value of use in auditing. To learn more about how the process label is set, see the <a href="#">JpdContext Interface</a> in <i>Building Integration Applications</i> in the WebLogic Workshop help.</p>
Tasks created by this instance	<p>Worklist tasks created by the instance. The task name and ID are displayed. The ID is a link to the Worklist Task Details page.</p>
Tasks this instance is listening to	<p>Worklist tasks this process is listening to. The task name and ID are displayed. The ID is a link to the Worklist Task Details page.</p>
B2B Events	<p>Summary information for any business messages are displayed. The event ID, direction (inbound or outbound), and trading partners (from and to) are displayed. The event ID is a link to the message detail.</p>
Variables	<p>Name, type, and value of each variable defined for the instance. Variables are displayed only for running instances. You can view the value of an XML or string variable by clicking it.</p>

# Viewing an Interactive or Printable Process Instance Graph

The Process Instance Details page allows you to view an interactive or printable graph of the process instance. The graph represents your business process and its interactions with clients and resources, such as databases, JMS queues, and file systems.

The interactive instance graph is a fully expanded version of the view provided in the Workshop Design View. Visual cues are provided to indicate node status as described in the following table:

If the node . . .	And the tracking level is . .	The node appears . . .
Has been visited	Full or Node	Normal
	Minimum	Normal
Is currently executing	Full or Node	Highlighted
	Minimum	Highlighted
Has not been visited	Full or Node	Dimmed
	Minimum	Normal

The information displayed is dependent on tracking level and current state of the process.

The top panel displays selected process properties. To learn more about the properties displayed, see [“Viewing Process Instance Details” on page 3-9](#). In addition to the properties, the commands applicable to the current state of the instance (terminate, suspend, resume, or unfreeze) are provided in the top panel. See [“Suspending, Resuming, Terminating, or Unfreezing Process Instances” on page 3-14](#).

When you click on a node, the node name and type are displayed. If the tracking level is set to Full or Node, the start time, elapsed time, finish time, completed visits, and description are also displayed. If the tracking level is set to Minimum, this additional information is only available for the currently executing node.

## To view a printable graph for a process instance:

1. Locate the process instance to view. See [“Listing and Locating Process Instances” on page 3-6](#).
2. Click the process name to display the Process Instance Details page.

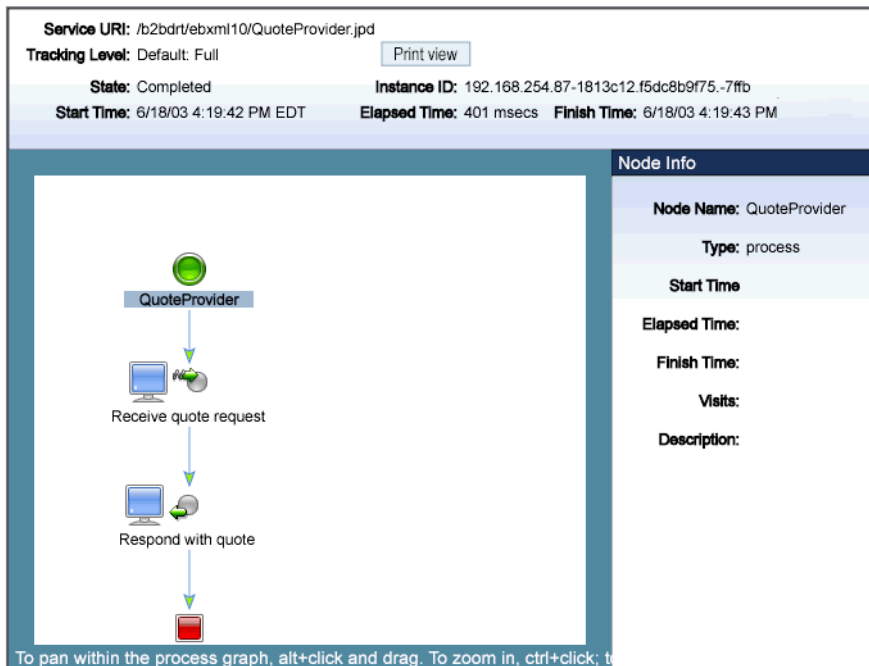
3. Click **Printable Graph**.

The process graph is displayed as a PDF document.




**To view the interactive graph for a process instance:**

1. Verify that your browser meets the requirements. See “[Browser Requirements for the Interactive Graph](#)” on page 3-4.
2. Locate the process instance to view. See “[Listing and Locating Process Instances](#)” on page 3-6.
3. Click the process name to display the Process Instance Details page.
4. Click **Graphical View**.

The Adobe SVG Viewer displays the interactive view.



5. Do any of the following:
  - To display node status, click the node image. The properties displayed are dependent on the tracking level set.

- To scroll the view, press and hold down the **Alt** key. The cursor changes to a hand  tool. Click and drag to scroll the process graph vertically or horizontally.
- To zoom in, press and hold down the **Ctrl** key. The cursor changes to a zoom in  tool. Click to zoom in.
- To zoom out, press and hold down the **Ctrl+Shift** keys. The cursor changes to a zoom out  tool. Click to zoom out.
- To change to a printable view, click **Print View**. The process graph is displayed as a PDF document.

# Suspending, Resuming, Terminating, or Unfreezing Process Instances

Depending on the current state of a process instance, you can suspend, resume, terminate, or unfreeze it. The following table summarizes the available actions by instance state:

Instance State	Available Actions
Running	Suspend, Terminate
Suspended	Resume, Terminate
Frozen	Terminate, Unfreeze
Aborted	Terminate

When you terminate a process, the operation in progress finishes, then the process completes without executing subsequent nodes.

A process can be designed to freeze, rather than abort, when it encounters an unhandled exception, by setting the freeze on failure property to true. To learn more see “Setting the Business Process Properties” in [Designing Your Application](#) in *Building Integration Applications*. This capability is useful for handling an exception due to a network outage, unavailable EIS, or other such transitory condition. When you unfreeze a process, if the condition that led the failure is still in effect, the process returns to the frozen state.

You can suspend, resume, terminate, or unfreeze an instance in the following contexts:

- Process Instance Detail page
- Process Instance Summary page
- Interactive Process Instance Graph

### **To suspend, resume, terminate, or unfreeze an instance from the Process Instance Details page:**

1. Locate the process. See [“Listing and Locating Process Instances” on page 3-6](#).
2. Click the process name to display the Process Instance Details page.
3. Click **Suspend**, **Resume**, **Terminate**, or **Unfreeze**, as required.  
A confirmation dialog box is displayed.
4. Click **OK** to confirm, or **Cancel** to dismiss the dialog and cancel the action.

### **To suspend, resume, terminate, or unfreeze one or more instances from the Process Instance Summary page:**

1. Display the Process Instance Summary page as described in [“Listing and Locating Process Instances” on page 3-6](#).
2. Click the check box to the left of each instance to be suspended, resumed, terminated, or unfrozen.
3. Click **Suspend**, **Resume**, **Terminate**, or **Unfreeze**.  
A confirmation dialog box is displayed.
4. Click **OK** to confirm, or **Cancel** to dismiss the dialog and cancel the action.

### **To suspend, resume, terminate, or unfreeze an instance from the Interactive Process Graph:**

1. Locate the process. See [“Listing and Locating Process Instances” on page 3-6](#).
2. Click the process name to display the Process Instance Details page.
3. Click **Graphical View**.
4. In the top panel of the interactive graph, click **Suspend**, **Resume**, **Terminate**, or **Unfreeze**, as required.  
A confirmation dialog box is displayed.

5. Click **OK** to confirm, or **Cancel** to dismiss the dialog and cancel the action.



# Message Broker

This section provides the information you need to use the *Message Broker* module of the WebLogic Integration Administration Console to:

- View a list of channels, with the number of subscribers and processed messages for each.
- View channel properties and set channel security policies.
- View the subscribers to a channel and quickly access a list of the subscriber process instances.
- View channel summary statistics (number of active channels, subscribed channels, and dead letter count).
- Reset the message counter.

**Note:** You must be logged in as a member of the Administrators or IntegrationAdministrators group to modify channel security policies. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About Message Broker Channels](#)
- [Overview of the Message Broker Module](#)
- [Viewing and Resetting Message Counts](#)
- [Listing and Locating Channels](#)
- [Viewing Channel Details and Subscriptions](#)

- [Setting Channel Security Policies](#)

## About Message Broker Channels

A Message Broker channel has similar properties to a Java Message Service (JMS) topic, but is optimized for use with WebLogic Integration processes, controls, and event generators. Within a WebLogic Integration application:

- Message Broker Publish controls are used by process or web service instances to publish messages to a Message Broker channel.
- Event generators that receive outside events route them as messages to a Message Broker channel.
- Subscription start nodes start processes upon receipt of a message from a Message Broker channel. This constitutes a static subscription to the channel.
- Message Broker Subscription controls are used by process or web service instances to receive messages from a Message Broker channel. This constitutes a dynamic subscription to the channel.

Publishers to a Message Broker channel can pass message metadata with the message. This metadata can be received by the subscriber as a parameter.

Channel files define the channels available in a deployed application. To restrict the messages routed to static or dynamic subscribers, XQuery filters can be applied against message metadata or message body (if the type is XmlObject). All subscribers registered to receive a message on a channel receive the message, subject to any filters they have set up. To learn more about defining channels, publishing or subscribing to channels, and creating subscription filters, see [Publishing and Subscribing to Channels](#) in *Building Integration Applications* in the WebLogic Workshop help.

## Overview of the Message Broker Module

The following table lists the pages you can access from the Message Broker module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
Channel Summary List	View a list of channels. Channel name, message type, number of subscribers, message count, and dead letter count are displayed.  Filter the list by channel name. Use ? to match any single character or * to match zero or more characters.	<a href="#">“Listing and Locating Channels” on page 4-4</a>
View Channel Details	View channel properties. Channel name, message type (xml, rawData, string, or none), number of subscribers, message count, dead letter count, security policies (publish roles, subscribe roles, and ‘dispatch as’ principal) and subscription rules are displayed. You can access the process details for a subscriber from this page.	<a href="#">“Viewing Channel Details and Subscriptions” on page 4-5</a>
Edit Channel Subscribe and Publish Properties	View and set the publish roles, subscribe roles, and ‘dispatch as’ principal defined for the channel.	<a href="#">“Setting Channel Security Policies” on page 4-6</a>
View Message Broker Statistics	View summary statistics, including number of active channels, subscribed channels, message count, dead letter count, and time of last reset.  Reset the counts (published messages and dead letter).	<a href="#">“Viewing and Resetting Message Counts” on page 4-7</a>

## Listing and Locating Channels

The Channel Summary List displays the channel name, type (xml, rawData, string, or none), number of subscribers, message count, and dead letter count for each channel.

### To list and locate channels:

1. From the home page, select the **Message Broker** module to display the Channel Summary List.
2. To locate a specific channel, do one of the following:
  - Filter by name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Search**. The channels matching the search criteria are displayed.
  - Note:** If the **Search** field is empty, all entries are returned.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the arrow to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◄, first |◄, or last ►| page.

## Viewing Channel Details and Subscriptions

The View Channel Details page displays the properties described in the following table.

Property	Description	Administrator Can Set (Yes/No)
Channel Name	<p>The name of the channel as defined in the channel file. For example, <code>/myproject/mygroup/mytype/mychannel</code> is displayed for the following:</p> <pre> &lt;channels xmlns="http://www.bea.com/wli/broker/channelfile"   xmlns:foo="http://www.foo.com/bar"   xmlns:fooMeta="http://www.foo.com/barMeta"   channelPrefix="/myproject"&gt;   &lt;channel name="mygroup" messageType="none"&gt;     &lt;channel name="mytype" messageType="none"&gt;       &lt;channel name="mychannel" messageType="xml"&gt;         &lt;/channel&gt;       &lt;/channel&gt;     &lt;/channel&gt;   &lt;/channel&gt; </pre>	No
Message Type	The message type set for the channel (xml, rawData, or string). The field is empty if the type is set to none.	No
Number of Subscribers	The number of processes or web services currently subscribed to the channel.	No
Message Count	The number of messages delivered to this channel.	No
Publish Roles	The roles authorized to publish to this channel. If no roles are defined, everyone is authorized.	Yes
Subscribe Roles	The roles authorized to subscribe to this channel. If no roles are defined, everyone is authorized.	Yes
Dispatch As	The user under which messages are dispatched to subscribers. If no user is specified, messages are dispatched as Anonymous.	Yes

Property		Description	Administrator Can Set (Yes/No)
Subscription Rules	Control Name	For dynamic subscriptions, the Message Broker Subscription control name.	No
	Filter Value	For subscriptions with filters, the filter value that must match the results of applying the filter to the message.  For static subscriptions, if a filter is set but the filter value is null, the subscriber only requires that the filter be satisfied and does not care about the specific results of evaluating the filter.  For dynamic subscriptions, if a filter is set, but the filter value is null, the filter value is not specified as part of the subscription, but rather may be specified with each instance.	No
	Subscriber URI	The URI of the subscriber. For processes, this URI is a link to the Process Instance Summary page.	No

### To view channel properties:

1. Locate the channel. See [“Listing and Locating Channels” on page 4-4](#).
2. Click the channel name to display the View Channel Details page.

## Setting Channel Security Policies

The Edit Channel Subscribe and Publish Policies page allows you to set the following channel properties:


- *Publish Roles*  
The roles authorized to publish to the channel.
- *Subscribe Roles*  
The roles authorized to subscribe to the channel.
- *Dispatch As*  
The user under which messages are dispatched to subscribers.

**Note:** If the publish and subscribe roles are not defined, everyone is authorized. If the dispatch as user is not defined, messages are dispatched as anonymous.


**To update channel publish and subscribe policies:**

1. Locate the channel. See [“Listing and Locating Channels” on page 4-4](#).
2. Click the channel name to display the View Channel Details page.
3. Click **Edit Security Details**.
4. Add or remove Publish Roles or Subscribe Roles as follows:
 

To add roles:

  - a. From the **Available Roles** list, select the required roles. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)
  - b. Click the  icon to move the selected roles to the **Current Roles** list.

To remove roles:

  - a. From the **Current Roles** list, select the required roles. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)
  - b. Click the  icon to move the selected roles to the **Available Roles** list.
5. From the **Dispatch As** drop-down list, select a valid user name.
 

**Note:** If no user is specified, messages are dispatched as anonymous.
6. Do one of the following:
  - To update the policies, click **Submit**.  
The View Channel Details page is displayed.
  - To disregard changes and return to the View Channel Details page, click **Cancel**.

## Viewing and Resetting Message Counts

The View Message Broker Statistics page displays the following:

Statistic	Description
Number of Active Channels	Number of channels available.
Number of Subscribed Channels	Number of channels that have one or more subscribers.

Statistic	Description
Dead Letter Count	When the Message Broker is unable to determine the URI to send a message to (that is, no subscribers are found), the message is sent to the <code>mb.dead.letter.queue</code> queue. The Dead Letter Count reflects the number of messages sent to the dead letter queue since the count was last reset.
Message Count	Messages published since the count was last reset.
Time of last reset	Time the message count was last reset.

### To view Message Broker statistics:

1. From the home page, select the **Message Broker** module.
2. From the left panel, select **View Statistics** to display the View Message Broker Statistics page.

### To reset the message counts:

1. From the home page, select the **Message Broker** module.
2. From the left panel, select **View Statistics** to display the View Message Broker Statistics page.
3. Click **Reset All**.



# Event Generators

This section provides the information you need to use the *Event Generator* module of the WebLogic Integration Administration Console to:

- Create and deploy new JMS, Email, File, and Timer event generators.
- Add channel rules to existing JMS, Email, File, and Timer event generators.
- Reset the read and error counters.
- Suspend and resume deployed event generators.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to create, change, or delete event generators. See [“Default Groups, Roles, and Security Policies”](#) on page 10-3.

The following topics are provided:

- [About the Event Generators](#)
- [Overview of the Event Generator Module](#)
- [Creating and Deploying Event Generators](#)
- [Defining Channel Rules for a File Event Generator](#)
- [Defining Channel Rules for an Email Event Generator](#)
- [Defining Channel Rules for a JMS Event Generator](#)
- [Defining Channel Rules for a Timer Event Generator](#)

- [Listing and Locating Event Generators](#)
- [Viewing and Updating Event Generator Channel Rules](#)
- [Suspending and Resuming Event Generators](#)
- [Resetting the Counters](#)
- [Deleting Channel Rules](#)
- [Deleting Event Generators](#)

## About the Event Generators

Event generators publish messages to Message Broker channels in response to system events (for example, files arriving in a directory, or messages arriving in an email account or JMS queue). The following event generators can be created from the WebLogic Integration Administration Console:

- *File event generator*  
Polls for files in file systems (local directory or ftp server) and publishes the files to Message Broker channels. File pattern matching, as well as other handling criteria, are specified in the channel rules for the event generator.
- *Email event generator*  
Polls for messages in email accounts and publishes the messages to Message Broker channels. Handling criteria are specified in the channel rules defined for the event generator.
- *JMS event generator*  
Polls for messages on JMS queues or topics and publishes the messages to Message Broker channels. Filters (message selectors) can be defined to control which messages are picked up from the JMS queue or topic. Property name and value matching, as well as other handling criteria specified in the channel rules, control which messages are published.
- *Timer event generator*  
Creates events at user designated times and publishes the events to Message Broker channels. When the Timer event generator detects that a designated time has passed, it publishes a message to a Message Broker channel. The message content can be specified in the channel rules defined for the event generator.

A set of channel rules is configured for each event generator. For a JMS event generator, the rules are applied to incoming JMS messages in the user-designated order. For example, suppose the following rules are configured for a JMS event generator:

Channel	Property	Value
myapp/orders/AllOrders	VendorId	
myapp/orders/ACMEOrders	VendorId	ACME Trading Corp

In this case, a message with a JMS header property “VendorId” set to “ACME Trading Corp” would be posted to the myapp/orders/AllOrders channel because the presence of the “VendorId property triggers the first rule. The order must be reversed to achieve the desired result.

Channel	Property	Value
myapp/orders/ACMEOrders	VendorId	ACME Trading Corp
myapp/orders/AllOrders	VendorId	

Now a message with a JMS header property “VendorId” set to “ACME Trading Corp” is properly posted to the myapp/orders/ACMEOrders channel.

Channel rule sequence is only significant for JMS event generators. The sequence is not significant for Email or File event generators.

## Overview of the Event Generator Module

The following table lists the pages you can access from the Event Generator module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
<b>File</b>		
View All File Event Generators	View a list of File event generators. Generator name, number of channels, files read, last reset time, number of errors, error reset time, and status (running or suspended) are displayed.	<a href="#">“Listing and Locating Event Generators” on page 5-17</a>
	Filter the list by generator name. Use ? to match any single character or * to match zero or more characters.	
	Suspend or resume the event generator.	<a href="#">“Suspending and Resuming Event Generators” on page 5-19</a>
	Reset the files read or error count.	<a href="#">“Resetting the Counters” on page 5-20</a>
	Delete one or more event generators.	<a href="#">“Deleting Event Generators” on page 5-21</a>
Create New File Event Generator	Create and deploy a File event generator. The event generator initially has no channel rules.	<a href="#">“Creating and Deploying Event Generators” on page 5-8</a>
File Event Generator Definition	Access the File Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	<a href="#">“Defining Channel Rules for a File Event Generator” on page 5-10</a>
	View the channel rules for an existing event generator. Select a channel rule to view details.	<a href="#">“Viewing and Updating Event Generator Channel Rules” on page 5-18</a>
	Delete one or more channel rules.	<a href="#">“Deleting Channel Rules” on page 5-21</a>

Page	Associated Tasks	Topics
File Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	<a href="#">“Defining Channel Rules for a File Event Generator” on page 5-10</a>
<b>Email</b>		
View All Email Event Generators	View a list of Email event generators. Generator name, number of channels, emails read, last reset time, number of errors, error reset time, and status (running or suspended) are displayed.	<a href="#">“Listing and Locating Event Generators” on page 5-17</a>
	Filter the list by generator name. Use ? to match any single character or * to match zero or more characters.	
	Suspend or resume the event generator.	<a href="#">“Suspending and Resuming Event Generators” on page 5-19</a>
	Reset the emails read or error count.	<a href="#">“Resetting the Counters” on page 5-20</a>
	Delete one or more event generators.	<a href="#">“Deleting Event Generators” on page 5-21</a>
Create New Email Event Generator	Create and deploy an Email event generator. The event generator initially has no channel rules.	<a href="#">“Creating and Deploying Event Generators” on page 5-8</a>
File Event Generator Definition	Access the Email Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	<a href="#">“Defining Channel Rules for an Email Event Generator” on page 5-12</a>
	View the channel rules for an existing event generator. Select a channel rule to view details.	<a href="#">“Viewing and Updating Event Generator Channel Rules” on page 5-18</a>
	Delete one or more channel rules.	<a href="#">“Deleting Channel Rules” on page 5-21</a>
Email Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	<a href="#">“Defining Channel Rules for an Email Event Generator” on page 5-12</a>

Page	Associated Tasks	Topics
<b>JMS</b>		
View All JMS Event Generators	View a list of JMS event generators. Generator name, number of channels, messages read, last reset time, number of errors, error reset time, and status (running or suspended) are displayed.	<a href="#">“Listing and Locating Event Generators” on page 5-17</a>
	Filter the list by generator name. Use ? to match any single character or * to match zero or more characters.	
	Suspend or resume the event generator.	<a href="#">“Suspending and Resuming Event Generators” on page 5-19</a>
	Reset the messages read or error count.	<a href="#">“Resetting the Counters” on page 5-20</a>
	Delete one or more event generators.	<a href="#">“Deleting Event Generators” on page 5-21</a>
Create New JMS Event Generator	Create and deploy a JMS event generator. When you create the generator, you specify the destination topic or queue, message selector, a default channel rule.	<a href="#">“Creating and Deploying Event Generators” on page 5-8</a>
JMS Event Generator Details	Update the default channel rule for the event generator.	<a href="#">“Viewing and Updating Event Generator Channel Rules” on page 5-18</a>
JMS Event Generator Definition	Access the JMS Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	<a href="#">“Defining Channel Rules for a JMS Event Generator” on page 5-15</a>
	View the channel rules for an existing event generator. Select a channel rule to view details.	<a href="#">“Viewing and Updating Event Generator Channel Rules” on page 5-18</a>
	Delete one or more channel rules.	<a href="#">“Deleting Channel Rules” on page 5-21</a>
JMS Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	<a href="#">“Defining Channel Rules for a JMS Event Generator” on page 5-15</a>

Page	Associated Tasks	Topics
<b>Timer</b>		
View All Timer Event Generators	View a list of Timer event generators. Generator name, number of channels, messages read, last reset time, number of errors, error reset time, and status (running or suspended) are displayed.	<a href="#">“Listing and Locating Event Generators” on page 5-17</a>
	Filter the list by generator name. Use ? to match any single character or * to match zero or more characters.	
	Suspend or resume the event generator.	<a href="#">“Suspending and Resuming Event Generators” on page 5-19</a>
	Reset the messages read or error count.	<a href="#">“Resetting the Counters” on page 5-20</a>
	Delete one or more event generators.	<a href="#">“Deleting Event Generators” on page 5-21</a>
Create New Timer Event Generator	Create and deploy a Timer event generator. The event generator initially has no channel rules.	<a href="#">“Creating and Deploying Event Generators” on page 5-8</a>
Timer Event Generator Definition	Access the Timer Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	<a href="#">“Defining Channel Rules for a Timer Event Generator” on page 5-16</a>
	View the channel rules for an existing event generator. Select a channel rule to view details.	<a href="#">“Viewing and Updating Event Generator Channel Rules” on page 5-18</a>
	Delete one or more channel rules.	<a href="#">“Deleting Channel Rules” on page 5-21</a>
Timer Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	<a href="#">“Defining Channel Rules for a Timer Event Generator” on page 5-16</a>

## Creating and Deploying Event Generators

The Event Generator module allows you to create and deploy File, Email, JMS, or Timer event generators. When you create a new event generator, it is packaged and deployed as an EJB. Once the event generator has been created, you can suspend, resume, or add additional channel rules as required.

### To create and deploy a JMS event generator:


1. From the home page, select the **Event Generator** module.
2. From the left panel, select **JMS**.
3. Select **Create New**.
4. In the **Generator Name** field, enter a unique name for the event generator.  
**Note:** Names are not case sensitive. Leading or trailing spaces are removed.
5. From the **Destination Type** drop-down list, select **javax.jms.queue** or **javax.jms.topic**.
6. From the **Destination JNDI Name** drop-down list, select the JNDI name for the topic or queue.
7. In the **Message Selector** field, specify the JMS message selector. See [http://java.sun.com/dtd/ejb-jar\\_2\\_0.dtd](http://java.sun.com/dtd/ejb-jar_2_0.dtd).
8. From the **Default Rule Channel** drop-down list, select the default channel. Messages that do not match any other channel rule are published to this channel.
9. Click **Submit** to create and deploy the event generator.

The Event Generator Definition page is displayed.

**Note:** The event generator is created and deployed without channel rules, therefore, the first task is to define channel rules for the generator.

10. Select **Define a New Channel Rule**.
11. Set the properties as required. see “[Defining Channel Rules for a JMS Event Generator](#)” on [page 5-15](#)
12. Click **Submit** to add the channel rule to the event generator.
13. If required, repeat steps 10 to 12 to add additional channels.




14. If multiple rules are defined, you can reorder them as required. Click the up or down arrow  button to move entries up or down the list. Changes take effect immediately.

**To create and deploy a File, Email, or Timer event generator:**

1. From the home page, select the **Event Generator** module.
2. From the left panel, select the type of event generator (**File**, **Email**, or **Timer**).
3. Select **Create New**.
4. In the **Generator Name** field, enter a unique name for the event generator.
5. Click **Submit** to create and deploy the event generator.

The Event Generator Definition page is displayed.

**Note:** The event generator is created and deployed without channel rules, therefore, the first task is to define channel rules for the generator.

6. Select **Define a New Channel Rule**.
7. Set the properties as required. For a description of the available properties, see the topic applicable to the event generator you are creating:
  - [“Defining Channel Rules for a File Event Generator” on page 5-10](#)
  - [“Defining Channel Rules for an Email Event Generator” on page 5-12](#)
  - [“Defining Channel Rules for a Timer Event Generator” on page 5-16](#)
8. Click **Submit** to add the channel rule to the event generator.
9. If required, repeat steps 6 to 8 to add additional channels.
10. If multiple rules are defined, you can reorder them. Click the up or down arrow  button to move entries up or down the list. Changes take effect immediately.

**Note:** This functionality is provided for convenience only. Channel rule sequence is not functionally significant for Email or File event generators.

## Defining Channel Rules for a File Event Generator

The File Generator Channel Rule Definition page allows you to define the properties for the channel rule. The following table summarizes the available settings.

Setting	Description	Required/ Optional
From the <b>File Type</b> drop-down list, select <b>Disk File</b> or <b>FTP</b> .	Type of file event.	Required
From the <b>Channel</b> drop-down list, select a Message Broker channel.	The name of the Message Broker channel to which messages matching the configured criteria are published.	Required
In the <b>Message Encoding</b> field, enter the name of the character set if other than the default.  <b>Note:</b> This property can only be set if the message broker channel type is string.	The character set if other than the default. This property applies only if the selected <b>Channel</b> is of type string. See <a href="http://www.iana.org/assignments/character-sets">http://www.iana.org/assignments/character-sets</a> for valid values.	Optional
In the <b>FTP Host Location</b> field, enter the FTP server.	Location of the FTP server (IP Address or host name) if the <b>File Type</b> is set to <b>FTP</b> .	Required if the <b>File Type</b> is set to <b>FTP</b>
In the <b>FTP User Name</b> field, enter the name.	Name required to access the FTP account.	Required if the <b>File Type</b> is set to <b>FTP</b>
Do one of the following to specify the <b>FTP User Password</b> : <ul style="list-style-type: none"> <li>Select the <b>Use Alias</b> option button, then select the password alias from the drop-down list.</li> <li>Select the <b>Use Value</b> option button, then enter the password in the field.</li> </ul>	If you enter the password in the <b>Use Value</b> field, it is stored in clear text in the event generator configuration file. To secure the password, add it to the password store. See “ <a href="#">Password Aliases and the Password Store</a> ” on page 9-6. After the alias has been added to the password store, it is available for selection from the <b>Use Alias</b> drop-down list.	Required if the <b>File Type</b> is set to <b>FTP</b>

Setting	Description	Required/ Optional
In the <b>FTP Local Directory field</b> , enter the path.	Specifies the path to a directory to which files from the FTP server are copied.	Required if the <b>File Type</b> is set to <b>FTP</b>
In the <b>Directory</b> field, enter a valid path.	<p>If <b>File Type</b> is set to <b>Disk</b>, specifies the path to the directory to poll for files.</p> <p>If <b>File Type</b> is set to <b>FTP</b>, specifies the path on the FTP server to poll for files.</p>	Required
From the <b>Pass by filename</b> drop-down list, select <b>Yes</b> or <b>No</b> .	<p>If set to <b>Yes</b>, the file is staged to the Archive directory, and is passed as reference in the FileControlPropertiesDocument sent as the payload of the message. If set to <b>Yes</b>, you must specify an Archive directory.</p> <p>The default is <b>No</b>.</p>	Required
From the <b>Scan Subdirectories</b> drop-down list, select <b>Yes</b> or <b>No</b> .	Specifies whether or not subdirectories are to be scanned.	Optional
In the <b>File Pattern</b> field, enter the pattern.	Optional pattern to filter on. Use ? to match any single character or * to match zero or more characters.	Optional
From the <b>Sort by Arrival</b> field, select <b>Yes</b> or <b>No</b> .	<p>If set to <b>Yes</b>, the files are sorted by arrival time. This maintains the sequence (files are processed by arrival time).</p> <p>The default is <b>No</b>.</p>	Required
Specify the <b>Polling Interval</b> in days, hours, minutes, and/or seconds.	How often to poll the specified directory. Enter the number of days (if the interval is greater than one day) in the <b>days</b> field, then select the number of hours, minutes, and/or seconds from the drop-down lists as required.	Required
In the <b>Read Limit</b> field, enter the maximum number of files to read per polling sweep.	Maximum number of files to read per polling sweep. Valid values are <b>0</b> or greater. If set to <b>0</b> all files are read.	Required

Setting	Description	Required/ Optional
From the <b>Post Read Action</b> drop-down list, select <b>Delete</b> or <b>Archive</b> .	Specifies what the event generator does with a file after it has been read.  The default is <b>Delete</b> .	Required
In the <b>Archive Directory</b> field, enter a valid path.	Specifies the path to a directory to which files are archived.	Required if <b>Post Read Action</b> is set to <b>Archive</b> , or <b>Pass by filename</b> is set to <b>Yes</b>
In the <b>Error Directory</b> field, enter a valid path.	Specifies the file system directory path to write the file if there is a problem reading it or publishing its contents to the Message Broker channel.	Required
In the <b>Description</b> field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional

## Defining Channel Rules for an Email Event Generator

The Email Generator Channel Rule Definition page allows you to define the properties for the channel rule. The following table summarizes the available settings.

Setting	Description	Required/ Optional
From the <b>Server Protocol</b> drop-down list, select <b>IMAP</b> or <b>POP3</b> .	Server type for the Email account. The default is <b>IMAP</b> .	Required
From the <b>Channel</b> drop-down list, select a Message Broker channel.	The name of the Message Broker channel to which messages matching the configured criteria are published.	Required
In the <b>Hostname</b> field, enter the server name.	The mail server to poll.	Required

Setting	Description	Required/ Optional
In the <b>Port Number</b> field, enter the email server port.	The mail server port.  The default is <b>-1</b> , which indicates the default port number for the mail server (143 for IMAP, 110 for POP3).	Required
In the <b>Username</b> field, enter the username for the account.	Username for the email account. The event generator polls the inbox for this account.	Required
Do one of the following to specify the <b>Password</b> : <ul style="list-style-type: none"> <li>Select the <b>Use Alias</b> option button, then select the password alias from the drop-down list.</li> <li>Select the <b>Use Value</b> option button, then enter the password in the field.</li> </ul>	If you enter the password in the <b>Use Value</b> field, it is stored in clear text in the event generator configuration file. To secure the password, add it to the password store. See <a href="#">“Password Aliases and the Password Store” on page 9-6</a> . After the alias has been added to the password store, it is available for selection from the <b>Use Alias</b> drop-down list.	Optional
From the <b>Attachments</b> field, select <b>Archive</b> or <b>Ignore</b> .	Specifies how attachments are handled. If <b>Archive</b> is selected, attachments are saved to the <b>Archive Directory</b> .	Required
In the <b>Polling Interval</b> field, enter the number of seconds.	How often to poll the account. Enter the number of days (if the interval is greater than one day) in the <b>days</b> field, then select the number or hours, minutes, and/or seconds from the drop-down lists as required.	Required
In the <b>Read Limit</b> field, enter the maximum number of messages to read per polling sweep.	Maximum number of messages to read per polling sweep. Valid values are 0 or greater.	Required
From the <b>Post Read Action</b> drop-down list, select <b>Delete</b> , <b>Archive</b> , or <b>Move</b> .	Specifies what the event generator does with a message after it has been read. <b>Move</b> is only available with the IMAP protocol.  The default is <b>Delete</b> .	Optional

Setting	Description	Required/ Optional
In the <b>IMAP Move Folder</b> field, enter a valid IMAP folder.	If <b>Post Read Action</b> is set to <b>Move</b> , the <b>IMAP Move Folder</b> specifies the folder to which the message is moved.	Required if <b>Post Read Action</b> is set to <b>Move</b>
In the <b>Archive Directory</b> field, enter a valid path.	If <b>Post Read Action</b> is set to <b>Archive</b> , the <b>Archive Directory</b> specifies the path to the archive location.	Required if <b>Post Read Action</b> is set to <b>Archive</b>
In the <b>Error Directory</b> field, enter a valid path.	Specifies the file system directory path to write the message and any attachments if there is a problem.	Required
In the <b>Description</b> field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional

## Defining Channel Rules for a JMS Event Generator

The JMS Generator Channel Rule Definition page allows you to define the properties for the channel rule. The following table summarizes the available settings.

Setting	Description	Required/ Optional
From the <b>Channel</b> drop-down list, select a Message Broker channel.	The name of the channel to which messages matching the configured criteria are published.	Required
In the <b>Property Name</b> field, enter the name of the required JMS property.	<p>If both <b>Property Name</b> and <b>Property Value</b> (below) are specified, the value of the property must match <b>Property Value</b> to trigger a match.</p> <p>If only <b>Property Name</b> is specified, then the presence of the property triggers a match.</p> <p>If both <b>Property Name</b> and <b>Property Value</b> are blank, all message on the JMS queue are a match.</p>	Optional
In the <b>Property Value</b> field, enter the required property value.	If <b>Property Name</b> is specified, <b>Property Value</b> can be used to specify the value required for a match.	Optional
In the <b>Description</b> field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional

## Defining Channel Rules for a Timer Event Generator

The Timer Event Generator Channel Rule Definition page allows you to define the properties for the channel rule. The following table summarizes the available settings.

Setting	Description	Required/ Optional
From the <b>Channel</b> drop-down list, select a Message Broker channel.	The name of the Message Broker channel to which messages matching the configured criteria are published.	Required
From the <b>Effective Time</b> drop-down lists, select the month, day, year, and time to initiate the first event.	The date and time the first event is to be generated. If the effective time has already passed, then the event generator publishes the first event as soon as it is deployed.	Required
Do one of the following: <ul style="list-style-type: none"> <li>Select the <b>Runs Once</b> option button.</li> <li>Select the <b>Runs Every</b> option button, then specify the interval in days, hours, minutes, and seconds.</li> </ul>	Intervals from the <b>Effective Time</b> that each event is to be generated. If the <b>Runs Once</b> option is selected, the <b>Effective Time</b> constitutes the first and last event generated.	Required
Do one of the following: <ul style="list-style-type: none"> <li>Select the <b>Never Expires</b> option button.</li> <li>Select the <b>Expires On</b> option button, then select the month, day, year, and time from the drop-down lists.</li> </ul>	The date and time the configured schedule expires. If the <b>Never Expires</b> option is selected, the configured schedule remains in effect indefinitely.	Required
In the <b>Message</b> field, enter the XML message to be delivered.	The content of the message to be delivered to the specified Message Broker channel. Message content is a single element of any type. Messages published are always XML messages.	Optional



Setting	Description	Required/ Optional
From the <b>Business Calendar</b> drop-down list, select a business calendar.	<p>If a business calendar is selected, the <b>Runs Every</b> interval represents business time calculated against the specified calendar. See <a href="#">“About Business Calendars and Business Time Calculations”</a> on page 11-2.</p> <p>If no calendar is selected, the <b>Runs Every</b> interval represents an absolute period (24 hour day, every day).</p>	Optional
In the <b>Description</b> field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional

## Listing and Locating Event Generators

The View All page displays the following information for each configured generator:

Property	Description
Name	Name assigned to the event generator. This is a link to the Event Generator Definition page.
Channel Count	The number of channel rules defined for the generator.
Files Read (File) Email Read (Email) Messages Read (JMS or Timer)	Number of items read by the event generator since the read counter was last reset.
Last Reset Time	Time the read counter was last reset.
Error Count	Number of errors since the error counter was last reset. The number is the total across all channel rules (an error directory is configured for each channel rule).
Error Reset Time	Time the error counter was last reset.
Status	Status of the event generator (running or suspended).

### To list and locate event generators:

1. From the home page, select the **Event Generator** module.
2. From the left panel, select the type of event generator (**File**, **Email**, **JMS**, or **Timer**).
3. To locate a specific event generator, do one of the following:
  - Filter by generator name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Search**. The generators matching the search criteria are displayed.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◄, first |◄, or last ►| page.

## Viewing and Updating Event Generator Channel Rules

The Event Generator Definition page allows you to update the channel rules. For a JMS event generator, you can also update the default rule channel.

### To update the default channel rule for a JMS event generator:

1. Locate the event generator. See [“Listing and Locating Event Generators” on page 5-17](#).
2. Click the event generator name to display the Event Generator Definition page.
3. Click **Edit Generator Details**.
4. Select a new channel from the **Default Rule Channel** drop-down list.
5. Click **Submit** to update.

### To view and update the channel rules:

1. Locate the event generator. See [“Listing and Locating Event Generators” on page 5-17](#).
2. Click the event generator name to display the Event Generator Definition page.

3. To add new rules or update existing rules:
  - a. Do one of the following:
 

To update a channel rule, click the name of the rule to display the current definition, and then **Click Edit Channel Rule**.

To add a channel rule, click **Define a New Channel Rule**.
  - b. Set the properties as required. For a description of the available properties, see the topic applicable to the event generator you are creating:
 


[“Defining Channel Rules for a File Event Generator” on page 5-10.](#)

[“Defining Channel Rules for an Email Event Generator” on page 5-12.](#)

[“Defining Channel Rules for a JMS Event Generator” on page 5-15.](#)

[“Defining Channel Rules for a Timer Event Generator” on page 5-16.](#)
  - c. Click **Submit** to add or update the channel rule.
4. To delete channel rules:
  - a. Click the check box to the left of the channel rules to be deleted.
  - b. Click **Delete**.
 

A confirmation dialog box is displayed.
  - c. Click **OK** to confirm.
 

The selected channel rules are deleted.
5. To reorder channel rules, click the up or down arrow  button to move entries up or down the list. Changes in list order take effect immediately.

## Suspending and Resuming Event Generators

You can suspend or resume an event generator from the View All page. Suspending a generator moves it to the deactivated state. Resuming redeploys the generator.

**Note:** If you attempt to resume a generator that is already running, or suspend a generator that is already suspended, the command is ignored.

**To suspend an event generator:**

1. Locate the event generators to be suspended. See [“Listing and Locating Event Generators” on page 5-17.](#)
2. Click the check box to the left of the event generators to select.
3. Click **Suspend**.

The selected generators are suspended.

**To resume an event generator:**

1. Locate the event generators to be resumed. See [“Listing and Locating Event Generators” on page 5-17.](#)
2. Click the check box to the left of the event generators to select.
3. Click **Resume**.

The selected generators are resumed.

## Resetting the Counters

You can reset the read and error counters from the View All page.

**To reset the read counter:**

1. Locate the event generators to be reset. See [“Listing and Locating Event Generators” on page 5-17.](#)
2. Click the check box to the left of the event generators to select.
3. Do one of the following:
  - On the View All File Event Generators page, click **Reset File Count**.
  - On the View All Email Event Generators page, click **Reset Email Count**.
  - On the View All JMS Event Generators or View All Timer Event Generators page, click **Reset the Message Count**.

**To reset the error counter:**

1. Locate the event generators to be reset. See [“Listing and Locating Event Generators” on page 5-17.](#)
2. Click the check box to the left of the event generators to select.

3. Click **Reset Error Count**.

## Deleting Channel Rules

You can delete an channel rules from the Event Generator Definition page.

### To delete a channel rule:

1. Locate the event generator. See [“Listing and Locating Event Generators” on page 5-17](#).
2. Click the event generator name to display the Event Generator Definition page.
3. Click the check box to the left of the channel rules to be deleted.
4. Click **Delete Selected Channel Rules**.

The selected channel rules are deleted.

## Deleting Event Generators

You can delete an event generator from the View All page.

### To delete an event generator:

1. Locate the event generators to be deleted. See [“Listing and Locating Event Generators” on page 5-17](#).
2. Click the check box to the left of the event generators to select.
3. Click **Delete**.

The selected generators are deleted.

# Event Generators

# Worklist Administration

This section provides the information you need to use the *Worklist Administration* module of the WebLogic Integration Administration Console to:

- View summary or detailed task status in order to monitor the progress of task completion against due dates.
- Perform queries to show individual workload.
- Reassign tasks in order to speed progress.
- Change task properties, such as state or due date.
- Control task routing by creating or changing substitute routing rules.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to make changes to task properties. See [“Default Groups, Roles, and Security Policies”](#) on page 10-3.

The following topics are provided:

- [Overview of the Worklist Administration Module](#)
- [Listing and Locating Worklist Tasks](#)
- [Listing and Locating Substitute Routing Rules](#)
- [Constructing a Custom Query for Task Instances](#)
- [Viewing and Changing Task Details](#)

- [Updating Task Comment, Owner, or Due Dates from the Summary Page](#)
- [Updating Task State or Deleting Tasks](#)
- [Adding a Substitute Routing Rule](#)
- [Changing a Substitute Routing Rule](#)
- [Deleting a Substitute Routing Rule](#)

# Overview of the Worklist Administration Module

The following table lists the pages you can access from the Worklist Administration module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
Worklist Task Summary	View a list of task instances. Task ID, name, description, state (assigned, claimed, started, completed, aborted, or suspended), complete due date, assignees, claimant, owner, and priority are displayed.	<a href="#">Listing and Locating Worklist Tasks</a>
	Filter the list by task name. Use * to match zero or more characters.	
	Access the Worklist Task Details page for a selected task instance.	
	Select task instances for update. Task state, comment, owner, and due dates can be updated.	
Update State for Selected Tasks	Update the state for one or more task instances.	<a href="#">Updating Task Comment, Owner, or Due Dates from the Summary Page</a> <a href="#">“Updating Task State or Deleting Tasks” on page 6-11</a>



Page	Associated Tasks	Topics
Update Comment for Selected Tasks	Update the comment for one or more task instances.	<a href="#">Updating Task Comment, Owner, or Due Dates from the Summary Page</a>
Update Complete Due Date for Selected Tasks	Update the due date for task completion for one or more task instances.	
Update Claim Due Date for Selected Tasks	Update the claim due date for one or more task instances.	
Update Owner for Selected Tasks	Update the owner for one or more task instances.	
Custom Query	Construct a custom query using properties such as task ID, parent process URI, description, or due dates.	<a href="#">Constructing a Custom Query for Task Instances</a>
Worklist Task Details	View task instance properties.	<a href="#">Viewing and Changing Task Details</a>
	Update the state of the task, or delete the task.	<a href="#">Updating Task State or Deleting Tasks</a>
Edit Worklist Task Details	Edit task instance details.	<a href="#">Viewing and Changing Task Details</a>
Work Substitute Routing Table	View the list of substitute routing rules. Rule name, effective date, expiration date, source, and target are displayed.	<a href="#">Listing and Locating Substitute Routing Rules</a>
	Filter the list by rule name. Use ? to match any single character or * to match zero or more characters.	
Add a Substitute	Define the name, effective date, expiration date, source, and target for a new substitute routing rule.	<a href="#">Adding a Substitute Routing Rule</a>
Edit a Substitute	Change the effective date, expiration date, source, or target for an existing substitute routing rule.	<a href="#">Changing a Substitute Routing Rule</a>

# Listing and Locating Worklist Tasks

The Worklist Task Summary page displays the following information for each task instance. For a more detailed description of the properties, see [“Viewing and Changing Task Details” on page 6-8](#).

Property	Description
Task ID	Unique task instance ID. This is a link to the Worklist Task Detail page. See <a href="#">“Viewing and Changing Task Details” on page 6-8</a> .
Task Name	Name assigned to the task.
Description	Description of the task.
State	Current state of the task (assigned, claimed, started, completed, suspended, or aborted).
Complete Due Date	Due date for task completion
Assignees	One or more users or groups to which the task is assigned.
Claimant	If the task is claimed, the user that claimed the task.
Owner	The owner of the task. A user or group.
Priority	The priority assigned to the task.

**To list and locate tasks:**

1. Select the **Worklist Administration** module from the home page.
2. To locate a specific task, do one of the following:
  - Filter by task name. Enter the search target (use \* to match zero or more characters.), then click **Search**. The tasks matching the search criteria are displayed.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◄, first |◄, or last ►| page.
  - Select Custom Query from the Go menu and construct a custom query. See [“Constructing a Custom Query for Task Instances” on page 6-6](#).

## Listing and Locating Substitute Routing Rules

The Substitute Routing Table page displays the following for each routing rule:

- *Name*  
Unique identifier for the rule.
- *Effective date*  
The date the rule takes effect. If null, the rule takes effect immediately.
- *Expiration date*  
The date the rule expires. If null, the rule remains in effect indefinitely.
- *Source*  
The user or group that will be unavailable.
- *Target*  
The substitute user or group. (Only a group can substitute for a group; only a user can substitute for a user.)

**To list and locate substitute routing rules:**

1. Select the **Worklist Administration** module from the home page.
2. From the left panel, select **Substitute Routing Table**.

3. To locate a specific substitute routing rule, do one of the following:
- Filter by name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Search**. The rules matching the search criteria are displayed.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◄, first |◄, or last ►| page.

# Constructing a Custom Query for Task Instances

The Custom Query page allows you to construct a complex task instance search. The following table summarizes the available search criteria.

Setting	Description
In the <b>Enter Task IDs</b> field, enter one or more task IDs (comma separated list).	Specify one or more task IDs. Do not use wildcards. The search returns task instances matching any of the task IDs specified.
In the <b>Task Name</b> field, enter the task name.	Specify the task name. Use * to match zero or more characters. The search returns tasks that match the target name that also match any other criteria specified.
In the <b>Parent Process IDs</b> field, enter one or more task IDs (comma separated list).	Specify one or more parent process IDs. Do not use wildcards. The search returns task instances associated with any of the parent process instances specified.
In the <b>Parent Process URI</b> field, enter the URI for the parent process. Regular expressions can be used.	Specify the a single parent process URI or a regular expression. The search returns tasks associated with matching process instances that also match any other criteria specified.
Using the <b>Task State</b> check boxes, select one or more states.	Specify one or more of the following states: <b>assigned, claimed, started, suspended, completed, aborted</b> . The search returns tasks in the specified states that also match any other criteria specified.

Setting	Description
In the <b>Description</b> field, enter a regular expression.	Specify a regular expression to match the target description. The search returns tasks with matching descriptions that also match the other criteria specified.
In the <b>Comment</b> field, enter a regular expression.	Specify a regular expression to match the target comment. The search returns tasks with matching comments that also match the other criteria specified.
In the <b>Priority from</b> and <b>to</b> fields specify the low and high ends of the range.	Specify the priority range. The search returns tasks with an assigned priority that falls within the range (inclusive) that also match any other criteria specified.
Under <b>Claim Due Date</b> , do one or both of the following: <ul style="list-style-type: none"> <li>Click the <b>After</b> check box, then select the target date from the drop-down lists.</li> <li>Click the <b>Before</b> check box, then select the target date from the drop-down lists.</li> </ul>	The search returns tasks with a claim due date later than the <b>After</b> date (if specified) and earlier than the <b>Before</b> date (if specified), that also match any other criteria specified.
Under <b>Complete Due Date</b> , do one or both of the following: <ul style="list-style-type: none"> <li>Click the <b>After</b> check box, then select the target date from the drop-down lists.</li> <li>Click the <b>Before</b> check box, then select the target date from the drop-down lists.</li> </ul>	The search returns tasks with a complete due date later than the <b>After</b> date (if specified) and earlier than the <b>Before</b> date (if specified), that also match any other criteria specified.
In the <b>Assignee contains</b> field, enter one or more users or groups in a comma separated list.	Specify one or more users or groups. Do not use wildcards. The search returns tasks with an assignee that matches any of the users or groups, that also match any other criteria specified.

Setting	Description
In the <b>Claimant contains</b> field, enter one or more users in a comma separated list.	Specify one or more users. The search returns tasks with a claimant that matches any of the users, that also match any other criteria specified.
In the <b>Owner contains</b> field, enter one or more users or groups in a comma separated list.	Specify one or more users or groups. Do not use wildcards. The search returns tasks with an owner that matches any of the users or groups, that also match any other criteria specified.

**To execute a custom query:**

1. Select the **Worklist Administration** module from the home page.
2. From the **Go** menu, select **Custom Query**.
3. Enter the search criteria. See the preceding table for settings.
4. Click **Search**.

The page displays a **Query successful** message.

5. Click **Close**.

You are returned to the Worklist Task Summary page. The tasks matching the criteria are displayed.

## Viewing and Changing Task Details

The Worklist Task Details page displays the properties described in the following table. If the task is in the assigned, claimed, or started state, you can link to the Edit Worklist Task Details page to update the task.

Property	Description	Administrator Can Set (Yes/No)
Task ID	Unique task instance ID.	No
Task Name	Name assigned to the task.	No
Parent Process URI	URI for the parent process. This is a link to the Process Type Details page for the process.	No

Property	Description	Administrator Can Set (Yes/No)
Parent Process ID	Instance ID for the parent process. This is a link to the Process Instance Details page for the process instance.	No
Claimant	If the task has been claimed, the user that claimed the task. Claiming a task indicates a user's intent to complete the task. If the task has not yet been claimed, this field is empty.	Yes
Assignees	Comma separated list that designates who should perform the task. A task can be assigned to one or more users or groups. Once assigned, the task can be claimed by: <ul style="list-style-type: none"> <li>Any user included in the list of assignees.</li> <li>A member of any group included in the list of assignees.</li> </ul>	Yes
Owner	User or group that owns the task. This is typically the stakeholder interested in getting the task completed. Use of the owner is application specific, but notification of task status (for example, task complete or overdue) is often sent to the owner.	Yes
State	State of the task.	Yes
	<b>Assigned</b> The assignees have be designated, but the task has not yet been claimed.	
	<b>Claimed</b> A user has claimed the task, thus indicating an intent to complete the task.	
	<b>Started</b> The claimant has started working on the task.	
	<b>Completed</b> The claimant has completed the task.	
	<b>Suspended</b> The task is "on hold." An assigned, claimed, or started task can be placed in the suspended state.	
Description	<b>Aborted</b> The task has been cancelled. An aborted task can be assigned or deleted.	No
Comment	Comment associated with the task.	Yes
Priority	Priority assigned to the task.	Yes

Property	Description	Administrator Can Set (Yes/No)
Complete Due Date	The date by which the task should be completed.	Yes
Claim Due Date	The date by which the task should be claimed.	Yes
Can Be Reassigned	Indicates whether or not the task can be reassigned.	Yes
Can Be Returned	Indicates whether or not the task can be returned.	Yes
Can Be Aborted	Indicates whether or not the task can be aborted.	Yes

### To view task properties:

1. Locate the task. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the task ID to display the Worklist Task Details page.

You can update the state of a task (for example, update assignees, claim an assigned task, or mark a task as complete) from the Worklist Task Details page as described in [“Updating Task State or Deleting Tasks” on page 6-11](#). If the task is not suspended, aborted, or completed, you can link to the Edit Worklist Task Details page to change other task properties as described in the following procedure.

### To change task properties:

1. On the Worklist Task Details page, click the **Edit** link to display the Edit Worklist Task Details page.

**Note:** The **Edit** link is only displayed if the task state is assigned, claimed, or started. If the task is completed, suspended, or aborted, the **Edit** option is not available.

2. Do one or more of the following as required:
  - In the **Comment** field, enter a new comment, or revise the existing comment.
  - In the **Priority** field, enter a new priority, or update an existing priority.



- Check or uncheck **Can be reassigned**, **Can be returned**, or **Can be aborted** check boxes as required.
  - Check or uncheck the **Claim Due Date** check box. If you have checked **Claim Due Date**, specify the **Month**, **Date**, **Year** (using *YYYY* format), **Hour**, and **Minute**.
  - Check or uncheck the **Complete Due Date** check box. If you have checked **Complete Due Date**, specify the **Month**, **Date**, **Year** (using *YYYY* format), **Hour**, and **Minute**.
  - From the **Owner** drop-down, select the owner (user or group).
3. Click **Submit** to save changes and return to the Worklist Task details page.

## Updating Task State or Deleting Tasks

Depending on the current state of a task instance, you can assign, claim, return, start, stop, complete, suspend, abort, or delete the task. The following tables describes each available action. To learn more about task states and operations, see [Worklist Controls and WebLogic Integration](#) in *Building Integration Applications* in the WebLogic Workshop help.

Action	Description
Assign	Designates who should perform the task. and updates the task to the assigned state. Tasks can be assigned to one or more users or groups. Once assigned, the task can be claimed by: <ul style="list-style-type: none"> <li>• Any user to which it is assigned.</li> <li>• A member of any group to which it is assigned.</li> </ul>
Claim	Claims the task on behalf of the specified user and updates the task to the claimed state. Claiming a task indicates an intent to complete the task.
Return	Reassigns a claimed task to the original assignees. The task returns to the assigned state.
Start	Updates a claimed task to the started state.
Stop	Returns a started task to the claimed state.
Complete	Updates a started task to the completed state.
Suspend	Updates the task to the suspended state, indicating that the task is “on hold.”

Action	Description
Abort	Updates the task to the aborted state.
Delete	Deletes the task from the system.

The following tables summarizes the available actions by task state:

Task State	Available Actions
Assigned	Assign, Claim, Suspend, Abort, or Delete
Claimed	Start, Return, Suspend, Abort, or Delete
Started	Complete, Suspend, Return, Stop, Abort, or Delete
Completed	Assign or Delete
Suspended	Resume or Delete
Aborted	Assign or Delete

You can update the state of a task in the following contexts:

- Worklist Task Detail page
- Worklist Task Summary page

**To update the state from the Worklist Task Details page:**

1. Locate the task. See [“Listing and Locating Worklist Tasks” on page 6-4](#).

2. Click the task ID to display the Worklist Task Details page.

**Note:** The buttons displayed depend on the current state of the task.

3. Do one of the following:

- To start, stop, complete, suspend, abort, or delete the task, click **Start Task**, **Stop Task**, **Complete Task**, **Suspend Task**, **Abort Task**, or **Delete Task** as required.
- To claim the task on behalf of a user, enter the user name in the **Claimant** field, then click **Claim Task**.

- To assign a task, enter the assignees (comma separated list that can include users or groups) in the **Assignees** field, then click **Assign Task**.
- To return a task, click **Return Task**. The task is returned to the original assignees.

The task state is updated to reflect the action.

#### To update the state from the Worklist Task Summary page:

1. Locate the task or tasks to be updated. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the check box to the left of each task to be updated.
3. Select **Update State** from the drop-down list, then click **Run Command**.

The Update State for Selected Tasks page is displayed.

**Note:** The buttons displayed depend on the current state of the selected tasks.

4. Do one of the following:
  - To start, stop, complete, suspend, abort, or delete the task, click **Start Task**, **Stop Task**, **Complete Task**, **Suspend Task**, **Abort Task**, or **Delete Task** as required.
  - To claim the task on behalf of a user, enter the user name in the **Claimant** field, then click **Claim Task**.
  - To assign a task, enter the assignees (comma separated list that can include users or groups) in the **Assignees** field, then click **Assign Task**.
  - To return a task, click **Return Task**. The task is returned to the original assignees.

The selected tasks are updated to reflect the action.

## Updating Task Comment, Owner, or Due Dates from the Summary Page

You can update the comment, owner, complete due date, or claim due date for one or more tasks from the Worklist Task Summary page.

#### To update the comment for one or more tasks:

1. Locate the tasks. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the check box to the left of each task to be updated.

**Note:** Only select assigned, claimed, or started task instances. You cannot update the comment for a suspended, completed, or aborted instance.

3. Select **Update Comment** from the drop-down list, then click **Run Command**.

The Update Comment for Selected Tasks page is displayed.

4. In the **Enter updated comment** field, enter the comment.
5. Click **Submit** to apply the comment to the selected tasks.

#### **To update the complete due date for one or more tasks:**

1. Locate the tasks. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the check box to the left of each task to be updated.

**Note:** Only select assigned, claimed, or started task instances. You cannot update the complete due date for a suspended, completed, or aborted instance.

3. Select **Update Complete Due Date** from the drop-down list, then click **Run Command**.  
The Update Complete Due Date for Selected Tasks page is displayed.
4. Do one of the following:
  - To clear the date, uncheck the **Complete Due Date** check box.
  - To specify the date, check the **Complete Due Date** check box, then specify the **Month, Date, Year** (using YYYY format), **Hour**, and **Minute**.
5. Click **Submit** to apply the new complete due date to the selected tasks.

#### **To update the Claim Due Date for one or more tasks:**

1. Locate the tasks. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the check box to the left of each task to be updated.  
**Note:** Only select assigned, claimed, or started task instances. You cannot update the claim due date for a suspended, completed, or aborted instance.
3. Select **Update Claim Due Date** from the drop-down list, then click **Run Command**.  
The Update Claim Due Date for Selected Tasks page is displayed.
4. Do one of the following:
  - To clear the date, uncheck the **Claim Due Date** check box.
  - To specify the date, check the **Claim Due Date** check box, then specify the **Month, Date, Year** (using YYYY format), **Hour**, and **Minute**.

5. Click **Submit** to apply the new claim due date to the selected tasks.

**To update the Owner for one or more tasks:**

1. Locate the tasks. See [“Listing and Locating Worklist Tasks” on page 6-4](#).
2. Click the check box to the left of each task to be updated.
 

**Note:** Only select assigned, claimed, or started task instances. You cannot update the owner for a suspended, completed, or aborted instance.
3. Select **Update Owner** from the drop-down list, then click **Run Command**.  
The Update Owner for Selected Tasks page is displayed.
4. From the **Select new owner** drop-down, select the owner (user or group).
5. Click **Submit** to apply the new claim due date to the selected tasks.

## Adding a Substitute Routing Rule

The Add a Substitute page allows you to create a substitute routing rule. These rules dynamically re-route tasks or task status notifications to a substitute user or group. Each rule consists of the following:

- *Name*  
Unique identifier for the rule.
- *Effective date*  
The date the rule takes effect. If no date is specified, the rule takes effect immediately.
- *Expiration date*  
The date the rule expires. If no date is specified, the rule remains in effect indefinitely.
- *Source*  
The user or group that will be unavailable.
- *Target*  
The substitute user or group. (Only a group can substitute for a group; only a user can substitute for a user.)

**To add a substitute routing rule:**

1. From the home page, select the **Worklist Administration** module.
2. From the left panel, select **Substitute Routing Table**.

3. From the left panel, select **Create New** to display the Add a Substitute page.
4. Check or uncheck the **Effective Date** check box. If you check **Effective Date**, specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**. If you do not check the **Effective Date** check box, the rule takes effect immediately.
5. Check or uncheck the **Expiration Date** check box. If you check **Expiration Date**, specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**. If you do not check the **Expiration Date** check box, the rule remains in effect indefinitely.
6. In the **Source** field, enter the user or group that will be unavailable.
7. In the **Target** field, enter the substitute user or group.
8. Do one of the following:
  - To create the rule, click **Submit**.

The Work Substitute Routing Table page is displayed. The new rule is included in the list.

**Note:** If there is an error, the Add a Substitute page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

- To disregard changes and return to the Work Substitute Routing Table page, click **Cancel**.

## Changing a Substitute Routing Rule

The Edit a Substitute page allows you to change the properties of a substitute routing rule.

### To change a substitute routing rule:

1. Locate the rule to be updated. See [“Listing and Locating Substitute Routing Rules” on page 6-5](#).
2. Click the name to display the Edit a Substitute page.
3. Do one or more of the following as required:
  - Check or uncheck the **Effective Date** check box. If you check **Effective Date**, specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**. If you do not check the **Effective Date** check box, the rule takes effect immediately.
  - Check or uncheck the **Expiration Date** check box. If you check **Expiration Date**, specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**. If you do not check the **Expiration Date** check box, the rule remains in effect indefinitely.

- In the **Source** field, select a new user or group.
  - In the **Target** field, select a new user or group.
4. Do one of the following:
- To update the rule, click **Submit**.  
The Work Substitute Routing Table page is displayed. The updated rule is included in the list.  
**Note:** If there is an error, the Edit a Substitute page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
  - To disregard changes and return to the Work Substitute Routing Table page, click **Cancel**.
  - To reset to the last saved values, click **Reset**.

## Deleting a Substitute Routing Rule

You can delete substitute routing rules from the Work Substitute Routing Table page.

### To delete substitute routing rules:

1. Locate the rules to be deleted. See [“Listing and Locating Substitute Routing Rules” on page 6-5](#).
2. Click the check box to the left of each substitute to be deleted.
3. Click **Delete Selected Substitutes**.





# Application Integration

This section provides the information you need to use the *Application Integration* module of the WebLogic Integration Administration Console to:

- View and reset event and service statistics.
- View adapter instances used by the application view.
- Set environment variables and security policy.
- Change event and service connections.
- Change auto suspend settings.
- Suspend application views or resume previously suspended application views.
- View event and service statistics.
- View application views that use the adapter instance.
- Change event and service connections.
- Manage principal mappings between WebLogic Server usernames and EIS usernames.
- Suspend, resume, and redeploy the adapter instance and all application views that depend on it.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to make changes to application views and adapter instances. See [“Default Groups, Roles, and Security Policies”](#) on page 10-3.

The following topics are provided:

- [Overview of the Application Integration Module](#)
- [Listing and Locating Application Views](#)
- [Listing and Locating Adapter Instances](#)
- [Viewing Application View Instance Statistics](#)
- [Viewing Adapter Instance Statistics](#)
- [Viewing and Changing Event Connection Properties](#)
- [Viewing Dependent Application Views of Adapter Instances](#)
- [Viewing and Changing Adapter Instance Details](#)
- [Viewing and Changing Event Connection Properties](#)
- [Viewing and Changing Service Connection Properties](#)
- [Viewing and Changing Connection Pool Size Parameters](#)
- [Viewing and Changing Application View Auto Suspend Settings](#)
- [Viewing and Changing Environment Variable Values for an Application View](#)
- [Viewing and Changing WebLogic Server to EIS Principal Mappings](#)
- [Changing Event Connections for an Application View](#)
- [Changing Service Connections for an Application View](#)
- [Changing Event Generation Targets](#)
- [Changing Application View Container-Managed Sign-On Settings](#)
- [Updating Security Policies](#)
- [Suspending or Resuming an Application View or Adapter Instance](#)
- [Redeploying an Adapter Instance](#)
- [Resetting the Counters](#)

## About Application Integration Monitoring and Configuration

WebLogic Integration applications consist of *application views* that include *adapters* to communicate with enterprise information systems (EISs). Adapters can be configured to provide *event connections* for event delivery, *service connections* for service invocations, or both.

**Note:** For more information about WebLogic Integration applications, application views, adapters, events, and services, see [Introducing Application Integration](#), which is available at the following URL:

<http://edocs.bea.com/wli/docs81/aiover/index.html>

The Application Integration module of the WebLogic Integration Administration Console enables you to monitor the status of application views and adapters, configure many of their properties, and suspend or restart (resume or redeploy) them, as necessary.

The following sections provide background information related to application integration administration:

### Monitoring Application Views and Adapter Instances

You can observe the health of your WebLogic Integration application by viewing the status of its application views and adapters. If you need more than summary information, you can drill down to detailed statistics for an individual application view or adapter instance.

**Note:** WebLogic Integration Administration Console displays statistics for application views and adapter instances being tested from the WebLogic Integration – Application Integration Design Console. To monitor production statistics only, you should make sure that no application views or adapter instances are in the process of being tested. WebLogic Integration Administration Console displays the names of application views and adapter instances in the Testing state preceded by underscore characters.

For information about testing application views and adapter instances, see “[Defining an Application View](#)” in *Using the Application Integration Design Console*, which is available at the following URL:

<http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html>

To learn more about viewing the status of a WebLogic Integration application, see the following topics:

- [Viewing Application View Instance Statistics](#)
- [Viewing Adapter Instance Statistics](#)
- [Resetting the Counters](#)

## Reconfiguring Application Views and Adapter Instances

Changes in your system environment may require you to update the configuration of application views and adapter instances. You can fine-tune your application's performance by changing its connection pool or auto suspend settings, or you can make major changes to the application by changing adapter instances, event connections, or service connections. In the case of system failures, you can change adapter instances or event targets to respond to EIS outages or the failure of a managed server in a WebLogic Server cluster.

To learn more about reconfiguring application view and adapter instance properties, see the following topics:

- [Viewing Dependent Application Views of Adapter Instances](#)
- [Viewing and Changing Adapter Instance Details](#)
- [Viewing and Changing Event Connection Properties](#)
- [Viewing and Changing Service Connection Properties](#)
- [Viewing and Changing Connection Pool Size Parameters](#)
- [Viewing and Changing Application View Auto Suspend Settings](#)
- [Viewing and Changing Environment Variable Values for an Application View](#)
- [Viewing and Changing WebLogic Server to EIS Principal Mappings](#)
- [Changing Event Connections for an Application View](#)
- [Changing Service Connections for an Application View](#)

- [Changing Application View Container-Managed Sign-On Settings](#)

## Suspending, Resuming, and Redeploying Application Views and Adapter Instances

Most of the changes you can make to application views are applied dynamically without causing an interruption in event delivery or service response. However, some changes require you to redeploy an adapter or application in order for the changes to take effect:

- If you edit properties of event or service connections for an adapter instance, you must redeploy that adapter instance.
- If you select a new event connection or service connection, you must redeploy the application.
- If you change the setting for container-managed sign-on, you must redeploy the application.
- If you change the values of environment variables, you may have to redeploy the adapter instance or the application that uses them—depending on the design of the adapter.

**Note:** Because redeploying an adapter instance or application causes a significant interruption in event delivery and service response, you should make these changes in a pre-production environment. In a production environment, you should redeploy only in emergency situations or when you know client usage is halted.

For routine system maintenance, you can suspend or resume an application view or adapter instance.

To learn more about suspending, resuming, and redeploying application views and adapter instances, see the following topics:

- [Suspending or Resuming an Application View or Adapter Instance](#)
- [Redeploying an Adapter Instance](#)

## Managing Security

You can specify a list of roles that are allowed to execute services and subscribe for events on an application view. (For information about roles, see [“Default Groups, Roles, and Security Policies” on page 10-3.](#)) If you enable container-managed sign-on, you can also provide a map of

WebLogic Server usernames to EIS usernames and password to use principals for obtaining service connections.

To learn more about managing security for application views and adapter instances, see the following topics:

- [Updating Security Policies](#)
- [Changing Application View Container-Managed Sign-On Settings](#)
- [Viewing and Changing WebLogic Server to EIS Principal Mappings](#)

# Overview of the Application Integration Module

The following table lists the pages you can access from the Application Integration module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
<b>Application View Management</b>		
Application View Summary	View a list of application views. Application view ID, state, service count, error count, service average elapsed time, event count, and associated adapter type are displayed.	<a href="#">“Listing and Locating Application Views” on page 7-11</a>
	Reset event counts and service counts.	<a href="#">“Resetting the Counters” on page 7-37</a>
	Access the Application View Details page for a selected application view.	

Page	Associated Tasks	Topics
Application View Details	View application view properties, including properties of its events and services.	<a href="#">“Viewing and Changing Application View Details” on page 7-16</a>
	Suspend or Resume the application view.	<a href="#">“Suspending or Resuming an Application View or Adapter Instance” on page 7-35</a>
	Access one of the following pages to view or update settings: Application View Container Managed Sign-On Settings Application View Instance Summary Application View Environment Variables Application View Security Application View Event Connection Application View Service Connection Application View Auto Suspend Settings	
	Access the Adapter Instance Details page for an application view’s adapter.	<a href="#">“Viewing and Changing Adapter Instance Details” on page 7-20</a>
Application View Container-Managed Sign-on Settings	Enable or disable container-managed sign-on.	<a href="#">“Changing Application View Container-Managed Sign-On Settings” on page 7-33</a>
Application View Instance Summary	For each event type, view a count of events and errors, events per second, and suspended events.	<a href="#">“Viewing Application View Instance Statistics” on page 7-13</a>
	For each service type, view a count of synchronous and asynchronous services, errors, and suspended services, average elapsed time, and average request wait time (for asynchronous services).	
	View last event count reset time and last service count reset time.	

Page	Associated Tasks	Topics
	Reset event counts and service counts.	<a href="#">“Resetting the Counters” on page 7-37</a>
Application View Environment Variables	View all environment variables defined in the application view and change their values. The default and current values for each environment variable are displayed.	<a href="#">“Viewing and Changing Environment Variable Values for an Application View” on page 7-27</a>
Application View Security	View and change the list of roles authorized to execute services and subscribe for events on an application view.	<a href="#">“Updating Security Policies” on page 7-34</a>
Application View Event Connection	Change adapter used by events for an application view.	<a href="#">“Changing Event Connections for an Application View” on page 7-29</a>
Application View Service Connection	View and change adapter used by services for an application view.	<a href="#">“Changing Service Connections for an Application View” on page 7-30</a>
Application View Auto Suspend Settings	View and set auto suspend properties. Change auto suspend timeout, or suspended request retry interval. Enable or disable auto suspend.	<a href="#">“Viewing and Changing Application View Auto Suspend Settings” on page 7-26</a>
<b>Adapter Instance Management</b>		
Adapter Instance Summary	View a list of all adapter instances. Adapter instance ID, status, event count, event error count, last event delivery time, and adapter type are displayed.	<a href="#">“Viewing Adapter Instance Statistics” on page 7-14</a>
	Access the Adapter Instance Details page for a selected adapter instance.	
Adapter Instance Details	View adapter instance information, including name, ID, application name, description, state, cause of current state, and whether or not events connections are enabled.	<a href="#">“Viewing and Changing Adapter Instance Details” on page 7-20</a>



Page	Associated Tasks	Topics
	Suspend or Resume the adapter instance.	<a href="#">“Suspending or Resuming an Application View or Adapter Instance” on page 7-35</a>
	Access Redeploy Adapter Instance page.	
	Access one of the following pages to view additional information about an adapter instance: Adapter Instance Statistics Dependent Application Views	
	Access one of the following pages to update settings: Edit Event Connection Select Service Connection	
Redeploy Adapter Instance	Redeploy specified adapter instance.	<a href="#">“Redeploying an Adapter Instance” on page 7-36</a>
Adapter Instance Statistics	View event and service statistics for an adapter instance.	<a href="#">“Viewing Adapter Instance Statistics” on page 7-14</a>
Dependent Application Views of Adapter Instances	View a list of all application views that depend on an adapter instance.	<a href="#">“Viewing Dependent Application Views of Adapter Instances” on page 7-15</a>
Adapter Instance Event Connection	View and change event properties for an adapter’s event connection.	<a href="#">“Viewing and Changing Event Connection Properties” on page 7-23</a>
	Set event generation targets.	<a href="#">“Changing Event Generation Targets” on page 7-31</a>

Page	Associated Tasks	Topics
Adapter Instance Service Connection	View a list of connection factories available to handle service invocations.	<a href="#">“Viewing and Changing Service Connection Properties” on page 7-24</a>
	Access the Adapter Instance Service Connection Detail page to view and change properties for a service connection.	
Adapter Instance Service Connection Detail	View and change service properties.	<a href="#">“Viewing and Changing Service Connection Properties” on page 7-24</a>
	View and change connection pool settings for a connection factory.	<a href="#">“Viewing and Changing Connection Pool Size Parameters” on page 7-24</a>
	View and change the list of roles authorized to obtain connections from the connection pool.	<a href="#">“Updating Security Policies” on page 7-34</a>
	Access WLS to EIS Principal Mapping page.	
WLS to EIS Principal Mapping	View and delete WebLogic Server usernames mapped to EIS usernames.	<a href="#">“Viewing and Changing WebLogic Server to EIS Principal Mappings” on page 7-28</a>
	Access the WLS to EIS Principal Mapping Detail page to add a mapping between a WebLogic Server username and an EIS username.	

## Listing and Locating Application Views

The Application View Summary page displays the following information for each application view. For a more detailed description of the properties, see [“Listing and Locating Adapter Instances” on page 7-12](#).

Property	Description
AppView ID	<p>Application View ID. This is a link to the Application View Details page. See <a href="#">“Viewing and Changing Application View Details” on page 7-16</a>.</p> <p><b>Note:</b> Names of application views in the Testing state are preceded by underscore characters.</p>
State	The current deployment state of the application view (Deployed, Undeployed, Deploying, Undeploying, Deploy Failed, Suspending, Suspended, Resuming, Testing).
Service Count	Number of service invocations since the service counter was last reset.
Error Count	Number of service errors since the service counter was last reset plus the number of event delivery errors since the event counter was last reset.
Svc Avg Elap (msec)	Service Average Elapsed Time (milliseconds). Average elapsed time in milliseconds for service invocations. This number averages elapsed time for both synchronous and asynchronous services. For asynchronous services, elapsed time includes only time spent communicating with the adapter and excludes time spent waiting on the asynchronous request queue.
Event Count	Number of events delivered since the event counter was last reset.
Associated Adapter Type	Name of adapter used by the application view.

**To list and locate application views:**

- 1. From the home page, select the **Application Integration** module.
- 2. In the left panel, click **Application Views**.
- 3. To locate a specific application view, scroll through the pages as necessary.

## Listing and Locating Adapter Instances

The Adapter Instance Summary page displays the following information for each adapter instance. For a more detailed description of the properties, see [“Viewing and Changing Adapter Instance Details” on page 7-20](#).

Property	Description
ID	Adapter ID. This is a link to the Adapter Instance Details page. See <a href="#">“Viewing and Changing Adapter Instance Details” on page 7-20</a> .  <b>Note:</b> Names of adapter instances in the Testing state are preceded by four underscore characters.
Status	The current status of the adapter instance (Deployed, Undeployed, Deploying, Undeploying, Deploy Failed, Suspending, Suspended, Resuming, Testing).
Event Count	Number of events delivered since the event counter was last reset.
Event Error Count	Number of event delivery errors since the event counter was last reset.
Last Event Delivery Time	System time at which the most recent event was delivered.
Adapter Type	Name of adapter type for the adapter instance.

**To list and locate adapter instances:**

1. From the home page, select the **Application Integration** module.
2. In the left panel, click **Adapter Instances**.
3. To locate a specific adapter instance, scroll through the pages as necessary.

## Viewing Application View Instance Statistics

The Application View Instance Summary page displays the following information for all instances of an application view type, and shows the last time the counters were reset. For more information about the counters, see [“Resetting the Counters” on page 7-37](#).

Property	Description
<b>Event Statistics</b>	
Event Name	Name of each event defined for the application view instance.
Event Count	Number of events delivered since the event counter was last reset.
Event Error Count	Number of event errors since the event counter was last reset.
Event Rate (events per second)	Number of events delivered per second since the event counter was last reset.
Suspended Event Count	Number of events that have been suspended due to the application view being placed in the Suspended state.
<b>Service Statistics</b>	
Service Name	Name of each service defined for the application view instance.
Sync Service Count	Number of synchronous service invocations since the service counter was last reset.
Sync Service Error Count	Number of synchronous service errors since the service counter was last reset.
Async Service Count	Number of asynchronous service invocations since the service counter was last reset.
Async Service Error Count	Number of asynchronous service errors.

Property	Description
Service Average Elapsed Time (seconds)	Average elapsed time in seconds for synchronous service invocations.
Suspended Async Service Count	Number of asynchronous service invocations that have been suspended due to the application view being placed in the Suspended state.

**To view the application view instance statistics:**

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click an application view ID to display the Application View Details page.
3. Click **Show Statistics**.

## Viewing Adapter Instance Statistics

The Adapter Instance Statistics page displays the following information for an adapter instance, and shows the last time the counters were reset. For more information about the counters, see [“Changing Application View Container-Managed Sign-On Settings” on page 7-33](#).

Property	Description
<b>Adapter Instance Statistics</b>	
ID	Adapter instance ID.
<b>Event Statistics</b>	
Event Count	Number of events delivered since the event counter was last reset.
Event Error Count	Number of event errors since the event counter was last reset.
Last Event Delivery Time	System time when the most recent event was delivered.
Suspended Event Count	Number of events that have been suspended due to the adapter instance being placed in the Suspended state.

Property	Description
<b>Service Statistics</b>	
Service Count	Number of synchronous and asynchronous service invocations since the service counter was last reset.
Service Error Count	Number of synchronous and asynchronous service errors since the service counter was last reset.
Service Avg Elapsed Time (seconds)	Average elapsed time in seconds for synchronous service invocations.
Suspended Async Service Request Count	Number of asynchronous service invocations that have been suspended due to the adapter instance being placed in the Suspended state.
Last Service Invocation Time	System time when most recent request for service was received.

**To view adapter instance statistics:**

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12](#).
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Show Statistics**.

## Viewing Dependent Application Views of Adapter Instances

When you redeploy an adapter instance, WebLogic Integration redeploys the dependent application views for that adapter instance. The Dependent Application Views of Adapter Instances page displays the application view ID and status of each application view that depends on the specified adapter instance for event delivery or service invocation. The adapter ID for the adapter instance and application name are displayed.

**To view dependent application views of adapter instances:**

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12](#).
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Dependent Application Views**.

## Viewing and Changing Application View Details

The Application View Details page allows you to:

- View and change application view properties.
- View application view statistics.
- Suspend or resume an application view.

### To view and change application view details:

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11.](#)
2. Click the application view ID to display the Application View Details page.
3. To view statistics for the application view, see [“Viewing Application View Instance Statistics” on page 7-13.](#)
4. To enable or disable the container-managed sign-on setting, see [“Changing Application View Container-Managed Sign-On Settings” on page 7-33.](#)
5. To enable or disable auto suspend, see [“Viewing and Changing Application View Auto Suspend Settings” on page 7-26.](#)
6. To set environment variables, see [“Viewing and Changing Environment Variable Values for an Application View” on page 7-27.](#)
7. To update the security policies, see [“Updating Security Policies” on page 7-34.](#)
8. To change the adapter used for event deliveries, see [“Changing Event Connections for an Application View” on page 7-29.](#)
9. To change the adapter used for service invocations, see [“Changing Service Connections for an Application View” on page 7-30.](#)
10. To suspend or resume the application view, see [“Suspending or Resuming an Application View or Adapter Instance” on page 7-35.](#)



The following table summarizes the information displayed on the Application View Details page.

Property	Description										
<b>Main Details</b>											
Name	Name of the J2EE application that contains the application view.										
Description	Description of the application view.										
State	Current state of the application view.										
	<table> <tr> <td><b>Undeployed</b></td><td>The application view is not available for service invocation or event deliveries.</td></tr> <tr> <td><b>Deploying</b></td><td>The application view is being prepared to allow for service invocation and event delivery.</td></tr> <tr> <td><b>Deployed</b></td><td>The application view is ready for use. Events are available as the EIS produces them and service invocations are allowed.</td></tr> <tr> <td><b>Deploy Failed</b></td><td>The application view could not be deployed and is not available for use.</td></tr> <tr> <td><b>Suspending</b></td><td>The application view is in the process of being suspended.</td></tr> </table>	<b>Undeployed</b>	The application view is not available for service invocation or event deliveries.	<b>Deploying</b>	The application view is being prepared to allow for service invocation and event delivery.	<b>Deployed</b>	The application view is ready for use. Events are available as the EIS produces them and service invocations are allowed.	<b>Deploy Failed</b>	The application view could not be deployed and is not available for use.	<b>Suspending</b>	The application view is in the process of being suspended.
<b>Undeployed</b>	The application view is not available for service invocation or event deliveries.										
<b>Deploying</b>	The application view is being prepared to allow for service invocation and event delivery.										
<b>Deployed</b>	The application view is ready for use. Events are available as the EIS produces them and service invocations are allowed.										
<b>Deploy Failed</b>	The application view could not be deployed and is not available for use.										
<b>Suspending</b>	The application view is in the process of being suspended.										

Property	Description
<b>Suspended</b>	The application view is suspended for events, services, or both. In-flight event deliveries and service invocations are allowed to complete. New events and asynchronous service invocations are accepted, but not delivered or serviced until the application view is in the deployed state. Synchronous service invocations will fail.
<b>Resuming</b>	The application view is in the process of returning to the deployed state from the suspended state.
<b>Undeploying</b>	The application view is in the process of being undeployed, and is unavailable for use. The resources for the application view are being released, and subscriptions are being withdrawn from the associated event adapter instance. Attempts to invoke services will fail with the ApplicationView exception, and no events will be delivered.
<b>Testing</b>	<p>The application view is in the process of being tested from the WebLogic Integration – Application Integration Design Console. Names of application views being tested are displayed in the WebLogic Integration Administration Console preceded by four underscore characters.</p> <p>For information about testing application views, see “<a href="#">Defining an Application View</a>” in <i>Using the Application Integration Design Console</i>, which is available at the following URL:</p> <p><a href="http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html">http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html</a></p>
Cause of Current State	If the application view is in Deploy Failed or Suspended state, the exception thrown or other explanation for why the application is in one of these two states.

Property	Description
Container managed sign on enabled	Specifies whether the connection factory for the associated adapter instance uses container-managed or application-managed sign-on.
	<b>false</b> Container-managed sign-on is disabled and any principal mapping on the service connection factory for this application view is ignored. The client component provides the necessary security information (typically a username and password) when making a call to make a connection to an EIS.
	<b>true</b> Container-managed sign-on is enabled. If WebLogic Server to EIS principal mappings exist, the service connection factory for this application view authenticates connections using the mapped EIS username any time the current WebLogic user has a WebLogic username for which there is a mapping.
<b>Events</b>	
Adapter Instance	ID of the adapter instance the application view uses for event delivery.
Event Name	Name of each event defined for the application view.
Description	Description of each event defined for the application view.
Last Event Invocation Time	Time at which the most recent event was delivered.
Event Error Count	Number of event errors encountered since the event counter was last reset.
Auto Suspend Enabled	Specifies whether the application view can be auto-suspended by a request from the event connection section of the adapter instance or if a connection-related exception is detected during service invocation.
	<b>false</b> Auto suspend is disabled.
	<b>true</b> Auto suspend is enabled. The application view will be suspended if WebLogic Integration determines that the EIS instance is temporarily unavailable. The application view will resume automatically if WebLogic Integration determines the EIS instance is available or the auto-suspend duration has been exceeded.
<b>Services</b>	
Adapter Instance	ID of the adapter instance the application view uses for service invocations.

Property	Description
Service Name	Name of each service defined for the application view.
Description	Description of each service defined for the application view.
Last Service Invocation Time	Time at which the most recent service invocation occurred.
Sync Service Error Count	Synchronous Service Error Count. Number of synchronous errors encountered since the service counter was last reset.
Async Service Error Count	Asynchronous Service Error Count. Number of asynchronous errors encountered since the service counter was last reset.

## Viewing and Changing Adapter Instance Details

The Adapter Instance Details page allows you to:

- View and change event and service connection properties for an adapter instance.
- Suspend, resume, or redeploy an adapter instance.

You can access the Adapter Instance Details page from the Adapter Instance Summary page or the Application View Details page.

### To view and change adapter instance details:

1. Do one of the following:
  - Locate the adapter instance on the Adapter Instance Summary page. See [“Listing and Locating Adapter Instances” on page 7-12](#).
  - Locate an application view (see [“Listing and Locating Application Views” on page 7-11](#)), and click its application view ID to display the Application View Details page.
2. Click the adapter ID to display the Adapter Instance Details page.
3. To view statistics for the adapter instance, see [“Viewing Adapter Instance Statistics” on page 7-14](#).
4. To view and change the properties of the adapter used for event deliveries, see [“Viewing and Changing Event Connection Properties” on page 7-23](#).

5. To view and change the properties of the adapter used for service invocations, see [“Viewing and Changing Service Connection Properties” on page 7-24](#).
6. To suspend or resume the adapter instance, see [“Suspending or Resuming an Application View or Adapter Instance” on page 7-35](#).
7. To redeploy the adapter instance, see [“Redeploying an Adapter Instance” on page 7-36](#).

The following table summarizes the information displayed on the Adapter Instance Details page.

Property	Description
Name	Adapter instance name.
ID	Adapter ID.
App Name	Application name.
Description	Description of the adapter instance.

Property	Description
State	Current state of the adapter instance.
	<b>Undeployed</b> The adapter instance is not available for getting connections or making event deliveries.
	<b>Deploying</b> The adapter instance is being prepared for getting connections or making event deliveries.
	<b>Deployed</b> The adapter instance is ready for use. Events are available as the EIS produces them and getting connections is allowed.
	<b>Deploy Failed</b> The adapter instance could not be deployed and is not available for use.
	<b>Suspending</b> The adapter instance is in the process of being suspended.
	<b>Suspended</b> The adapter instance is suspended for events only. In-flight event deliveries are allowed to complete. New events are accepted, but not delivered until the adapter instance is in the deployed state.
	<b>Resuming</b> The adapter instance is in the process of returning to the deployed state from the suspended state.
	<b>Undeploying</b> The adapter instance is in the process of being undeployed, and is unavailable for use. Attempts to obtain connections will fail with exceptions, and no events will be delivered.
Testing	The adapter instance is in the process of being tested from the WebLogic Integration – Application Integration Design Console. Names of adapter instances being tested are displayed in the WebLogic Integration Administration Console preceded by four underscore characters.
	For information about testing adapter instances, see “ <a href="#">Defining an Application View</a> ” in <i>Using the Application Integration Design Console</i> , which is available at the following URL: <a href="http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html">http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html</a>

Property	Description
Cause of Current State	If the adapter instance is in Deploy Failed or Suspended state, the exception thrown or other explanation for why the instance is in one of these two states.
Events Connections Enabled	Indicates whether or not the adapter instance was configured at design time to support events. For information about configuring event connections, see <a href="#">“Defining an Application View”</a> in <i>Using the Application Integration Design Console</i> , which is available at the following URL:  <a href="http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html">http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html</a>

## Viewing and Changing Event Connection Properties

The Adapter Instance Event Connection page enables you to view and change event properties for an adapter instance. The name and current value of each event property are displayed.

**Note:** Event properties are adapter-specific. For descriptions of event properties and their settings, see your adapter documentation.

### To view and change event connection properties:

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances”](#) on page 7-12.
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Edit Event Connection**.
4. Enter new settings in the New Value column for one or more event properties, as necessary.
5. Do one of the following:
  - To update the event connection properties, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** In order for changes in event connection properties to take effect, you must redeploy the adapter instance. For information about redeploying, see [“Redeploying an Adapter Instance”](#) on page 7-36.

## Viewing and Changing Service Connection Properties

The Adapter Instance Service Connection Detail page enables you to view and change service properties for an adapter instance. The name and current value of each service property are displayed.

**Note:** Service properties are adapter-specific. For descriptions of service properties and their settings, see your adapter documentation.

### To view and change service connection properties:

1. Locate the adapter instance. See [“Viewing and Changing Adapter Instance Details” on page 7-20](#).
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Select Service Connection** to display the Adapter Instance Service Connection page.
4. Click the name of the service connection for which you want to change properties.

The Adapter Instance Service Connection Detail page is displayed.

5. Enter new settings in the New Value column for one or more service properties, as necessary.
6. Do one of the following:
  - To update the service connection properties, click **Submit**.
  - To reset to the last saved values, click **Reset**.
  - To disregard changes, click **Cancel**.

**Note:** In order for changes in service connection properties to take effect, you must redeploy the adapter instance. For information about redeploying, see [“Redeploying an Adapter Instance” on page 7-36](#).

## Viewing and Changing Connection Pool Size Parameters

The Adapter Instance Service Connection Detail page enables you to view and change the minimum and maximum connection pool size for the connection factory associated with an adapter instance, and to specify whether or not the pool is allowed to shrink.



The following table summarizes the available settings.

Setting	Description	Required/ Optional
In the <b>Min Pool Size</b> field, enter the minimum number of connections.	Minimum connection pool size for the connection factory. Valid values are from <b>0</b> to <b>2147483647</b> .  The default is <b>1</b> .	Required
In the <b>Max Pool Size</b> field, enter the maximum number of connections.	Maximum connection pool size for the connection factory. Valid values are the greater of minimum pool size or <b>1</b> to <b>2147483647</b> .  The default is <b>10</b> .	Required
Click the <b>Allow Pool to Shrink</b> check box to enable or disable this option.	With <b>Allow Pool to Shrink</b> enabled, WebLogic Server can destroy idle connections, reducing the number of connections in the pool to the greater of either the initial pool capacity or the number of connections currently in use.	Required

#### To view and change connection pool size parameters:

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12](#).
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Select Service Connection** to display the Adapter Instance Service Connection page.
4. Click the name of the service connection for which you want to view or change connection pool parameters.  
  
The Adapter Instance Service Connection Detail page is displayed.
5. Configure the settings as described in the preceding table.
6. Do one of the following:
  - To update the service connection properties, click **Submit**.
  - To reset to the last saved values, click **Reset**.
  - To disregard changes, click **Cancel**.

**Note:** In order for changes in service connection properties to take effect, you must redeploy the adapter instance. For information about redeploying, see [“Redeploying an Adapter Instance” on page 7-36](#).

# Viewing and Changing Application View Auto Suspend Settings

The Application View Auto Suspend Settings page allows you to view and change the auto suspend enabled, auto suspend timeout, and auto suspend retry interval settings for an application view. The following table summarizes the available settings.

Setting	Description	Required/Optional
Click the <b>Auto Suspend</b> check box to enable or disable auto suspend.	With auto suspend enabled, the application view will be suspended if WebLogic Integration determines that the EIS instance is temporarily unavailable. The application view will resume automatically if WebLogic Integration determines the EIS instance is available or the auto-suspend duration has been exceeded.	Required
In the <b>Auto Suspend Timeout</b> field, enter the number of seconds.	How long auto suspend should last. Valid values are from <b>0</b> to <b>2147483647</b> seconds, and <b>-1</b> to specify an infinite timeout period.  The default is <b>1800</b> .	Required
In the <b>Suspended Request Retry Interval</b> field, enter the number of seconds.	How long to wait before retrying a suspended request. Valid values are from <b>0</b> to <b>2147483647</b> seconds.  The default is <b>3</b> .	Required

## To view and change application view auto suspend settings:

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click the application view ID to display the Application View Details page.

3. In the Events group, click **Change Settings** to display the Application View Auto Suspend Settings page.
4. Configure the settings as described in the preceding table.
5. To update the settings, click **Submit**.

## Viewing and Changing Environment Variable Values for an Application View

The Application View Environment Variables page allows you to view the name, description, type, default value, and current value of environment variables defined for an application view. The Application View Environment Variables page also enables you to change the values of these variables.

**Note:** To add or delete environment variables, you must use the WebLogic Integration – Application Integration Design Console. For information about adding and deleting environment variables, see “[Defining an Application View](#)” in *Using the Application Integration Design Console*, which is available at the following URL:

<http://edocs.bea.com/wli/docs81/aiuser/2usrdef.html>

When you change the values of environment variables, you may have to redeploy the adapter instance or the application that uses them—depending on the design of the adapter. For example, the DBMS sample adapter can dynamically apply changes to environment variables used by services, but requires a redeployment of the adapter hosting the event connection for changes in event-related environment variables to take effect. For more information about specific environment variables, see the documentation for your adapter.

### To set new values for application view environment variables:

1. Locate the application view. See “[Listing and Locating Application Views](#)” on page 7-11.
2. Click the application view ID to display the Application View Details page.
3. In the Main Details group, click **Set Environment Variables** to display the Application View Environment Variables page.
4. Enter new values for one or more environment variables, as necessary.
5. Do one of the following:
  - To update the settings, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** For changes that are not applied dynamically, you must redeploy the adapter instance or application that uses the environment variables. Valid changes to environment variable settings are always applied when an application is successfully redeployed.

For information about redeploying an adapter instance, see [“Redeploying an Adapter Instance” on page 7-36](#). For information about using the WebLogic Server Administration Console to redeploy applications, see “Deploying, Redeploying, and Stopping Applications” in [“Deploying Applications and Modules”](#) in the *WebLogic Server Administration Console Online Help*, which is available at the following URL:  
<http://edocs.bea.com/wls/docs81/ConsoleHelp/deployment.html>

## Viewing and Changing WebLogic Server to EIS Principal Mappings

If container-managed sign-on is enabled for an application view, WebLogic Integration can map principals from WebLogic Server usernames to EIS usernames and passwords when obtaining service connections for the application view. The WLS to EIS Principal Mapping page enables you to view and change principal mappings. The WebLogic Server username and EIS username for each existing principal mapping are displayed for the named adapter instance and connection factory.

**Note:** If container-managed sign-on is disabled, WebLogic Integration ignores any principal mappings.

### To view WebLogic Server to EIS principal mappings for a service connection:

1. Locate the adapter instance for the service connection. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click the adapter instance ID to display the Adapter Instance Details page.
3. Click **Select Service Connection** to display the Adapter Instance Service Connection page.
4. Click the name of the service connection for which you want to map principals.

The Adapter Instance Service Connection Detail page is displayed.

5. Click **WLS to EIS Principal Map** to display existing principal mappings on the WLS to EIS Principal Mapping page.

**To delete WebLogic Server to EIS principal mappings for a service connection:**

1. On the WLS to EIS Principal Mapping page, click the check box to the left of one or more principal mappings that you want to delete.
2. Click **Delete**.

The selected mappings are deleted, and the WLS to EIS Principal Mapping page displays the remaining principal mappings for the service connection.

**To add WebLogic Server to EIS principal mappings for a service connection:**

1. On the WLS to EIS Principal Mapping page, click **Add Mapping** to display the WLS to EIS Principal Mapping Detail page.
2. Create a new principal mapping by entering a WebLogic Server username, EIS username, and EIS password for the Source WLS User Name, Target EIS User Name, and Target EIS Password, respectively.
3. Do one of the following:
  - To add the new mapping, click **Submit**.
  - To disregard the mapping, click **Cancel**.

## Changing Event Connections for an Application View

The Application View Event Connection page displays the names of the adapter instances defined for the application view and allows you to select an adapter to use for event delivery.

**To change event connection for an application view:**

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click the application view ID to display the Application View Details page.
3. In the Events group, click **Change Event Connection** to display the Application View Event Connection page.
4. Select an event connection.
5. Do one of the following:
  - To update the event connection setting, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** In order for a change in event connection to take effect, you must redeploy the application using the WebLogic Server Administration Console. For information about using the WebLogic Server Administration Console to redeploy applications, see “Deploying, Redeploying, and Stopping Applications” in “[Deploying Applications and Modules](#)” in the *WebLogic Server Administration Console Online Help*, which is available at the following URL:

<http://edocs.bea.com/wls/docs81/ConsoleHelp/deployment.html>

## Changing Service Connections for an Application View

The Application View Service Connection page displays the adapter instances and service connection factories that are defined for the application view, and allows you to select an adapter to use for service invocations.

### To change service connection for an application view:

1. Locate the application view. See “[Listing and Locating Application Views](#)” on page 7-11.
2. Click the application view ID to display the Application View Details page.
3. In the Services group, click **Change Service Connection** to display the Application View Service Connection page.
4. Select a service connection.
5. Do one of the following:
  - To update the service connection setting, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** In order for a change in service connection to take effect, you must redeploy the application using the WebLogic Server Administration Console. For information about using the WebLogic Server Administration Console to redeploy applications, see “Deploying, Redeploying, and Stopping Applications” in “[Deploying Applications and Modules](#)” in the *WebLogic Server Administration Console Online Help*, which is available at the following URL:

<http://edocs.bea.com/wls/docs81/ConsoleHelp/deployment.html>

## Changing Event Generation Targets

Application Integration event generators work with resource adapters and publish EIS events to message broker channels. These event generators allow you to start a business process based on events, such as an updated record in a database.

For more information about event generators and message broker channels, see *Introducing Application Integration*, which is available at the following URL:

<http://edocs.bea.com/wli/docs81/aiover/index.html>

## Basic Event Generation Targeting

By default, the event generator for an adapter instance is started on all servers on which the adapter instance is deployed or started. The Adapter Instance Event Connection page enables you to specify a list (in comma-separated format) of the names of managed servers on which the event generator for an adapter instance is to be started.

## Advanced Event Generation Targeting

Some adapters, such as the DBMS sample adapter, support advanced event generation targeting using the event connection instance ID. This is useful when multiple instances of an event connection are processing events in a cluster. One event connection instance is deployed per server, and the instance ID is used to load balance the delivery of events between these instances.

The syntax for advanced event generation targeting is:

```
servername1=[event_conn_instance_ID_1,event_conn_instance_ID_2,...],
servername2[event_conn_instance_ID_3,...],...
```

The arguments for this syntax are defined as follows:

- *servername* is the name of a server whose event connection you want to target
- *event\_conn\_instance\_ID* is the event connection instance ID whose events you want to target to the specified server

If a managed server in your WebLogic Server cluster fails, you can move the event connection instance from the failed server to a live server—potentially configuring multiple event connection instances to operate on a single live server. For example, in a three node cluster with *server1*, *server2*, *server3* and *instance1*, *instance2*, *instance3*, the target specification would be:

```
server1=[instance1],server2=[instance2],server3=[instance3]
```

If `server2` fails, you could move the load for `server2` to a server that is still operational, such as `server1`, using the following target specification:

```
server1=[instance1,instance2],server3=[instance3]
```

In this case, the event connection on `server1` consumes events destined for `instance1` and `instance2`. The event connection on `server3` consumes events destined only for `instance3`.

When `server2` is back in operation, you could return to your original configuration using the following target specification:

```
server1=[instance1],server2=[instance2],server3=[instance3]
```

The event connection on `server1` stops consuming events for `instance2`, and the event connection on `server2` starts consuming events for `instance2`.

### To change event generation targets:

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12](#).
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Edit Event Connection**.
4. Do one of the following:

- In the Event Generation Targets group, enter a comma-separated list of server names using the following syntax:

```
servername1,servername2,servername3,...
```

The event generator for the adapter instance will be started on the named servers only.

- If advanced event targeting is supported by your adapter, enter mapping for servers and event connection instances using the following syntax:

**Note:** The following syntax represents a single entry for Targets. It is shown here on multiple lines for the sake of readability.

```
servername1=[event_conn_instance_ID_1,event_conn_instance_ID_2,...],  
servername2[event_conn_instance_ID_3,...],...
```

The arguments for this syntax are defined as follows:

- *servername* is the name of a server whose event connection you want to target
- *event\_conn\_instance\_ID* is the event connection instance ID whose events you want to target to the specified server



5. Do one of the following:
  - To update event targets, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** In order for changes in event targets to take effect, you must redeploy the adapter instance. For information about redeploying, see [“Redeploying an Adapter Instance” on page 7-36](#).

## Changing Application View Container-Managed Sign-On Settings

The Application View Container Managed Signon Settings page allows you to change the container-managed sign-on setting for an application view. For information about container-managed sign-on, see [“Managing Security” on page 7-5](#).

### To change the container-managed sign-on setting:

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click the application view ID to display the Application View Details page.
3. In the Main Details group, click **Change Settings** to display the Application View Container Managed Signon Settings page.
4. Click the check box to enable or disable the setting.
5. Do one of the following:
  - To update the setting, click **Submit**.
  - To disregard changes, click **Cancel**.

**Note:** In order for a new container-managed sign-on setting to take effect, you must redeploy the application using the WebLogic Server Administration Console. For information about using the WebLogic Server Administration Console to redeploy applications, see “Deploying, Redeploying, and Stopping Applications” in [“Deploying Applications and Modules”](#) in the *WebLogic Server Administration Console Online Help*, which is available at the following URL:

<http://edocs.bea.com/wls/docs81/ConsoleHelp/deployment.html>

## Updating Security Policies

The WebLogic Integration Administration Console enables you to view and update the security policies for application views and adapter instances. The Application View Security page allows you to specify a list of roles that are allowed to execute services and subscribe for events. The Adapter Instance Service Connection Detail page allows you to specify a list of roles that can obtain service connections from the connection factory for an adapter instance.

### To view security policies for an application view:

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11](#).
2. Click the application view ID to display the Application View Details page.
3. In the Main Details group, click **Set Security Policy** to display the Application View Security page.

### To view security policies for an adapter instance:


1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12](#).
2. Click the adapter instance ID to display the Adapter Instance Details page.
3. Click **Select Service Connection** to display the Adapter Instance Service Connection page.
4. Click the name of the service connection for which you want to set security policies.

The Adapter Instance Service Connection Detail page is displayed. You set authorized roles in the Security Policy group.

### To update security policies:


1. Add or remove role assignments as follows:

To add roles:

- a. From the **Available Roles** list, select the required roles. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)
- b. Click the  icon to move the selected roles to the **Current Roles** list.

To remove roles:

- a. From the **Current Roles** list, select the roles to remove. (To select multiple roles, press and hold the **Ctrl** key as you click each additional role.)

- b. Click the  icon to move the selected roles to the **Available Roles** list.
2. Do one of the following:
  - To update the policy, click **Submit**.
  - To reset to the last saved values, click **Reset**.
  - To disregard changes, click **Cancel**.

## Suspending or Resuming an Application View or Adapter Instance

Depending on the current state of an application view or adapter instance, you may be able to suspend or resume it. The following table summarizes the available actions by state:

Instance State	Available Actions
Deployed	Suspend
Suspended	Resume
Undeployed Deploying Deploy Failed Suspending Resuming Undeploying	None

The Application View Details page enables you to suspend or resume an application view instance.

**Note:** When an application view is suspended, current service invocations and event deliveries complete. New asynchronous service invocations are accepted, but not serviced. No new event deliveries are made. Synchronous service requests fail with an `ApplicationViewException`.

The Adapters Instance Details page enables you to suspend or resume an adapter instance.

**Note:** When you suspend an adapter instance, you also suspend its dependent application views.

**To suspend or resume an application view instance:**

1. Locate the application view. See [“Listing and Locating Application Views” on page 7-11.](#)
2. Click the application view name to display the Application View Details page.
3. Click **Suspend** or **Resume**, as required.

**To suspend or resume an adapter instance:**

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12.](#)
2. Click the adapter ID to display the Adapters Instance Details page.
3. Click **Suspend** or **Resume**, as required.

**Note:** While application views and adapter instances are in the Suspending or Resuming states, the button to resume or suspend is not available. Refresh your browser to display this button.

## Redeploying an Adapter Instance

If you have made changes to the event connection or service connection for an adapter instance, you must redeploy the instance for those changes to take effect. Redeploying an adapter instance causes its dependent application views to be redeployed, as well.

The Adapter Instance Details page enables you to redeploy an adapter instance.

**To redeploy an adapter instance:**

1. Locate the adapter instance. See [“Listing and Locating Adapter Instances” on page 7-12.](#)
2. Click an adapter ID to display the Adapter Instance Details page.
3. Click **Redeploy**.

The Redeploy Adapter Instance page displays the name and ID of the adapter instance to be redeployed.

4. Do one of the following:
  - To redeploy the adapter instance and apply changes to its configuration, click **Submit**.

Event connections and service connections are updated to reflect any changes that have been made to their general properties, event generation targets, connection pool size parameters, security policies, and principal maps. Dependent application views are redeployed.

- To allow the adapter instance to continue to operate without applying changes to its configuration, click **Cancel**.

## Resetting the Counters

You can reset the event delivery, service invocation, and error counters in the following contexts:

- Application View Summary page
- Application View Instance Summary page

When you reset the event or service counter, you also reset the associated error counter.

**Note:** Resetting counters does not reset the count for suspended events or suspended asynchronous services.

### To reset the counters for one or more application views from the Application View Summary page:

1. Display the Application View Summary page as described in [“Listing and Locating Application Views” on page 7-11](#).
2. Click the check box to the left of each application view for which counters are to be reset.
3. Do one or both of the following:
  - Click **Reset Event Count**.
  - Click **Reset Service Count**.

### To reset the counters for all instances of a single application view type from the Application View Instance Summary page:

1. Display the Application View Instance Summary page as described in [“Listing and Locating Application Views” on page 7-11](#).
2. Do one or both of the following:
  - Click **Reset Event Count**.
  - Click **Reset Service Count**.



# Trading Partner Management

This section provides the information you need to use the *Trading Partner Management* module of the WebLogic Integration Administration Console to manage trading partners and services, and to monitor messages and other indicators of trading partner activity. The Trading Partner Management module is divided into the following functional areas which can be accessed from the Trading Partner Management home page:

- *Profile Management*  
Allows administrators to configure the local and remote trading partners that conduct business transactions. The required basic information, security certificates, protocol bindings, and any custom properties required for the transactions are configured.
- *Service Management*  
Allows administrators to manage the services and service profiles that constitute the business processes offered or called by trading partners.
- *Message Tracking*  
Allows administrators to set the message tracking criteria and view summary and message content for the messages tracked.
- *Partner Profile Import/Export*  
Allows administrators to import or export trading partner management data (trading partners and services).
- *Statistics*  
Allows administrators to view summary statistics that reflect the level of trading partner activity.

- *Configuration*

Allows administrators to configure the resources required and to set system defaults.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to create, change, or delete trading partner management data. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About Trading Partner Management](#)
- [Overview of the Trading Partner Management Module](#)
- [Configuring Trading Partner Management](#)
- [Adding Trading Partner Profiles](#)
- [Adding Certificates to a Trading Partner](#)
- [Adding Protocol Bindings to a Trading Partner](#)
- [Adding a Custom Extension to a Trading Partner](#)
- [Adding Services](#)
- [Adding Service Profiles to a Service](#)
- [Defining Trading Partner Profiles](#)
- [Defining Protocol Bindings](#)
- [Listing and Locating Trading Partners](#)
- [Listing and Locating Services](#)
- [Viewing and Changing Trading Partner Profiles](#)
- [Viewing and Changing Certificates](#)
- [Viewing and Changing Bindings](#)
- [Viewing and Changing a Custom Extension](#)
- [Viewing and Changing Services](#)
- [Viewing and Changing Service Profiles](#)
- [Enabling and Disabling Trading Partner and Service Profiles](#)



- [Importing Management Data](#)
- [Exporting Management Data](#)
- [Deleting Trading Partner Profiles and Services Using Bulk Delete](#)
- [Deleting Trading Partner Profiles](#)
- [Deleting Certificates, Bindings, or Custom Extensions](#)
- [Deleting Services](#)
- [Deleting Service Profiles from a Service](#)
- [Viewing Statistics](#)
- [Monitoring Messages](#)

## About Trading Partner Management

The basic building blocks of trading partner integration are trading partner profiles, services, and service profiles. In WebLogic Integration, a trading partner is understood as an entity that has an agreement with another entity to participate in a specific business transaction, or service, by playing a predefined role. A trading partner profile includes the trading partner's identifying information, and any certificates or protocol binding definitions required to conduct the business transactions.

A service represents a business process that is either offered by a local trading partner, or a business process that is being called via a control on a remote trading partner. In the case of a service *offered* by a local trading partner, this element directly corresponds to a web service or process type deployed in the local domain. In the case of a service *called* by a local trading partner, the service corresponds to a control in the local domain that is used to invoke the remote service. Service profiles specify the protocol binding and URL endpoints for the local and remote trading partners that offer and call the service.

The WebLogic Integration Administration Console allows administrators to configure and manage the required profiles, certificates, and protocol bindings, and to monitor trading partner activity.

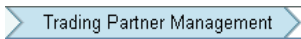
To learn more about:

- The entities and elements that comprise trading partner management data, see [Appendix A, "TPM Schema."](#)

- How trading partner management data is used to support business transactions, see [Introducing Trading Partner Integration](#).
- Security in Trading Partner Integration, see “Using WebLogic Integration Security” in [Deploying WebLogic Integration Solutions](#).

# Overview of the Trading Partner Management Module

The following table lists the pages you can access from the Trading Partner Management module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
Trading Partner Management		
Trading Partner Management Home Page	Select a trading partner management module (Profile Management, Service Management, Message Tracking, Partner Profile Import/Export, Statistics, or Configuration). Return to this page at any time by selecting  from the navigation bar.	“Trading Partner Management” on page 8-1
Profile Management: Partner Profiles		
View and Edit Trading Partner Profiles	View a list of trading partners. Trading partner name, type (remote or local), business ID, description, and status of the service profiles associated with the partner (enabled or disabled) are displayed.	“Listing and Locating Trading Partners” on page 8-41
	Filter the list by name. Use ? to match any single character or * to match zero or more characters.	
	Delete one or more trading partners.	“Deleting Trading Partner Profiles” on page 8-71
	Enable or disable the service profiles associated with a trading partner.	“Enabling and Disabling Trading Partner and Service Profiles” on page 8-64
Add a New Trading Partner	Add a trading partner.	“Adding Trading Partner Profiles” on page 8-13

Page	Associated Tasks	Topics
View and Edit Trading Partner Profile	View a partner profile. The name, business ID, business type, trading partner type (local or remote), status, description, and contact information are displayed.	<a href="#">“Viewing and Changing Trading Partner Profiles” on page 8-43</a>
	View summary information for the protocol bindings associated with the trading partner. Add a new binding or select a binding for edit.	<a href="#">“Viewing and Changing Bindings” on page 8-47</a>
	View summary information for the certificates associated with the trading partner. Add a new certificate or select a certificate for edit.	<a href="#">“Viewing and Changing Certificates” on page 8-46</a>
	View summary information for a custom extension. Update the existing custom extension, or add a new custom extension if one does not exist.	<a href="#">“Viewing and Changing a Custom Extension” on page 8-59</a>
Edit Trading Partner Profile	Update trading partner properties. Change the description, business ID, business type, trading partner type (local or remote), status (enabled or disabled), contact information, or user identity.	<a href="#">“Viewing and Changing Trading Partner Profiles” on page 8-43</a>
<b>Profile Management: Bindings</b>		
Add Binding	Add a new protocol binding to the selected trading partner.	<a href="#">“Adding Protocol Bindings to a Trading Partner” on page 8-19</a>
View Binding Details	View the properties of a binding.	<a href="#">“Viewing and Changing Bindings” on page 8-47</a>
Edit Binding	Edit the properties of a binding.	<a href="#">“Viewing and Changing Bindings” on page 8-47</a>
<b>Profile Management: Certificates</b>		
Add Certificate	Add a new certificate to the selected trading partner.	<a href="#">“Adding Certificates to a Trading Partner” on page 8-15</a>
View and Edit Trading Partner Certificate	View the properties of a certificate or update a certificate.	<a href="#">“Viewing and Changing Certificates” on page 8-46</a>

Page	Associated Tasks	Topics
Edit Certificate	Update a certificate by importing certificate files.	<a href="#">“Viewing and Changing Certificates” on page 8-46</a>
<b>Profile Management: Custom Extension</b>		
Add Custom Extension	Add custom properties to the trading partner.	<a href="#">“Adding a Custom Extension to a Trading Partner” on page 8-19</a>
View and Edit Custom Extension	View the custom properties for a trading partner.	<a href="#">“Viewing and Changing a Custom Extension” on page 8-59</a>
Edit Custom Extension	Change the custom properties for a trading partner.	<a href="#">“Viewing and Changing a Custom Extension” on page 8-59</a>
<b>Service Management: Services</b>		
View and Edit Services	View a list of services. Service name, business service name, description, type, business protocol, and description are displayed.	<a href="#">“Viewing and Changing Services” on page 8-60</a>
	Filter the list by service name. Use ? to match any single character or * to match zero or more characters.	
	Delete a service.	<a href="#">“Deleting Services” on page 8-74</a>
Add Service	Add a service definition for a newly deployed service. Assign the name, type, and business protocol. Optionally assign a description.	<a href="#">“Adding Services” on page 8-21</a>
View and Edit Service Details	View service properties. The type, business protocol, description, version, and associated service profiles are displayed.	<a href="#">“Viewing and Changing Services” on page 8-60</a>
	Select a service profile to view or edit.	
Edit Service Details	Update service properties. Change the type, business protocol, description or version. Add service profiles.	<a href="#">“Viewing and Changing Services” on page 8-60</a>

Page	Associated Tasks	Topics
Add Service Profile	Define a service profile to be added to the service. Enable or disable, specify the message tracking level, and specify the binding and URL endpoint for the local and remote trading partners.	<a href="#">“Adding Service Profiles to a Service” on page 8-22</a>
View Service Profile	View the properties of a service profile.	<a href="#">“Viewing and Changing Service Profiles” on page 8-62</a>
Edit Service Profile	Update a service profile. Enable or disable the service, change the message tracking level, or change the binding and URL endpoint for the local and remote trading partners.	<a href="#">“Viewing and Changing Service Profiles” on page 8-62</a>
Add Authentication	Add authentication to a service profile.	<a href="#">“Adding Authentication to a Service Profile” on page 8-24</a>
<b>Message Tracking</b>		
View Messages	View the list of messages. Event ID, time of event, direction (inbound or outbound), and status are displayed.	<a href="#">“Monitoring Messages” on page 8-76</a>
Filter the Displayed Messages	Configure the filter for the messages displayed on the View Messages page. Criteria include trading partner sender and receiver, tracking start time and interval, and status.	<a href="#">“Filtering the Messages Displayed” on page 8-77</a>
Message Details	View message properties and link to detail, such as header, status, or message part data.	<a href="#">“Filtering the Messages Displayed” on page 8-77</a>
<b>Import/Export</b>		
Import Trading Partner Management Data	Select a trading partner management file for import, and set the import properties.	<a href="#">“Importing Management Data” on page 8-67</a>
Export Trading Partner Management Data	Select trading partners and services for export, and set the export properties.	<a href="#">“Exporting Management Data” on page 8-68</a>

Page	Associated Tasks	Topics
Bulk Delete	Select trading partner profiles and services to delete and set the delete properties.	<a href="#">“Deleting Trading Partner Profiles and Services Using Bulk Delete” on page 8-70</a>
<b>Statistics</b>		
Trading Partner Management Statistics	View summary statistics. Trading partner count, service count by type (process, service control, or web service), service profile count, number of conversations, and a count of the sent and received messages are displayed.	<a href="#">“Viewing Statistics” on page 8-75</a>
<b>Configuration</b>		
General Configuration	Set the message tracking properties. Specify the tracking level (all, metadata, or none), directory used to store the messages, and whether or not to trace raw messages.	<a href="#">“Configuring the Mode and Message Tracking” on page 8-9</a>
	Set the trading partner integration mode (test or production).	
Proxy Configuration	Configure a proxy host.	<a href="#">“Configuring a Proxy Host” on page 8-11</a>
Audit Log Configuration	Enable or disable secure audit logging. If enabled, specify the secure audit logging class.	<a href="#">“Configuring Secure Audit Logging” on page 8-11</a>
Secure Timestamp Configuration	Specify the Java class used for secure time stamping.	<a href="#">“Configuring Secure Audit Logging” on page 8-11</a>
Refresh Keystore	Refresh the KeyStores (identity and trust) in memory from the disk.	<a href="#">“Refreshing the Keystore” on page 8-12</a>
Certificate Verification Provider	Specify the certificate verification provider.	<a href="#">“Specifying the Certificate Verification Provider” on page 8-12</a>

## Configuring Trading Partner Management

The Trading Partner Management Configuration module allows you configure system resources, set the message tracking defaults, or refresh the keystore. See the appropriate topic for instructions:

- [“Configuring the Mode and Message Tracking” on page 8-9](#)
- [“Configuring a Proxy Host” on page 8-11](#)
- [“Configuring Secure Audit Logging” on page 8-11](#)
- [“Refreshing the Keystore” on page 8-12](#)
- [“Specifying the Certificate Verification Provider” on page 8-12](#)

## Configuring the Mode and Message Tracking

The General Configuration page allows you to define the mode (test or production), and message tracking properties for trading partner integration.

### To set the message tracking properties:

1. From the Trading Partner Management home page, select the **Configuration** module.
2. Set the message tracking properties as required. See the table following this procedure for settings.
3. Click **Submit** to save your changes and return to the Trading Partner Management home page.

The following table summarizes settings available on the General Configuration page.

Setting	Description	Required/ Optional
From the <b>Message Tracking Level</b> drop-down list, select <b>All</b> , <b>Metadata</b> , or <b>None</b> .	<p>The default message tracking level for trading partner integration. If the tracking level for a service profile is set to <b>Default</b>, the tracking level for the service profile defaults to the setting specified here. The options are:</p> <p><b>All</b> Message metadata and a reference to message contents in the document store are persisted in message tracking tables. Both message metadata and contents are available for view in the Message Tracking module of the console.</p> <p><b>Metadata</b> Only message metadata is persisted in message tracking tables. Message contents are not tracked and are not available for view in the Message Tracking module of the console.</p> <p><b>None</b> No message tracking information or history is stored in repository and no information is available for view in the Message Tracking module of the console.</p>	Required
From the <b>Mode</b> drop-down list, select <b>Test</b> or <b>Production</b> .	The trading partner integration mode. In <b>Test</b> mode service profiles are not required for sending and receiving business messages between collocated trading partners. Default bindings for both partners can be used in test mode.	Required
In the <b>Directory</b> field, enter the path.	The path to a directory used to store messages.	Required if message content is tracked.
Select the <b>Trace Raw Messages Yes</b> or <b>No</b> option button.	When set to <b>Yes</b> , messages are also stored in their raw format (the format of the message as it is sent over the wire). This setting can be useful for debugging purposes.	Required



## Configuring a Proxy Host

The Proxy Configuration page allows you to define a proxy host for trading partner integration.

**Note:** A proxy server is used to protect local network addresses from hackers and restrict and monitor external network access from the network hosting WebLogic Integration.

### To set the proxy host:

1. From the Trading Partner Management home page, select the **Configuration** module.
2. From the left panel, select **Proxy Host**.
3. In the **Proxy Host** field, enter the host name or IP address.
4. In the **Port number of proxy server**, enter the port.
5. Click **Submit** to save your changes and return to the Trading Partner Management home page.

## Configuring Secure Audit Logging

The Audit Log Configuration page allows you to specify whether or not signed messages are logged to the secure audit log. If secure audit logging is enabled, the Secure Timestamp Configuration page allows you to specify the Java class that implements the secure timestamp class.

**Note:** The classes specified for secure audit logging and secure timestamp must be in the server classpath. Changes to the secure audit logging or secure timestamp configuration require server restart.

### To enable or disable secure audit logging:

1. From the Trading Partner Management home page, select the **Configuration** module.
2. From the left panel, select **Secure Audit Log**.
3. Do one of the following:
  - Select the **Disable** option button to disable secure audit logging.
  - Select the **Enable** option button, then enter the class to be used in the **Secure Audit Logging Class** field.

**Note:** The default `com.bea.wli.security.audit.DefaultAuditLogProvider` class is provided.

4. Click **Submit** to save your changes and return to the Trading Partner Management home page.

**To specify the Java class for secure time stamping:**

1. From the Trading Partner Management home page, select the **Configuration** module.
2. From the left panel, select **Secure Timestamp**.
3. In the **Secure Timestamp Class** field, enter the class.  
**Note:** If no class is entered, secure time stamping is disabled.
4. Click **Submit** to save your changes and return to the Trading Partner Management home page.

## Refreshing the Keystore

The Refresh Keystore page allows you to refresh the KeyStores (identity and trust) in memory from the disk.

**To refresh the keystore:**

1. From the Trading Partner Management home page, select the **Configuration** module.
2. From the left panel, select **Refresh Keystore**.
3. Click the **Refresh Keystore** button to refresh the keystore and return to the Trading Partner Management home page.

## Specifying the Certificate Verification Provider

The Certificate Verification Provider page allows you specify the certificate verification provider for trading partner integration. Trading partner integration provides a service provider interface that allows you to insert a Java class that implements an interface that calls out to a third-party service to verify trading partner certificates. Such an implementation, called a certificate verification provider (CVP), can call out to one of the following certificate verification applications:

- A Certificate Revocation List (CRL) implementation
- An Online Certificate Status Protocol (OCSP) implementation that interacts with a trusted third-party entity, such as a certificate authority, for real-time certificate status checking
- Your own certificate verification implementation

To learn how to implement the CVP, see “Using WebLogic Integration Security” in [Deploying WebLogic Integration Solutions](#).

**Note:** The CVP class must be in the server classpath. Changes to the CVP configuration require server restart.

**To specify the certificate verification provider:**

1. From the Trading Partner Management home page, select the **Configuration** module.
2. From the left panel, select **Certificate Verification Provider**.
3. In the **Certificate Verification Provider** field, enter the CVP Java class.
4. Click **Submit** to save your changes and return to the Trading Partner Management home page.

## Adding Trading Partner Profiles

The Add Trading Partner Profile page allows you to create a new trading partner profile.

**To add a trading partner profile:**

1. From the Trading Partner Management home page, select the **Profile Management** module.
2. From the left panel, select **Create New**.
3. Set trading partner profile properties as required. See “[Defining Trading Partner Profiles](#)” on page 8-30 for a description of the available settings.
4. Click **Submit**.

The View and Edit Trading Partner Profile page is displayed with the new profile definition.

**Note:** If there is an error, the Add Trading Partner Profile page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

5. Do one or more of the following:

- To add certificates to the trading partner, see [“Adding Certificates to a Trading Partner” on page 8-15](#).
- To add bindings to the trading partner, see [“Adding Protocol Bindings to a Trading Partner” on page 8-19](#).
- To add a custom extension to the trading partner, see [“Adding a Custom Extension to a Trading Partner” on page 8-19](#).

## Adding Certificates to a Trading Partner

The Add Certificate page allows you to add certificates to a trading partner profile.

**Note:** You can also add a certificate from the Add Trading Partner Binding or Edit Trading Partner Binding page by clicking the **Configure** link to the left of the **Signature Certificate** drop-down list. If you are adding a certificate in this way, start with step 3 of the following procedure.

### To select the type of certificate:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Certificates** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. Click the **Add Certificate** button to display the Add Certificate (Step 1 of 2) page.
3. Select one of the following options:
  - **Generate a certificate for TEST USE only**  
Select this option to create a client, signature, or encryption certificate definition. The certificate generated is a self-signed certificate appropriate for use only in testing.
  - **Import certificate from file**  
Select this option to create a client, signature, or encryption certificate definition, and to import the certificate file(s) from the local file system into the configured key store.
  - **Use alias for an already imported certificate**  
Select this option to create a reference to an existing client, signature, encryption, or server certificate definition.
4. Click **Next** to display the Add Certificate (Step 2 of 2) page. Refer to the procedure appropriate to the selected type:
  - [“Creating a Certificate for Testing” on page 8-16](#)
  - [“Creating and Importing the Files for a Certificate” on page 8-17](#)
  - [“Creating a Reference to an Existing Certificate” on page 8-18](#)

## Creating a Certificate for Testing

After you select **Generate a certificate for TEST USE only** and click **Next**, the Add Certificate (Step 2 of 2) page is displayed. This page allows you to create a client, signature, or encryption certificate definition. The certificate generated is appropriate for use only in testing.

### To create a certificate for testing:

1. In the **Name** field, enter the name used to identify the certificate within the system. This name is also the entry name in the local keystore.
2. From the **Type** drop-down list, select the type:
  - For a local trading partner, the options are **CLIENT**, **SIGNATURE**, or **ENCRYPTION**.
  - For a remote trading partner, the options are **CLIENT**, **SERVER**, **SIGNATURE**, or **ENCRYPTION**.
3. From the **Password Alias** drop-down list, select the password alias for the password associated with the keystore entry. This alias is used to retrieve the required password from the password store. See [“Password Aliases and the Password Store”](#) on page 9-6.

**Note:** If you have not yet defined an entry for the password in the password store, click **Add Alias**. After you add the entry, you are returned to the Add Certificate page. The newly added alias is now included in the drop-down list.
4. Check the **Import Certificate in Keystore** check box.
5. Click **Create Certificate**.

The View and Edit Trading Partner Profile page is displayed. The certificate is included in the certificates summary table.

**Note:** If there is an error, the Add Certificate page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Creating and Importing the Files for a Certificate

After you select **Import certificate from file** and click **Next**, the Add Certificate (Step 2 of 2) page is displayed. This page allows you to create a client, signature, or encryption certificate definition, and to import the certificate files.

### To create a certificate definition and import the certificate files:

1. In the **Name** field, enter the name used to identify the certificate within the system. This name is also the entry name in the local keystore.
2. From the **Type** drop-down list, select the type:
  - For a local trading partner, the options are **CLIENT**, **SIGNATURE**, or **ENCRYPTION**.
  - For a remote trading partner, the options are **CLIENT**, **SERVER**, **SIGNATURE**, or **ENCRYPTION**.
3. From the **Password Alias** drop-down list, select the password alias for the password associated with the keystore entry. This alias is used to retrieve the required password from the password store. See [“Password Aliases and the Password Store”](#) on page 9-6.
 

**Note:** If you have not yet defined an entry for the password in the password store, click **Add Alias**. After you add the entry, you are returned to the Add Certificate page. The newly added alias is now included in the drop-down list.
4. Do one of the following to specify the location of the certificate file:
  - Click the **Browse** button to the right of the **Import Certificate Location** field, then locate the certificate file. Select the file and click **Open**.
  - Enter the path to the certificate file in the **Import Certificate Location** field.
5. To specify the location of the private key file for a **LOCAL** trading partner, do one of the following:
  - Click the **Browse** button to the right of the **Private Key Location** field, then locate the private key file. Select the file and click **Open**.
  - Enter the path to the private key file in the **Private Key Location** field.
6. Check the **Import Certificate in Keystore** check box.

7. Click **Create Certificate**.

The View and Edit Trading Partner Profile page is displayed. The certificate is included in the certificates summary table.

**Note:** If there is an error, the Add Certificate page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Creating a Reference to an Existing Certificate

After you select **Use alias for an already imported certificate** and click **Next**, the Add Certificate (Step 2 of 2) page is displayed. This page allows you to create a reference to an existing client, signature, encryption, or server certificate definition.

### To create a reference to an existing certificate definition:

1. In the **Name** field, enter the name used to identity the certificate within the system.
2. From the **Type** drop-down list, select **CLIENT**, **SERVER**, **SIGNATURE**, or **ENCRYPTION**.
3. From the **Password Alias** drop-down list, select the password alias for the password associated with the keystore entry. This alias is used to retrieve the required password from the password store. See [“Password Aliases and the Password Store” on page 9-6](#).

**Note:** If you have not yet defined an entry for the password in the password store, click **Add Alias**. After you add the entry, you are returned to the Add Certificate page. The newly added alias is now included in the drop-down list.

4. Click **Create Certificate**.

The View and Edit Trading Partner Profile page is displayed. The certificate reference is included in the certificates summary table.

**Note:** If there is an error, the Add Certificate page is redisplayed. A message indicating the problem is displayed above the input requiring correction.



## Adding Protocol Bindings to a Trading Partner

The Add Binding page allows you to add bindings to a trading partner profile.

### To add a binding to a trading partner profile:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. Click the **Add Binding** button to display the Add Binding (Step 1 of 2) page.
3. Select the **ebXML 1.0**, **ebXML 2.0**, **RosettaNet 1.1**, **RosettaNet 2.0**, or **Web Service** option button.
4. Click **Create Binding** to display the Add Binding (Step 2 of 2) page.
5. Set the binding properties as required. See [“Defining Protocol Bindings” on page 8-31](#) for a description of the available settings.
6. Click **Submit**.

The View and Edit Trading Partner Profile page is displayed. The binding is included in the binding summary table.

**Note:** If there is an error, the Add Binding page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

7. If the new binding is an ebXML 1.0 or ebXML 2.0 binding, you can configure signature transforms as described in [“Configuring Signature Transforms for ebXML Bindings” on page 8-55](#).

## Adding a Custom Extension to a Trading Partner

The default properties associated with a trading partner can be augmented to support application-specific requirements through the addition of a custom extension. A custom extension is modeled in the repository so that defined properties can be retrieved as subtrees within an XML document. The properties can be retrieved using the TPM control.

The extension is composed of a user-defined root element that contains well-formed XML elements and attributes that define the required properties. The user-defined root element is a child of the `<extended-property-set>` element, which is the last child of the `<trading-partner>` element. The following example shows the XML representation of a trading partner with a custom extension.

### Custom Extension Example

```
...
<trading-partner
  name="ABC"
  business-id-type="duns"
  business-id="123123123"
  phone="+1 123 456 7890">
  email="admin@abc.com"
  <address>123 ABC Street., Anytown, CA 95131</address>
  <extended-property-set
    name="ABC International Extension"
    description="Contact">
      <myxmllement>
        <business-contact>Joe Smith</business-contact>
        <phone type="work">+1 123 456 7654</phone>
        <phone type="cell">+1 321 654 4567</phone>
        <city>Anytown</city>
        <state>California</state>
      </myxmllement>
    </extended-property-set>
  </trading-partner>
...
```

An administrator can add a custom extension as described in the following procedure, or by importing a trading partner data file that contains an XML representation of the extended properties as described in [“Importing Management Data” on page 8-67](#).

### To add custom properties to a trading partner profile:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Custom Extension** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. Click the **Add Custom Extension** button to display the Add Custom Extension page.
3. In the **Name** field, enter a name for the custom extension.
4. In the **Description** field, enter an optional description.
5. In the **XML** field, enter the XML document.

The extension is composed of a user-defined root element that contains well-formed XML elements and attributes that define the required properties. For example, the XML highlighted in bold in the [“Custom Extension Example” on page 8-20](#) constitutes a valid entry.

6. Click **Create Custom Extension**.

The View and Edit Trading Partner Profile page is displayed. The custom extension is displayed in the Custom Extension summary table.

**Note:** If there is an error, the Add Custom Extension page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Adding Services

The Add Service page allows you to create a new service definition.

### To add a service:

1. From the Trading Partner Management home page, select the **Service Management** module.
2. From the left panel, select **Create New**.

3. Do one of the following:
  - To locate a newly deployed ebXML or RosettaNet processes and associated controls, click the **Browse** button to the right of the **Name** field. Click the name of the process or control to select it. Skip to step 6. (The **Type** and **Business Protocol** are specified based on the process or control you select.)
  - To specify a web service, enter the service URI in the **Name** field.
4. From the **Type** drop-down list, select **Service Control**, **Process**, or **Web Service** to specify the type of service.
5. From the **Business Protocol** drop-down list, select **EBXML**, **ROSETTANET**, or **WEBSERVICE** to specify the service protocol.
6. In the **Description** field, enter an optional description of the service.
7. Click **Submit**.

The View and Edit Service Details page is displayed with the new definition.

**Note:** If there is an error, the Add Service page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
8. To add service profiles to the service, see [“Adding Service Profiles to a Service” on page 8-22](#).

## Adding Service Profiles to a Service

The View and Edit Service Details page allows you to add service profiles to a service.

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the service name to select it.

The View and Edit Service Details page is displayed.
3. Click the **Add Service Profile** button to display the Add Service Profile page.
4. From the **Status** drop-down list, select **Enabled** or **Disabled**.
5. From the **Message Tracking Level** drop-down list, select one of the following:
  - **ALL**

Message metadata and a reference to message contents in the document store are persisted in message tracking tables. Both message metadata and contents are available for view in the Message Tracking module of the console.

- **DEFAULT**

The tracking level for this profile is set to the system default tracking level. See [“Configuring the Mode and Message Tracking” on page 8-9](#).

- **METADATA**

Only message metadata is persisted in message tracking tables. Message contents are not tracked and are not available for view in the Message Tracking module of the console.

- **NONE**

No message tracking information is sent to the message tracking JMS queue, therefore, no message history is stored in repository and no information is available for view in the Message Tracking module of the console.

6. Configure the **Local** trading partner as follows:

- a. From the **Name** drop-down list, select the name of the trading partner.
- b. From the **Binding** drop-down list, select the binding. Only bindings of the same type as the **Business Protocol** defined for the service are allowed.

The **Endpoint** field displays the URL for the transport endpoint for the selected binding.

7. Configure the **Remote** trading partner as follows:

- a. From the **Name** drop-down list, select the name of the trading partner.
- b. From the **Binding** drop-down list, select the binding. Only bindings of the same type as the **Business Protocol** defined for the service are allowed.

The **Endpoint** field displays the URL for the transport endpoint for the selected binding.

8. Click **Submit**.

You are prompted with the following message” “Do you wish to configure authentication?”

9. Do one of the following:

- Click **Yes**. Go to step 4 of “To add HTTPS authentication to a service profile” or “To add HTTP authentication to a service profile” in [“Adding Authentication to a Service Profile” on page 8-24](#).
- Click **No**. You can configure authentication later as described in [“Adding Authentication to a Service Profile” on page 8-24](#).

The View and Edit Service Details page is displayed. The new profile is displayed in the service profile summary table.

**Note:** If there is an error, the Add Service Profile page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Adding Authentication to a Service Profile

The View Service Profile page allows you to configure the authentication properties for the local and remote trading partners.

When you add authentication to a service profile, the required authentication configuration is added to each respective trading partner binding. The authentication configuration associated with a binding can be updated or deleted as described in [“Updating or Deleting Authentication” on page 8-53](#).

The following table summarizes the available modes of authentication by transport protocol and describes the authentication properties added to each trading partner binding.

Transport Protocol	Authentication Mode	Local Trading Partner (LocalTP) Configuration	Remote Trading Partner (RemoteTP) Configuration
HTTP	Basic	<b>Client Trading Partner:</b> RemoteTP	<b>Client Trading Partner:</b> LocalTP  <b>Username and Password Alias:</b> RemoteTP username and password (the password alias for the password is specified). The username and password required to access the RemoteTP transport endpoint.

Transport Protocol	Authentication Mode	Local Trading Partner (LocalTP) Configuration	Remote Trading Partner (RemoteTP) Configuration
HTTPS	One-Way	<b>Client Trading Partner:</b> RemoteTP	<b>Client Trading Partner:</b> LocalTP  <b>Server Certificate:</b> RemoteTP server certificate to be used for SSL authentication.
	One-Way with Basic	<b>Client Trading Partner:</b> RemoteTP	<b>Client Trading Partner:</b> LocalTP  <b>Username and Password Alias:</b> RemoteTP username and password (the password alias for the password is specified). The username and password required to access the RemoteTP transport endpoint.  <b>Server Certificate:</b> RemoteTP server certificate to be used for SSL authentication.
	Mutual	<b>Client Trading Partner:</b> RemoteTP  <b>Client Certificate:</b> RemoteTP client certificate to be used for SSL mutual authentication.	<b>Client Trading Partner:</b> LocalTP  <b>Client Certificate:</b> LocalTP client certificate to be used for SSL mutual authentication.  <b>Server Certificate:</b> RemoteTP server certificate to be used for SSL authentication.

### To add HTTPS authentication to a service profile:

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the service name to select it.  
The View and Edit Service Details page is displayed.
3. In the Service Profiles table, click the **View** link for the service profile entry. (The **View** link is in the third column from the right.)  
The View Service Profile page is displayed.

4. Click **Configure Authentication**.

You are prompted to select the authentication mode for the local and remote trading partners as shown in the following figure:

Choose type of Authentication Mode

LOCAL

☐ One Way

☐ One Way with Basic

☒ Mutual

REMOTE

☐ One Way

☐ One Way with Basic

☒ Mutual

**Note:** Although it is not enforced, typically the same type of authentication is selected for both the local and remote trading partner.

- 5. Select the **One Way**, **One-Way with Basic**, or **Mutual** option button to specify the type for the **Local** trading partner.
- 6. Select the **One Way**, **One-Way with Basic**, or **Mutual** option button to specify the type for the **Remote** trading partner.
- 7. Click the **Next** button.
- 8. Select the certificate(s), or enter the username and password alias, required for the selected type. The following table summarizes the settings by authentication type.

Authentication Type	Local	Remote
One-Way	No local setting.	Select the <b>Server Certificate</b> from the drop-down list.
One-Way with Basic	Enter the <b>Username</b> required to access the remote endpoint.  Select the <b>Password Alias</b> from the drop-down list.	Select the <b>Server Certificate</b> from the drop-down list.
Mutual	Select the <b>Client Certificate</b> from the drop-down list.	Select the <b>Client Certificate</b> from the drop-down list.  Select the <b>Server Certificate</b> from the drop-down list.



**Note:** If the certificate has not yet been added, click the **Add Certificate** link to the right of the drop-down list. See [“Adding Certificates to a Trading Partner” on page 8-15](#) for instructions. Once the certificate has been added, it is available for selection. Similarly, if the password alias has not been added, click the **Add Alias** link to the left of the drop-down list. See [“Adding Passwords to the Password Store” on page 9-13](#) for instructions. Once the alias has been added, it is available for selection.

9. To preview the configuration, click **Preview config**. To learn more about the preview function, see [“Previewing the Authentication Configuration:” on page 8-28](#).

10. Click **Add**.

Authentication is added and the View and Edit Service Details page is displayed.

**Note:** If there is an error, the Add Authentication page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

#### To add HTTP authentication to a service profile:

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).

2. Click the service name to select it.

The View and Edit Service Details page is displayed.

3. In the Service Profiles table, click the **View** link for the service profile entry. (The **View** link is in the third column from the right.)

The View Service Profile page is displayed.

4. Click **Configure Authentication**.

The authentication mode is displayed as shown in the following figure:

Choose type of Authentication Mode	
<b>LOCAL</b>	<b>REMOTE</b>
<input checked="" type="radio"/> Basic	<input type="radio"/> Basic

5. Click the **Next** button.
6. Enter the **Username** required to access the remote endpoint.
7. Select the **Password Alias** from the drop-down list.

**Note:** If the password alias has not been added, click the **Add Alias** link to the left of the drop-down list. See [“Adding Passwords to the Password Store” on page 9-13](#) for instructions. Once the alias has been added, it is available for selection.

- 8. To preview to the configuration, click **Preview config**. To learn more about the preview function, see [“Previewing the Authentication Configuration:” on page 8-28](#).
- 9. Click **Add**.

Authentication is added and the View and Edit Service Details page is displayed.

**Note:** If there is an error, the Add Authentication page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

**Previewing the Authentication Configuration:**

The verification of certificates and exchange of public keys that occurs in order to set up a secure channel over which to communicate is known at the SSL handshake. When you configure authentication, you have the option of previewing the configuration.

For the HTTPS transport protocol, the preview provides a summary of the handshake configured as shown in the following figures:

	LOCAL	REMOTE
<b>Name</b>	BEATP	ACME
<b>Type</b>	LOCAL	REMOTE
<b>EndPoint</b>	https://127.0.0.1:7001/ebxml2.0/beatp	https://216.239.50.100:7001/ebxml2.0/ACME
<b>Type</b>	One Way	One Way
<===== I N B O U N D =====>		
<----- Server Cert ----->		
===== O U T B O U N D =====>		
<----- Server Cert (ACME-server) ----->		

	LOCAL	REMOTE
<b>Name</b>	BEATP	ACME
<b>Type</b>	LOCAL	REMOTE
<b>EndPoint</b>	https://127.0.0.1:7001/ebxml2.0/beatp	https://216.239.50.100:7001/ebxml2.0/ACME
<b>Type</b>	One Way with Basic	One Way with Basic
<===== I N B O U N D =====>		
<----- UserName/Password ----->		
<----- Server Cert ----->		
===== O U T B O U N D =====>		
<----- UserName/Password ----->		
<----- Server Cert (ACME-server) ----->		

	LOCAL	REMOTE
Name	BEATP	ACME
Type	LOCAL	REMOTE
EndPoint	https://127.0.0.1:7001/ebxml2.0/beatp	https://216.239.50.100:7001/ebxml2.0/ACME
Type	Mutual	Mutual
<===== I N B O U N D =====>		
----- Server Cert ----->		
<----- Client Cert (ACME-client) -----		
===== O U T B O U N D =====>		
<----- Server Cert (ACME-server) -----		
----- Client Cert (beatp-client) ----->		

For HTTP basic authentication, the preview displays the configuration as shown in the following figure:

	LOCAL	REMOTE
Name	BEATP	ACME
Type	LOCAL	REMOTE
EndPoint	http://127.0.0.1:7001/ebXML20/BEATP-id	http://216.239.50.100:7001/ebxml2.0/ACME
Type	Basic	Basic
<===== I N B O U N D =====>		
<----- UserName/Password -----		
===== O U T B O U N D =====>		
----- UserName/Password ----->		

## Defining Trading Partner Profiles

The Add Trading Partner Profile and Edit Trading Partner Profile pages allow you to define the properties of a profile. The following table summarizes the available settings.

Setting	Description	Required/ Optional
In the <b>Name</b> field, enter the name.	<p>The name used to identify the trading partner within the system. Do not use spaces.</p> <p><b>Note:</b> This field is only available on the Add Trading Partner Profile page. It cannot be edited on the Edit Trading Partner Profile page.</p>	Required
In the <b>Description</b> field, enter a description.	An optional description. This value is for administrative purposes only. It is not included in messages.	Optional
In the <b>Business ID</b> field, enter an appropriate identifier.	Identifier for the trading partner. The value is used to identify the partner in message exchanges.	Required
In the <b>Business ID Type</b> field, enter the type of <b>Business ID</b> .	The type or naming convention for the <b>Business ID</b> . For example, if the value entered for <b>Business ID</b> is a D-U-N-S number, enter <b>DUNS</b> for the <b>Business ID Type</b> .	Optional
Check or uncheck the <b>Default Trading Partner</b> check box.	<p>When checked, the trading partner is designated the default trading partner for sending or receiving messages for the local host system. <b>Default Trading Partner</b> can only be checked if <b>Type</b> is set to <b>LOCAL</b>. Only one <b>LOCAL</b> trading partner can be designated the default.</p> <p>The default is unchecked.</p>	Optional
From the <b>Type</b> drop-down list, select <b>LOCAL</b> or <b>REMOTE</b> .	<p>Specifies whether the trading partner is hosted locally or represents an external, remote trading partner.</p> <p>The default is <b>LOCAL</b>.</p>	Optional

Setting	Description	Required/ Optional
From the <b>Status</b> drop-down list, select <b>ENABLED</b> or <b>DISABLED</b> .	<p>Specifies whether or not to allow business messages to be sent or received by the partner</p> <p>You cannot set the <b>Status</b> to <b>DISABLED</b> until all service profiles associated with the partner are disabled. If you attempt to set the <b>Status</b> to <b>DISABLED</b>, you are prompted to disable any enabled service profiles before the change takes effect.</p> <p>Setting the <b>Status</b> to <b>ENABLED</b> does not automatically enable the service profiles associated with the trading partner. After you enable the trading partner profile, you must enable the associated service profiles as described in <a href="#">“Enabling and Disabling Trading Partner and Service Profiles” on page 8-64</a>.</p> <p>The default is <b>ENABLED</b>.</p>	Optional
In the <b>Email</b> field, enter an email address.	A contact email address for the trading partner.	Optional
In the <b>Address</b> field, enter a mailing address.	A mailing address for the trading partner.	Optional
In the <b>Phone</b> field, enter a telephone number.	A contact telephone number for the trading partner.	Optional
In the <b>Fax</b> field, enter a fax number.	A fax number for the trading partner.	Optional
In the <b>WLS User Name</b> field, enter a valid user name.	The user name that is used to authorize remote trading partners at the transport level. This user must exist in the default security realm. See <a href="#">“Listing and Locating Users” on page 10-16</a> . The value applies only if <b>Type</b> is set to <b>Remote</b> .	Optional

## Defining Protocol Bindings

The Add Binding and Edit Binding pages allow you to define the properties for the protocol bindings. The following sections describe the available settings for each protocol type:

- [Defining an ebXML 1.0 or 2.0 Binding](#)
- [Defining a RosettaNet 1.1 or 2.0 Binding](#)

- [Defining a Web Service Binding](#)

## Defining an ebXML 1.0 or 2.0 Binding

The following table describes the settings available for an ebXML 1.0 or 2.0 binding.

Setting	Description	Required/ Optional
In the <b>Name</b> field, enter the binding name.	<p>The name used to identify the binding within the system. The name must be unique within the trading partner profile. Naming conventions, such as the following, are typically used in naming the binding:</p> <pre>&lt;partner&gt;-&lt;protocol&gt;&lt;version&gt;-&lt;transport&gt;-&lt;qualifier&gt;-binding</pre> <p>For example:</p> <pre>acme-ebxml120-https-reliable-binding</pre> <p><b>Note:</b> This field is only available on the Add Binding page. It cannot be edited on the Edit Binding page.</p>	Required
Check or uncheck the <b>Default Binding</b> check box.	<p>When checked, the binding is designated as the default binding for the ebXML protocol. Only one binding of the same protocol version can be designated the default binding.</p> <p>The default is unchecked.</p>	Optional
<b>Transport Configuration</b>		
From the <b>Transport Protocol</b> drop-down list, select the <b>HTTP</b> or <b>HTTPS</b> .	<p>The transport protocol for sending and receiving messages.</p> <p>The default is <b>HTTP</b>.</p>	Optional
From the <b>Transport Protocol Version</b> , select the version.	<p>The version of the transport protocol.</p> <p>If <b>HTTP</b> is selected for the Transport Protocol, select <b>1.0</b> or <b>1.1</b>. The default is <b>1.0</b>.</p> <p>If <b>HTTPS</b> is selected for Transport Protocol, <b>1.1</b> is currently the only option.</p>	Optional
In the <b>Endpoint</b> field, enter the <b>URL</b> for the transport endpoint.	The URL for the transport endpoint.	Required

Setting	Description	Required/ Optional
In the <b>Timeout</b> field, enter the transport timeout.	The transport timeout for the specified Endpoint. The default value is <b>0</b> , which indicates <b>no timeout</b> .	Optional
<b>Quality of Service</b>		
<p>From the <b>Delivery Semantics</b> drop-down list, do one of the following:</p> <ul style="list-style-type: none"> <li>For <b>ebXML 1.0</b>, select <b>BESTEFFORT</b> or <b>ONCEANDONLYONCE</b></li> <li>For <b>ebXML 2.0</b>, select <b>BESTEFFORT</b>, <b>ONCEANDONLYONCE</b>, <b>ATLEASTONCE</b>, or <b>ATMOSTONCE</b></li> </ul>	<p>The reliable message service behavior:</p> <p><b>BESTEFFORT</b> Best effort. No reliable messaging.</p> <p><b>ONCEANDONLYONCE</b> Once and only once reliable messaging. Select this option for messaging that requires acknowledgement and duplicate elimination.</p> <p><b>ATLEASTONCE</b> At least once reliable messaging. Select this option for messaging that requires acknowledgement, but not duplicate elimination.</p> <p><b>ATMOSTONCE</b> At most once reliable messaging. Select this option for messaging that requires duplicate elimination, but not acknowledgement.</p>	Required
In the <b>Retry Count</b> field, enter the number of retries.	<p>The maximum number of retries for sending a reliably delivered message. The default is <b>0</b>.</p> <p>The value is ignored if <b>BESTEFFORT</b> or <b>ATMOSTONCE</b> is selected for <b>Delivery Semantics</b>. If <b>ONCEANDONLYONCE</b> or <b>ATLEASTONCE</b> is selected, the message is retried until the acknowledgement is received or the number of retries specified in the <b>Retry Count</b> field is exhausted.</p>	Required if <b>ONCEANDONLYONCE</b> or <b>ATLEASTONCE</b> is selected,

Setting	Description	Required/ Optional
In the <b>Retry Interval</b> field, enter the interval.	<p>The time interval before a message is resent following a timeout waiting for a message acknowledgement. The default is <b>1 min</b>.</p> <p>The following are valid entries:            500 ms or 500 msecs,            5 s, or 5 sec, or 5 secs            5 m or 5 mins            5 h or 5 hours            5 d or 5 days</p> <p>Any combination of the above are also valid. For example:            1 d 5 h            1 sec 500 ms</p>	Required if <b>Retry Count</b> is 1 or greater.
In the <b>Persist Duration</b> , enter the interval.	Specifies the duration for which messages have to be stored persistently for the purpose of duplicate elimination. The default is <b>0</b> .	Required if <b>ONCEANDONLYONCE</b> or <b>ATMOSTONCE</b> is selected,
<b>XML Digital Signature Configuration for Non-Repudiation</b>		
<p>From the <b>Signature Certificate</b> drop-down list, select an existing certificate or <b>NONE</b>.</p> <p>If you have not yet added the certificate, click <b>Configure</b> and follow the instructions in <a href="#">“Adding Certificates to a Trading Partner”</a> on page 8-15.</p>	The name of the signature certificate used to digitally sign messages. <b>NONE</b> indicates no digital signature.	Optional
Check or uncheck the <b>Signature Required</b> check box.	<p>When checked, the message is digitally signed using the signature certificate of the trading partner sending the message. The default is unchecked.</p> <p>Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See <a href="#">“Configuring Secure Audit Logging”</a> on page 8-11.</p>	Optional



Setting	Description	Required/ Optional
Check or uncheck the <b>Signature Receipt Required</b> check box.	<p>When checked, the message is acknowledged by a digitally signed receipt acknowledgement message using the signature certificate of the trading partner sending the acknowledgement. The default is unchecked.</p> <p>Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See <a href="#">“Configuring Secure Audit Logging” on page 8-11</a>.</p>	Optional
<p><b>Note:</b> Within WebLogic Integration, the ebXML protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the settings for the <b>Signature Required</b> and <b>Signature Receipt Required</b> properties of the binding. In addition to the preceding properties:</p> <ul style="list-style-type: none"> <li>• A predefined set of algorithms and parameters are provided by the WebLogic Integration implementation. To learn more about the implementation, see “Using WebLogic Integration Security” in <a href="#">Deploying WebLogic Integration Solutions</a>.</li> <li>• Optional XPath filtering transforms can be applied to messages for signing purposes. See <a href="#">“Configuring Signature Transforms for ebXML Bindings” on page 8-55</a>.</li> </ul>		

## Defining a RosettaNet 1.1 or 2.0 Binding

The following table describes the settings available for a RosettaNet 1.1 or 2.0 binding.

Setting	Description	Required/ Optional
In the <b>Name</b> field, enter the binding name.	<p>The name used to identify the binding within the system. The name must be unique within the trading partner profile. Naming conventions, such as the following, are typically used in naming the binding:</p> <pre>&lt;partner&gt;-&lt;protocol&gt;&lt;version&gt;-&lt;transport&gt;-&lt;qualifier&gt;-binding</pre> <p>For example:</p> <pre>acme-rosettanet20-https-encryption-binding</pre> <p><b>Note:</b> This field is only available on the Add Binding page. It cannot be edited on the Edit Binding page.</p>	Required
Check or uncheck the <b>Default Binding</b> check box.	When checked, the binding is designated as the default binding for the RosettaNet protocol. Only one binding of the same protocol version can be designated the default binding.	Required
<b>Transport Configuration</b>		
From the <b>Transport Protocol</b> drop-down list, select the <b>HTTP</b> or <b>HTTPS</b> .	The transport protocol for sending and receiving messages.	Required
From the <b>Transport Protocol Version</b> , select the version.	<p>The version of the transport protocol.</p> <p>If <b>HTTP</b> is selected for the Transport Protocol, select <b>1.0</b> or <b>1.1</b>.</p> <p>If <b>HTTPS</b> is selected for Transport Protocol, <b>1.1</b> is currently the only option.</p>	Required
In the <b>Endpoint</b> field, enter the <b>URL</b> for the transport endpoint.	The URL for the transport endpoint.	Required
In the <b>Timeout</b> field, enter the transport timeout.	The transport timeout for the specified endpoint. The default value is <b>0</b> , which indicates <b>no timeout</b> .	Required

Setting	Description	Required/ Optional
<b>Quality of Service</b>		
In the <b>Retry Count</b> field, enter the number of retries.	The number of times a RosettaNet message should be retried in case of failure. The default is <b>0</b> .	Required
In the <b>Retry Interval</b> field, enter the interval.	<p>The amount of time to wait between subsequent retries. The default is <b>1 min</b>.</p> <p>The following are valid entries:            500 ms or 500 msecs,            5 s, or 5 sec, or 5 secs            5 m or 5 mins            5 h or 5 hours            5 d or 5 days</p> <p>Any combination of the above are also valid. For example:            1 d 5 h            1 sec 500 ms</p>	Required for if <b>Retry Count</b> is 1 or greater.
In the <b>Process Timeout</b> , enter the interval.	Specifies the amount of time a PIP can be active without completion before timing out. The default is <b>0</b> .	Optional
<b>Note:</b> The values specified for <b>Retry Count</b> , <b>Retry Interval</b> , and <b>Process Timeout</b> are not directly enforced by the RosettaNet messaging runtime. These values can be accessed from a business process that implements a RosettaNet process.		
<b>Message-Level Encryption (RosettaNet 2.0 Only)</b>		
<p>From the <b>Encryption Certificate</b> drop-down list, select an existing certificate or <b>NONE</b>.</p> <p>If you have not yet added the certificate, click <b>Configure</b> and follow the instructions in <a href="#">“Adding Certificates to a Trading Partner”</a> on page 8-15.</p>	The name of the encryption certificate used to encrypt and decrypt messages. <b>NONE</b> indicates no message-level encryption. The default is <b>NONE</b> .	Optional

Setting	Description	Required/ Optional
From the <b>Encryption Level</b> drop-down list, select <b>NONE</b> , <b>PAYLOAD</b> , or <b>ENTIRE_PAYLOAD</b> .	<p>The encryption level specifies how much of the message content is to be encrypted. Select <b>PAYLOAD</b> to encrypt only the XML business document(s) part of the message.</p> <p>Select <b>ENTIRE_PAYLOAD</b> if you want to encrypt the business documents and all attachments in the message.</p> <p>The default is <b>NONE</b>.</p>	Optional
From the <b>Cipher Algorithm</b> drop-down list, select <b>NONE</b> , <b>RC5</b> , <b>DES</b> , or <b>3DES</b> .	<p>Type of cipher algorithm:</p> <p>If <b>RC5</b> is selected, the algorithm object identifier passed to the RSA security code is <code>RC5-0x10-32-16/CBC/PKCS5Padding</code>. If the algorithm object identifier is equal to <code>RC5-0x10-32-16/CBC/PKCS5Padding</code>, then an RC5 in CBC mode, with the PKCS5 padding algorithm, is used to encrypt the message.</p> <p>If <b>DES</b> is selected, the algorithm object identifier passed to the RSA security code is <code>DES/CBC/PKCS5Padding</code>. If the algorithm object identifier is equal to <code>DES/CBC/PKCS5Padding</code>, then a DES in CBC mode with the PKCS5 padding algorithm, is used to encrypt the message.</p> <p>If <b>3DES</b> is selected, the algorithm object identifier passed to the RSA security code is <code>3DES_EDE/CBC/PKCS5Padding</code>. If the algorithm object identifier is equal to <code>3DES_EDE/CBC/PKCS5Padding</code>, then a Triple DES in EDE mode, with the PKCS5 padding algorithm, is used to encrypt the message. A domestic license is required.</p> <p>The default is <b>NONE</b>.</p>	Required if Encryption Level is <b>PAYLOAD</b> or <b>ENTIRE_PAYLOAD</b>
<b>XML Digital Signature Configuration for Non-Repudiation</b>		
From the <b>Signature Certificate</b> drop-down list, select the certificate.	<p>The name of the signature certificate to be used for digitally signing messages. If you have not yet added the certificate, click Configure. To learn how to add a certificate, see <a href="#">“Adding Certificates to a Trading Partner” on page 8-15</a> for instructions.</p>	
Check or uncheck the <b>Signature Required</b> check box.	<p>When checked, the message is digitally signed using the signature certificate of the trading partner sending the message. The default is unchecked.</p> <p>Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See <a href="#">“Configuring Secure Audit Logging” on page 8-11</a>.</p>	Required

Setting	Description	Required/ Optional
Check or uncheck the <b>Signature Receipt Required</b> check box.	<p>When checked, the message is acknowledged by a digitally signed receipt acknowledgement message using the signature certificate of the trading partner sending the acknowledgement. The default is unchecked.</p> <p>Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See <a href="#">“Configuring Secure Audit Logging” on page 8-11</a>.</p>	Required
<p><b>Note:</b> Within WebLogic Integration, the RosettaNet protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the settings for the <b>Signature Required</b> and <b>Signature Receipt Required</b> properties of the binding. For all RosettaNet messages, the non-repudiation protocol is <b>PKCS7</b>, the hash function is <b>SHA1</b>, and the signature algorithm is <b>RSA</b>.</p> <p>In addition to the preceding properties:</p> <ul style="list-style-type: none"> <li>A predefined set of algorithms and parameters are provided by the WebLogic Integration implementation. To learn more about the implementation, see “Using WebLogic Integration Security” in <a href="#">Deploying WebLogic Integration Solutions</a>.</li> <li>PIP failure notification can also be configured by the administrator. See <a href="#">“Configuring PIP Notification of Failure Roles for RosettaNet Bindings” on page 8-57</a>.</li> </ul>		



## Defining a Web Service Binding

The following table describes the settings available for a Web service binding.



Setting	Description	Required/ Optional
In the <b>Name</b> field, enter the binding name.	<p>The name used to identify the binding within the system. The name must be unique within the trading partner profile. Naming conventions, such as the following, are typically used in naming the binding:</p> <pre>&lt;partner&gt;-&lt;protocol&gt;-&lt;transport&gt;-&lt;qualifier&gt;-binding</pre> <p>For example:</p> <pre>acme-webservice-http-binding</pre> <p><b>Note:</b> This field is only available on the Add Binding page. It cannot be edited on the Edit Binding page.</p>	Required
<b>Transport Configuration</b>		
From the <b>Transport Protocol</b> drop-down list, select the <b>HTTP</b> , <b>HTTPS</b> , or <b>JMS</b> .	The transport protocol for sending and receiving messages.	Required
From the <b>Transport Protocol Version</b> drop-down list, select the version.	<p>The version of the transport protocol.</p> <p>If <b>HTTP</b> is selected for the Transport Protocol, select <b>1.0</b> or <b>1.1</b>.</p> <p>If <b>HTTPS</b> is selected for Transport Protocol, <b>1.1</b> is currently the only option.</p> <p>This value is ignored if <b>JMS</b> is selected.</p>	Required
In the <b>Endpoint</b> field, enter the <b>URL</b> for the transport endpoint.	The URL for the transport endpoint.	Required
In the <b>Timeout</b> field, enter the transport timeout.	The transport timeout for the specified endpoint. The default value is <b>0</b> , which indicates <b>no timeout</b> .	Required





## Listing and Locating Trading Partners

The View and Edit Trading Partner Profiles list displays the following information for each trading partner:

Property	Description
Trading Partner Name	The name assigned to the trading partner. The name is a link to the View and Edit Trading Partner Profile page for the partner.
Type	The trading partner type (local or remote).
Business ID	Identifier for the trading partner. The value is used to identify the partner in message exchanges.
Description	An optional description. This value is for administrative purposes only. It is not included in messages.
Status	<p>Status of the trading partner:</p> <ul style="list-style-type: none"> <li>• A red light  indicates that the trading partner cannot send or receive messages. The trading partner profile and any service profiles associated with the trading partner are disabled.</li> <li>• A green light  indicates that the trading partner profile is enabled. If there are any service profiles associated with the trading partner, they may, or may not, be enabled (the system does not enforce the status of the service profiles for an enabled trading partner).</li> </ul>

### To list and locate trading partners:

1. From the Trading Partner Management home page, select the **Profile Management** module.
2. To locate a specific trading partner do one of the following:
  - Filter by trading partner name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Search**. The partners matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.







- Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Listing and Locating Services

The View and Edit Services list displays the following information for each service:

Property	Description
Service Name	The service URI or control name. The name is a link to the View and Edit Service Details page for the service.
Business Service Name	The business service name as defined for the process. For an ebXML process, this is the <b>ebxml-service-name</b> specified in the <a href="#">@jpd:ebxml Annotation</a> . For a RosettaNet process, this is the <b>pip-name</b> specified in the <a href="#">@jpd:rosettanet Annotation</a> . The business service name is empty for web services.
Description	An optional description. This value is for administrative purposes only. It is not included in messages.
Type	The type of service (process, service control, or web service).
Business Protocol	Business protocol (ebXML, RosettaNet, or web service).

### To list and locate services:

1. From the Trading Partner Management home page, select the **Service Management** module.
2. To locate a specific service do one of the following:
  - Filter by service name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Search**. The services matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.



## Viewing and Changing Trading Partner Profiles

The View and Edit Trading Partner Profile page allows you to view and change the properties of the profile. The following table summarizes the information displayed on the View and Edit Trading Partner Profile page.

Property	Description	Administrator Can Set (Yes/No)
Name	The name used to identify the trading partner within the system.  <b>Note:</b> You cannot update the name of an existing trading partner. To change the name, you must delete the partner, then recreate it with the new name.	No
Business ID	Identifier for the trading partner. The value is used to identify the partner in message exchanges.	Yes
Business ID Type	The type or naming convention for the Business ID (for example, DUNS for a D-U-N-S number).	Yes
Type	Trading partner type (local or remote).	Yes
Status	Status of the trading partner: <ul style="list-style-type: none"> <li>Disabled indicates that the trading partner cannot send or receive messages. The trading partner profile and any service profiles associated with the trading partner are disabled.</li> <li>Enabled indicates that the trading partner can send and receive messages. If there are any service profiles associated with the trading partner, they may, or may not, be enabled (the system does not enforce the status of the service profiles for an enabled trading partner).</li> </ul>	Yes
Description	An optional description. This value is for administrative purposes only. It is not included in messages.	Yes
Default	Indicator of whether or not the trading partner is designated the default trading partner for sending or receiving messages for the local host system (true or false).	Yes
Email	A contact email address for the trading partner.	Yes
Address	A mailing address for the trading partner.	Yes

Property	Description	Administrator Can Set (Yes/No)
Phone	A contact telephone number for the trading partner.	Yes
Fax	A fax number for the trading partner.	Yes
WLS User Name	The user name that is used to authorize remote trading partners at the transport level. (The WLS User name is only displayed for remote trading partners.)	Yes

### Bindings

Binding table	Entry for each binding configured for the trading partner.	Yes
Name	The name assigned to the binding. The name is a link to the View Binding Details page.	
Business Protocol	The business protocol (ebXML, RosettaNet, or web service).	
Default Binding	Indicator of whether or not this is the designated default binding for the local host system (true or false).	
Protocol Version	The protocol version. The value can be 1.0 or 2.0 (ebXML), 1.1 or 2.0 (RosettaNet), or No Data (web service).	
Delete	A <b>Delete</b> link that can be used to delete the entry.	

### Certificates

Certificate table	Entry for each certificate configured for the trading partner.	Yes
Name	The name assigned to the certificate. The name is a link to the View and Edit Trading Partner Certificates page.	
Type	Type of certificate (client, signature, encryption, or server)	
Delete	A <b>Delete</b> link that can be used to delete the entry.	

Property	Description	Administrator Can Set (Yes/No)
<b>Custom Extension</b>		
Custom Extension table	Entry for the custom extension, if one exists.	Yes
	Name      The name assigned to the custom extension. The name is a link to the View and Edit Custom Extension page.	
	Delete      A <b>Delete</b> link that can be used to delete the entry.	

**To view trading partner properties:**

1. Locate the trading partner. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the trading partner name.

The View and Edit Trading Partner Profile page is displayed.

**To change trading partner properties:**

1. On the View and Edit Trading Partner Profile page, click **Edit profile**.
2. Update properties as required. See [“Defining Trading Partner Profiles” on page 8-30](#).
3. Click **Submit**.
4. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View and Edit Trading Partner Profile page is displayed with the new profile definition.

**Note:** If there is an error, the edit page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

5. Do one or more of the following as required:
  - To add certificates to the trading partner, see [“Adding Certificates to a Trading Partner” on page 8-15](#).
  - To add bindings to the trading partner, see [“Adding Protocol Bindings to a Trading Partner” on page 8-19](#).

- To add a custom extension to the trading partner, see [“Adding a Custom Extension to a Trading Partner” on page 8-19](#).
- To update a certificate, see [“Viewing and Changing Certificates” on page 8-46](#).
- To update a binding, see [“Viewing and Changing Bindings” on page 8-47](#).
- To update a custom extension, see [“Viewing and Changing a Custom Extension” on page 8-59](#).

## Viewing and Changing Certificates

The View and Edit Trading Partner Certificates page allows you to:

- View the properties of a certificate.
- Import certificate files to update a certificate.

### To view a certificate for a trading partner:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Certificates** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the certificate table, click the certificate name.

The View and Edit Trading Partner Certificate page is displayed.

### To import files to update a certificate:

1. On the View and Edit Trading Partner Certificate page, click **Edit Certificate**.

The Edit Certificate page is displayed.
2. If required, update the Password alias. From the **Password Alias** drop-down list, select a new password alias.

**Note:** If you have not yet defined an entry for the password in the password store, click **Add Alias**. After you add the entry, you are returned to the Edit Certificate page. The newly added alias is now included in the drop-down list.

3. Do one of the following to specify the location of the certificate file:
  - Click the **Browse** button to the right of the **Import Certificate Location** field, then locate the certificate file. Select the file and click **Open**.
  - Enter the path to the certificate file in the **Import Certificate Location** field.
4. To specify the location of the private key file for a **LOCAL** trading partner, do one of the following:
  - Click the **Browse** button to the right of the **Private Key Location** field, then locate the private key file. Select the file and click **Open**.
  - Enter the path to the private key file in the **Private Key Location** field.
5. Click **Submit**.
6. If any service profiles are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View and Edit Trading Partner Certificate page is displayed.

**Note:** If there is an error, the Edit Certificate page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Viewing and Changing Bindings

The View Binding Details page allows you to:

- View the properties of a binding.
- Change the properties of a binding.
- Configure signature transforms for ebXML bindings.
- Configure the trading partner and delivery channel for the PIP Failure Notifier or PIP Failure Report Administrator roles.

The following table summarizes the information displayed on the View Binding Details page.

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
Name	<p>The name used to identify the binding within the system.</p> <p><b>Note:</b> You cannot update the name, business protocol, or business protocol version of an existing binding. To change these properties, you must delete the binding, then recreate it with the new values.</p>	All binding types	No
Business Protocol	The business protocol (ebXML, RosettaNet, or web service).	All binding types	No
Business Protocol Version	The protocol version. The value can be 1.0 or 2.0 (ebXML), 1.1 or 2.0 (RosettaNet), or No Data (web service).	ebXML 1.0/2.0 RosettaNet 1.1/2.0	No
Default Binding	<p>Indicator of whether or not the binding is designated as the default binding for the protocol (true or false). Only one binding of the same protocol version can be designated the default binding.</p>	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
<b>Transport Configuration</b>			
Transport Protocol	<p>The transport protocol for sending and receiving messages:</p> <ul style="list-style-type: none"> <li>For ebXML or RosettaNet, HTTP or HTTPS.</li> <li>For a web service, HTTP, HTTPS, or JMS.</li> </ul>	All binding types	Yes
Transport Protocol Version	<p>The version of the transport protocol.</p> <ul style="list-style-type: none"> <li>For HTTP 1.0 or 1.1.</li> <li>For HTTPS the value is 1.1.</li> </ul>	All binding types	Yes
Endpoint URL	The URL for the transport endpoint.	All binding types	Yes
Timeout	The transport timeout for the specified endpoint. A value of 0 indicates no timeout.	All binding types	Yes

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
<b>Quality of Service</b>			
Retry Count	The maximum number of retries for sending a reliably delivered message.	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Retry Interval	The retry interval: <ul style="list-style-type: none"> <li>For ebXML reliable messaging, the time interval before a message is resent following a timeout waiting for a message acknowledgement. The default is 1 min.</li> <li>For RosettaNet, the number of times a message should be retried in case of failure.</li> </ul>	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Persist Duration	The duration for which messages have to be stored persistently for the purpose of duplicate elimination.	ebXML 1.0/2.0	Yes
Process Timeout	The amount of time a PIP can be active without completion before timing out.	RosettaNet 1.1/2.0	Yes
Delivery Semantics	The reliable message service behavior: <ul style="list-style-type: none"> <li>Best effort. No reliable messaging.</li> <li>Once and only once reliable messaging. For messaging that requires acknowledgement and duplicate elimination.</li> <li>At least once reliable messaging (ebXML 2.0 only). For messaging that requires acknowledgement, but not duplicate elimination.</li> <li>At most once reliable messaging (ebXML 2.0 only). For messaging that requires duplicate elimination, but not acknowledgement.</li> </ul>	ebXML 1.0/2.0	Yes
<b>Digital Signature Configuration for Non-Repudiation</b>			
Signature Required	Indicator of whether or not the message is digitally signed using the signature certificate of the trading partner sending the message (true or false).	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
Signature Receipt Required	Indicator of whether or not the message is acknowledged by a digitally signed receipt acknowledgement message using the signature certificate of the trading partner sending the acknowledgement (true or false).	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Signature Certificate	The name of the signature certificate used to digitally sign messages.	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Non Repudiation Protocol	The predefined non-repudiation protocol (PKCS7).	RosettaNet 1.1/2.0	No
Hash Function	The predefined hash function (SHA1).	RosettaNet 1.1/2.0	No
Signature Algorithm	The predefined signature algorithm (RSA).	RosettaNet 1.1/2.0	No
<b>Message-Level Encryption Configuration</b>			
Encryption Certificate	The name of the encryption certificate used to encrypt and decrypt messages. None indicates no message-level encryption.	RosettaNet 2.0	Yes
Cipher Algorithm	Type of cipher algorithm (RC5, DES, or 3DES). See <a href="#">“Defining a RosettaNet 1.1 or 2.0 Binding” on page 8-36</a> for a description of the values.	RosettaNet 2.0	Yes
Encryption Level	<p>The encryption level specifies how much of the message content is to be encrypted.</p> <ul style="list-style-type: none"> <li>• PAYLOAD—Only the XML business document(s) part of the message is encrypted.</li> <li>• ENTIRE_PAYLOAD—The business documents and all attachments in the message are encrypted.</li> <li>• NONE—Message is not encrypted.</li> </ul>	RosettaNet 2.0	Yes



Property	Description	Property Applies To	Administrator Can Set (Yes/No)
<b>Authentication</b>			
Authentication table	Entry for each authentication configured for the binding. See <a href="#">“Adding Authentication to a Service Profile”</a> on page 8-24.	All binding types	Yes
	Mode		Basic, one-way, one-way with basic, or mutual.
	Client TP		The name of the trading partner that this authentication applies to.
	Delete		A <b>Delete</b> link that can be used to delete the entry.
<b>PIP Failure</b>			
PIP failure notification table	Entry for PIP notification of failure:	RosettaNet 1.1/2.0	Yes
	Failure Type		Type of failure (Failure Report Admin or Failure Notifier).
	Trading Partner		The trading partner name of the PIP Failure Notifier or PIP Report Administrator role. This specifies the party used to start the Notification of Failure Error (PIP0A1).
	Trading Partner Binding		The trading partner binding.
	Delete		A <b>Delete</b> link that can be used to delete the entry.

### To view binding properties:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the binding table, click the binding name.

The View Binding Details page is displayed.

### To change binding properties:

1. On the View Binding Details page, click the name of the binding.

The Edit Binding page is displayed.
2. Update properties as required. See [“Defining Protocol Bindings” on page 8-31](#).
3. Click **Submit**.
4. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View Binding Details page is displayed with the updated properties.

**Note:** If there is an error, the Edit Binding page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
5. Do one or more of the following as required:
  - To configure signature transforms for an ebXML binding, see [“Configuring Signature Transforms for ebXML Bindings” on page 8-55](#).
  - To Configure PIP failure notification to a RosettaNet binding, see [“Configuring PIP Notification of Failure Roles for RosettaNet Bindings” on page 8-57](#).

## Updating or Deleting Authentication

The authentication required for an exchange is configured as part of the service profile definition, but can only be updated or deleted from the respective binding definitions for the service profile participants. Although you can delete any type of authentication from a binding, the properties that can be edited are limited. The following table summarizes the changes that can be made by authentication type.

**Table 8-1 Changes by Authentication Type**

Authentication Type	If the authentication is configured for the local trading partner in the service profile . . .	If the authentication is configured for remote trading partner in the service profile . . .
Basic	No properties can be edited.	You can enter a new user name in the <b>Username</b> field or select a new alias from the <b>Password Alias</b> drop-down list.
One-Way	No properties can be edited.	You can select a new certificate from the <b>Server Certificate</b> drop-down list.
One-Way with Basic	No properties can be edited.	You can enter a new user name in the <b>Username</b> field or select a new alias from the <b>Password Alias</b> drop-down list. You can select a new certificate from the <b>Server Certificate</b> drop-down list.
Mutual	You can select a new certificate from the <b>Client Certificate</b> drop-down list.	You can select a new certificate from the <b>Client Certificate</b> drop-down list. You can select a new certificate from the <b>Server Certificate</b> drop-down list.

To learn more about adding authentication to a service profile, see [“Adding Authentication to a Service Profile” on page 8-24](#). The following procedures describe how to update or delete an authentication from the View Binding Details page.

### To display the View Binding Details page:

Do one of the following to display the View Binding Details page:

- Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name. On the View and Edit Trading Partner Profile page, click the name of the binding in the **Bindings** table.
- From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**. Click the name of the binding in the **Bindings** table.
- Locate the Service as described in [“Listing and Locating Services” on page 8-42](#), then click the service name to select it. On the View and Edit Service Details page, click the name of the binding in the **Local Binding** or **Remote Binding** column of the **Service Profiles** table.

### To delete authentication from the View Binding Details page:

- In the Authentication section of the View Binding Details page, click the **Delete** link for the entry to be deleted.

The entry is removed from the Authentication table.

**Note:** After you have deleted authentication from the binding of a participant in a service profile, you can reconfigure it as described in [“Adding Authentication to a Service Profile” on page 8-24](#). In this case, options are only offered for configuring authentication for the participant whose authentication was deleted.

### To update authentication from the View Binding Details page:

1. In the Authentication section of the View Binding Details page, select the authentication entry by clicking the type.

The authentication configuration is displayed.

2. Click **Edit Authentication**.
3. Depending on the type of authentication, you can do one or more of the following. See [Table 8-1](#) for summary of the changes that can be made by authentication type:
  - Select a new certificate from the **Server Certificate** drop-down list. If the certificate has not yet been added, click **Add Certificate**. See [“Adding Certificates to a Trading Partner” on page 8-15](#) for instructions. Once the certificate has been added, it is available for selection.

- Select a new certificate from the **Client Certificate** drop-down list. If the certificate has not yet been added, click **Add Certificate**. See [“Adding Certificates to a Trading Partner” on page 8-15](#) for instructions. Once the certificate has been added, it is available for selection.
  - Enter a new user name in the **Username** field and select a new alias from the **Password Alias** drop-down list. If the password alias has not yet been added, click **Add Alias**. See [“Adding Passwords to the Password Store” on page 9-13](#) for instructions. Once the password alias has been added, it is available for selection.
4. Click **Submit**.

The View Binding Details page is displayed.

## Configuring Signature Transforms for ebXML Bindings

The ebXML protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the settings for the **Signature Required** and **Signature Receipt Required** properties of the binding. Optional XPath filtering transforms can be applied to the message for signing purposes as described in the following procedure.

**Note:** A default transform is defined which cannot be deleted. The default XPath expression ensures that, while signing and verifying signed messages, XMLDSig processing engines exclude all elements with `SOAP:actor` attributes targeting the `nextMSH` or next SOAP node. The default transform is required to exclude `SOAP:actor` and other dynamic information used in routing which can invalidate a signature.


To learn more about the digital signature implementation, see “Using WebLogic Integration Security” in [Deploying WebLogic Integration Solutions](#).

### To configure signature transforms for XML digital signatures:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the binding table, click the binding name.

The View Binding Details page is displayed.

3. In the **XML Digital Signature Configuration for Non-Repudiation** section, click **Configure Signature Transforms**.
4. To add new transforms, do the following:
  - a. Click **Add new transform**.
  - b. Enter the XPath expression in the **XPath Transforms** field.
  - c. Click **Add**.

The Configure Signature Transforms for XML DSIG page is displayed with the new transform.
  - d. Repeat steps a to c as required to add additional transforms.
5. To sort the XPath transforms:
  - a. Click **Sort transforms**.
  - b. Move the position of a condition by clicking the up or down arrow  to the right of the condition.
  - c. Click **Submit**.
6. To delete XPath transforms:
  - a. Click the **Delete** link to the right of the transform.

A confirmation message is displayed.
  - b. Click OK to confirm and delete the transform.
7. When all changes are complete, click Cancel to return to the View Binding Details page.

## Configuring PIP Notification of Failure Roles for RosettaNet Bindings

From the View Binding Details page you can add PIP Failure Notifier and PIP Report Administrator roles, edit existing roles, or delete roles.

### To add a notification of failure role:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the binding table, click the binding name.  
The View Binding Details page is displayed.
3. In the **PIP Failure** section, click **Add pip failure**.
4. From the **Failure Type** drop-down list, select **Failure Report Admin** or **Failure Notifier**.
5. From the **Name** drop-down list, select the trading partner name of the PIP Failure Notifier role (if **Failure Notifier** is selected) or PIP Report Administrator role (if **Failure Report Admin** is selected).
6. From the Binding Name drop-down list, select the binding.
7. Click **Add**.

The View Binding Details page is displayed with the addition.

**Note:** If there is an error, the Add PIP Failure page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

**To edit a notification failure role:**

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the binding table, click the binding name.

The View Binding Details page is displayed.
3. In the PIP Failure section, click the Failure Type (**Failure Notifier** or **Failure Report Admin**).

The View or Edit PIP Level Failure page is displayed.
4. Click **Edit pip failure**.

The Edit PIP Failure page is displayed.
5. From the **Name** drop-down list, select a new trading partner name.
6. From the **Binding Name** drop-down list, select a new binding.
7. Click **Submit**.
8. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View Binding Details page is displayed with the update.



## Viewing and Changing a Custom Extension

The View and Edit Custom Extension page allows you to view and update the custom extension for a trading partner.

### To view the custom extension:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Custom Extension** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the custom extension table, click the custom extension name.

The View and Edit Custom Extension page is displayed.

### To change the custom extension:

1. On the View and Edit Custom Extension page, click **Edit Custom Extension**.  
The Edit Custom Extension page is displayed.
2. In the **Description** field, enter or update the optional description.
3. In the **XML** field, update the XML document.

The extension is composed of a user-defined root element that contains well-formed XML elements and attributes that define the required properties. For example, the XML highlighted in bold in the [“Custom Extension Example” on page 8-20](#) constitutes a valid entry.

4. Click **Submit**.

The custom extension is displayed in the Custom Extension summary table.

**Note:** If there is an error, the Edit Custom Extension page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Viewing and Changing Services

The View and Edit Service Details page allows you to view and change service properties. The following table summarizes the information displayed on the View and Edit Service Details page.

Property	Description	Administrator Can Set (Yes/No)
Name	The service URI or control name. The name is a link to the View and Edit Service Details page for the service.	No
Business Service Name	The business service name as defined for the process. For an ebXML process, this is the <b>ebxml-service-name</b> set in the <a href="#">@jpd:ebxml annotation</a> . For a RosettaNet process, this is the <b>pip-name</b> set in the <a href="#">@jpd:rosettanet annotation</a> . The business service name is empty for web services.	No
Description	An optional description. This value is for administrative purposes only. It is not included in messages.	Yes
Business Protocol	Business protocol (ebXML, RosettaNet, or web service).	Yes
Type	The type of service (process, service control, or web service).	Yes

Property	Description	Administrator Can Set (Yes/No)
<b>Service Profiles</b>		
Service profile table	Entry for each service profile:	Yes
	Local Trading Partner	Name of the local trading partner. The name is a link to the View and Edit Trading Partner Profile page for the partner.
	Remote Trading Partner	Name of the remote trading partner. The name is a link to the View and Edit Trading Partner Profile page for the partner.
	Local Binding	Local binding.
	Remote Binding	Remote binding.
	Message Tracking Level	Message tracking level for the service profile (all, default, metadata, or none). For a description of the value, see <a href="#">“Adding Service Profiles to a Service” on page 8-22.</a>
	Status	Status of the service profile (enabled or disabled).
	View	A <b>View</b> link that displays the View Service Profile page. To learn more, see <a href="#">“Viewing and Changing Service Profiles” on page 8-62.</a>
	Statistics	A link to the Trading Partner Management Statistics page for the service profile.

**To view a service:**

1. Locate the service as described in [“Listing and Locating Services” on page 8-42.](#)
2. Click the service name to select it.

The View and Edit Service Details page is displayed.

### To change service properties:

1. On the View and Edit Service Details page, click **Edit Service**.  
The Edit Service Details page is displayed.
2. From the **Type** drop-down list, select **Service Control**, **Process**, or **Web Service** to specify the type of service.
3. From the **Business Protocol** drop-down list, select **EBXML**, **ROSETTANET**, or **WEBSERVICE** to specify the service protocol.
4. In the **Description** field, enter an optional description of the service.
5. Click **Submit**.
6. If any service profiles are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View and Edit Service Details page is displayed with the new definition.

**Note:** If there is an error, the Edit Service Details page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Viewing and Changing Service Profiles

The View and Edit Service Details page allows you to:

- View a list of the service profiles defined for the service.
- View the properties of a selected service profile.
- Edit a selected service profile.

### To view a service profile:

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the service name to select it.

The View and Edit Service Details page is displayed.

3. In the Service Profiles table, click the **View** link for the service profile entry. (The **View** link is in the third column from the right.)

The View Service Profile page is displayed.

**To change a service profile:**

1. On the View Service Profile page, click **Edit Service Profile**.  
The Edit Service Profile page is displayed.
2. To change the status, select **Enabled** or **Disabled** from the **Status** drop-down list,
3. To change the **Message Tracking Level**, select one of the following from the drop-down list.
  - **ALL**  
Message metadata and a reference to message contents in the document store are persisted in message tracking tables. Both message metadata and contents are available for view in the Message Tracking module of the console.
  - **DEFAULT**  
The tracking level for this profile is set to the system default tracking level. See [“Configuring the Mode and Message Tracking” on page 8-9](#).
  - **METADATA**  
Only message metadata is persisted in message tracking tables. Message contents are not tracked and are not available for view in the Message Tracking module of the console.
  - **NONE**  
No message tracking information is sent to the message tracking JMS queue, therefore, no message history is stored in the repository and no information is available for view in the Message Tracking module of the console.
4. To update binding for the **Local** trading partner, select a new binding from the **Binding** drop-down list. Only bindings of the same type as the **Business Protocol** defined for the service are allowed.  
The **Endpoint** field displays the URL for the transport endpoint for the selected binding.
5. To update binding for the **Remote** trading partner, select a new binding from the **Binding** drop-down list. Only bindings of the same type as the **Business Protocol** defined for the service are allowed.  
The **Endpoint** field displays the URL for the transport endpoint for the selected binding.

6. Click **Submit**.
7. If the service profile is enabled, you are prompted to disable it before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View and Edit Service Details page is displayed. The new profile is displayed in the service profile summary table. To enable to service profile, see [“Enabling and Disabling Trading Partner and Service Profiles” on page 8-64](#).

**Note:** If there is an error, the Edit Service Profile page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Enabling and Disabling Trading Partner and Service Profiles

You can enable and disable trading partners and service profiles in the following ways:

- Disable a trading partner, and all the service profiles associated with the trading partner, from the View and Edit Trading Partner Profiles list.
- Enable a trading partner, and all the service profiles associated with the trading partner, from the View and Edit Trading Partner Profiles list.
- Disable an enabled trading partner from the View and Edit Trading Partner Profile page. If there are any enabled service profiles associated with the trading partner, you are prompted to disable them in order to disable the trading partner.
- Enable a disabled trading partner profile from the View and Edit Trading Partner Profile page.

**Note:** Only the trading partner profile is enabled. The associated service profiles are not automatically enabled when you enable a trading partner in this way.

- Enable or disable individual service profiles from the Edit Service Profile page.

In addition to the above:

- When you update a trading partner profile, certificate, or binding, if any of the service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect.
- When you update a service profile, if it is enabled, you are prompted to disable it before the change can take effect.


The following procedures describe the various methods for enabling and disabling trading partner and service profiles.

**To disable trading partners, and the associated service profiles, from the View and Edit Trading Partner Profiles list:**

1. Locate the trading partner(s) to be disabled. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the check box to the left of each trading partner to select.
3. Click **Disable**.

The Disable Trading Partner Service Profile page is displayed, listing the service profiles that must be disabled.

4. Click **Disable** to disable the service profiles.

You are returned to the View and Edit Trading Partner Profiles list. A red light  in the status column indicates that the trading partners cannot send or receive messages.

**To enable trading partners, and the associated service profiles, from the View and Edit Trading Partner Profiles list:**

1. Locate the trading partner(s) to be enabled. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the check box to the left of each trading partner to select.
3. Click **Enable**.

The Enable Trading Partner Service Profiles page lists the service profiles that can be enabled.

**Note:** You can selectively enable profiles by deselecting the profiles that you do not want to enable.

4. Click **Enable** to enable the selected service profiles.

You are returned to the View and Edit Trading Partner Profiles list. A green light  in the status column indicates that the trading partners can now send or receive messages.

**To disable a trading partner, and the associated service profiles, from the View and Edit Trading Partner Profile page:**

1. Locate the trading partner. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the trading partner name.

The View and Edit Trading Partner Profile page is displayed.

3. Click **Edit profile**.
4. From the **Status** drop-down list, select **DISABLED**.
5. Click **Submit**.
6. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The View and Edit Trading Partner Profile page is displayed with the updated status.

**Note:** If there is an error, the edit page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

#### **To enable a trading partner from the View and Edit Trading Partner Profile page:**

**Note:** The associated service profiles are not automatically enabled.

1. Locate the trading partner. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the trading partner name.

The View and Edit Trading Partner Profile page is displayed.

3. Click **Edit profile**.
4. From the **Status** drop-down list, select **ENABLED**.
5. Click **Submit**.

The View and Edit Trading Partner Profile page is displayed with the updated status.

**Note:** If there is an error, the edit page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

#### **To disable or enable a service profile from the Edit Service Profile page:**

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the service name to select it.

The View and Edit Service Details page is displayed.

3. In the Service Profiles table, click the **View** link for the service profile entry. (The **View** link is in the third column from the right.)

The View Service Profile page is displayed.

4. Click **Edit Service Profile**.



The Edit Service Profile page is displayed.

5. From the **Status** drop-down list, select **Disabled** or **Enabled**.
6. Click **Submit**.

The View and Edit Service Details page is displayed. The updated status is displayed in the service profile summary table.

**Note:** If there is an error, the Edit Service Profile page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

## Importing Management Data

You can add or update management data (trading partner profiles, service definitions, and service profiles) by importing an XML representation of the data contained in a trading partner management (TPM) file. Whether you use the console or the Bulk Loader command line utility to import, the TPM file must either:

- Conform to the `tpm.xsd` schema.

Or

- Contain a single trading partner profile exported from WebLogic Integration - Business Connect or from WebLogic Integration using the business connect format.

When you export TPM data using the console or the Bulk Loader utility, a file suitable for import is created. To learn more about the required structure, and how the file is used in import, export, and bulk delete operations, see [Appendix B, “Using the Bulk Loader.”](#)

In the following procedure, it is assumed that the required TPM file has been created. If the file contains entities (trading partners or services) that already exist, the entities are updated as described in [Appendix B, “Using the Bulk Loader.”](#) Otherwise the entities are added. If the entity being updated is in active use, then the operation will fail with an error message.

### To add or update management data by importing XML:

1. From the Trading Partner Management home page, select the **Partner Profile Import/Export** module.
2. Do one of the following:
  - Click the **Browse** button to the right of the **File Name** field, then locate the TPM file. Select the file and click **Open**.
  - Enter the path to the TPM file in the **File Name** field.

3. Specify the **Transaction Level** by selecting one of the following option buttons:
  - **All**  
Imports the data in a single transaction. If invalid data is detected the entire transaction is rolled back.
  - **Default**  
Imports data using multiple transactions. The import initiates a transaction for each trading partner or service. If invalid data is detected during a transaction for any entity, the import is rolled back for the current transaction only; importing stops with the rolled back transaction.
4. Specify the **Import Format** by selecting one of the following option buttons:
  - **WLI Standard**  
Imports the data that conforms to the TPM.xsd schema.
  - **Business Connect**  
Imports data that has been exported from WebLogic Integration - Business Connect or from WebLogic Integration using business connect format.
5. Click **Import**.

## Exporting Management Data

Before trading partners can participate in transactions hosted by WebLogic Integration, they must set up their environments to meet the requirements of the application. To facilitate trading partner setup, one partner can define the required components (trading partner profiles, service definitions, and service profiles), and then export them so they become available for import by other trading partners.

### To export trading partner management data:

1. From the Trading Partner Management home page, select the **Partner Profile Import/Export** module.
2. From the left panel, select **Export**.
3. Do one the following:
  - To export all trading partner management entities, check the **All** check box.
  - To export selected trading partner profiles, check the **Trading Partner** check box, then click the **Browse** button to display the Choose Trading Partner Profiles page. On the

Choose Trading Partner Profiles page, check or uncheck trading partners as required. When the trading partners to be exported are checked, click **Done**.

- To export selected services, check the **Services** check box, then click the **Browse** button to display the Choose Services page. On the Choose Services page, check or uncheck services as required. When the services to be exported are checked, click **Done**.

**Note:** The above options are mutually exclusive.

4. Specify the **Export Format** by selecting one of the following option buttons:

- **WLI Standard**  
Export data that conforms to the TPM.xsd schema.
- **Business Connect**  
Export for import by WebLogic Integration - Business Connect.

**Note:** If you are exporting for import to WebLogic Integration - Business Connect, you can only export one trading partner profile at a time. Before continuing, verify that a single trading partner is selected.

5. In the **Encoding** field, specify the encoding, if other than the default. See <http://www.iana.org/assignments/character-sets> for valid values.

6. If you checked the **Trading Partners** or **Services** check box, do one of the following:

- Check the **Export All Referenced Entities** check box to export all entities referenced by the selected trading partners or services. For trading partners, referenced entities include the entities referenced by any service profile the trading partner is referenced in. For services, referenced entities include the trading partner profiles referenced in the service profiles. (A trading partner profile always includes its bindings, certificates, and custom extension.)

**Note:** Although it is not required, if you are exporting selected services, it is standard practice to check the **Export All Referenced Entities** option. If you selected the **Business Connect** format, *do not* check **Export All Referenced Entities**.

- Uncheck the **Export All Referenced Entities** check box to export only the selected trading partners or services.

7. Click **Export**.

A download of the file is initiated. The dialog box that is displayed is browser-dependent, but typically, you are prompted to open or save the file.

8. Select **Save File to Disk** if prompted.
9. Specify the location and name of the file, then click **Save**.

The file is saved to the specified location.

## Deleting Trading Partner Profiles and Services Using Bulk Delete

You can delete trading partner management data in bulk from the Delete Trading Partner Management Data page.

### To delete trading partner management data:

1. From the Trading Partner Management home page, select the **Partner Profile Import/Export** module.
2. From the left panel, select **Bulk Delete**.
3. Specify the **Transaction Level** by selecting one of the following option buttons:
  - **All**  
Deletes the data in a single transaction. If an error is encountered, the entire transaction is rolled back.
  - **Default**  
Deletes the data using multiple transactions. A delete transaction is initiated for each trading partner or service. If an error is encountered during the transaction for any entity, the transaction is rolled back; deleting stops with the rolled back transaction.
4. Do one the following:
  - To delete all trading partner management entities, check the **All** check box.
  - To delete selected trading partner profiles, check the **Trading Partner** check box, then click the **Browse** button to display the Choose Trading Partner Profiles page. On the Choose Trading Partner Profiles page, check or uncheck trading partners as required. When the trading partners to be deleted are checked, click **Done**.
  - To delete selected services, check the **Services** check box, then click the **Browse** button to display the Choose Services page. On the Choose Services page, check or uncheck services as required. When the services to be deleted are checked, click **Done**.

**Note:** The above options are mutually exclusive.

5. If you checked the **Trading Partners** or **Services** check box, do one of the following:
  - Check the **Delete All Referenced Entities** check box to delete all entities referenced by the selected trading partners or services. For trading partners, referenced entities include the entities referenced by any service profile the trading partner is referenced in. For services, referenced entities include the trading partner profiles referenced in the service profiles. (A trading partner profile always includes its bindings, certificates, and custom extension.)
  - Note:** Although it is not required, if you are exporting selected services, it is standard practice to check the **Export All Referenced Entities** option.
  - Uncheck the **Export All Referenced Entities** check box to export only the selected trading partners or services.
6. Click **Delete**.

The Trading Partner Management home page is displayed.

## Deleting Trading Partner Profiles

You can delete trading partner profiles from the View and Edit Trading Partner Profiles list or from the View and Edit Trading Partner Profiles page. When you delete a trading partner, you must also delete all associated service profiles.

### To delete one or more trading partners from the View and Edit Trading Partner Profiles list:

1. Locate the trading partners to be deleted. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the check box to the left of each trading partner to select.
3. Click **Delete**.
4. If the selected trading partners are referenced in any service profiles, you are prompted to delete the them. Click **Delete All** to delete the service profiles and continue.

The View and Edit Trading Partner Profiles list is displayed. The deleted trading partners are no longer listed.

### To delete a trading partner from the View and Edit Trading Partner Profile page:

1. Locate the trading partner to be deleted. See [“Listing and Locating Trading Partners” on page 8-41](#).
2. Click the trading partner name to select it.

3. On the View and Edit Trading Partner Profile page, click **Delete**.

A confirmation message is displayed.

4. Click **OK** to confirm.
5. If the trading partner is referenced in any service profiles, you are prompted to delete the them. Click **Delete All** to delete the service profiles and continue.

The View and Edit Trading Partner Profiles list is displayed. The deleted trading partner is no longer listed.

## Deleting Certificates, Bindings, or Custom Extensions

You can delete certificates, bindings, or custom extension from the Trading Partner Management Profile page.

### To delete a certificate:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Certificates** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the certificate table, click the **Delete** link for the entry to be deleted.

A confirmation dialog box is displayed.
3. Click **OK** to confirm.

A dialog box is displayed with the following question: “Do you want to remove the certificate from the keystore also?”
4. Click **OK** to remove the certificate from the keystore, or **Cancel** to leave the certificate in the keystore.

5. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The certificate summary table is displayed. The deleted certificate has been removed.

#### To delete a binding:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Bindings** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the binding table, click the **Delete** link for the entry to be deleted.

A confirmation dialog box is displayed.
3. Click **OK** to confirm.
4. If any service profiles for the trading partner are enabled, you are prompted to disable them before the change can take effect. Click **Disable** to disable the service profiles and continue.

The binding summary table is displayed. The deleted binding has been removed.

#### To delete a custom extension:

1. Do one of the following:
  - Locate the trading partner as described in [“Listing and Locating Trading Partners” on page 8-41](#), then click the trading partner name.
  - From the Trading Partner Management home page, select the **Profile Management** module, then select **Custom Extension** from the left panel. On the Choose Trading Partner page, select the trading partner name from the **Name** drop-down list, then click **Go**.
2. In the custom extension table, click the **Delete** link for the entry to be deleted.

A confirmation dialog box is displayed.

3. Click **OK** to confirm.

The custom extension summary table is displayed. The table is now empty.

## Deleting Services

You can delete a service from the View and Edit Services list.

### To delete a service:

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the **Delete** link for the service to be deleted. (The **Delete** link is in the right-most column.)

A confirmation dialog box is displayed.

3. Click **OK** to confirm.
4. If the service includes any service profiles, you are prompted to delete the them. Click **Delete All** to delete the service profiles and continue.

The View and Edit Services list is displayed. The deleted service has been removed.

## Deleting Service Profiles from a Service

You can delete service profiles from the View And Edit Service Details page.

### To delete service profiles:

1. Locate the service as described in [“Listing and Locating Services” on page 8-42](#).
2. Click the service name to select it.

The View and Edit Service Details page is displayed.

3. In the service profile table, click the **Delete** link for the entry to be deleted. (The **Delete** link is in the second column from the right.)

A confirmation dialog box is displayed.

4. Click **OK** to confirm.

The View and Edit Service Details page is displayed. The deleted service profile has been removed from the service profile table.



## Viewing Statistics

You can view summary statistics from the Trading Partner Management Statistics page. You can view statistics for the entire system or for a specific service profile.

### To view statistics for the system:

- From the Trading Partner Management home page, select the **Statistics** module.

The Trading Partner Management Statistics page displays the following statistics:

Current Statistics	
Trading Partner Count	8
Service Count	16
Process	8
Service Control	8
Web Service	0
Service Profile Count	8
Active Service Profile Count	3
Current throughput	
Total Conversation Count	0
Sent Message Count	0
Received Message Count	0

### To view statistics for a service profile:

- Locate the service as described in [“Listing and Locating Services”](#) on page 8-42.
- Click the service name to select it.

The View and Edit Service Details page is displayed.

3. In the service profile table, click the **Statistics** link for the profile. (The **Statistics** link is in the right-most column.)

The Trading Partner Management Statistics page displays the following statistics:

Current Statistics	
Total Conversation Count	0
Sent Message Count	0
Received Message Count	0

# Monitoring Messages

You can monitor the exchange of business messages from the Message Tracking module. The message data available is dependent on:

- The message tracking level set for each service profile in the system. To learn more about the message tracking levels, see [“Adding Service Profiles to a Service” on page 8-22](#).
- The archive and purge schedule for the system. To learn more, see [“Archiving and Purging Tracking Data” on page 9-4](#).

From the message tracking module, you can:

- View a list of the business messages exchanged.
- Filter the list.
- View message detail, including header or part content, for selected messages.

In the following procedures, it is assumed that the desired message data is available.

## Listing and Locating Messages

You can view a summary listing of the business messages exchanged on View Messages page.

### To view a list of the messages:

1. From the Trading Partner Management home page, select the Message Tracking Module.  
The View Messages page is displayed.
2. Do one or more of the following:
  - Filter the messages on the list as described in [“Filtering the Messages Displayed” on page 8-77](#).
  - Sort the list by time of the event. Click the ascending ▲ and descending ▼ arrow button to change the sort. order.
  - View the details of a selected message as described in [“Viewing Message Detail” on page 8-78](#).

## Filtering the Messages Displayed

The messages displayed on the View Messages page can be filtered as described in the following procedure. The filter you set remains in effect until you update it, or until the server is restarted.

### To filter the messages displayed on the View Messages page:

1. From the Trading Partner Management home page, select the Message Tracking Module.  
The View Messages page is displayed.
2. Select Configure View from the **Go** drop-down list in the upper right corner.
3. Click **Go** to display the Filter the Displayed Messages page.
4. Do one of the following:
  - To specify an explicit start and end time, click the **Start Time** option button, then select the start and end times from the drop-down lists.
  - To specify an interval relative to the current time, click the **For Last** option button, then enter the interval.

5. Do one or more of the following:
  - To filter by recipient, select the trading partner from the **For Trading Partner** drop-down list.
  - To filter by sender, select the trading partner from the **To Trading Partner** drop-down list.
  - To filter by status, select **ALL**, **SUCCEEDED**, or **FAILED** from the Status drop-down list.

## Viewing Message Detail

You can view message detail from the Message Details page.

### To view message detail:

1. From the Trading Partner Management home page, select the Message Tracking Module.  
The View Messages page is displayed.
2. Select the Event ID to display detail for the selected message.

The message detail is displayed as shown in the following figure. You can view the message header, status description, message part headers, message part data, or details for the process instance or type.

**Note:** The information available is dependent on the message tracking level for the service profile. To learn more about the message tracking levels, see [“Adding Service Profiles to a Service” on page 8-22](#).

The screenshot displays the 'Integration Administration Console' with two main sections. The top section, titled 'Message Part Header', shows the 'Content-Type' as 'text/xml x-ebxmlattachment: true content-id: &lt;QuoteService- ACME -id-1056903979060-6- ACME -id-1056903982455-9-header&gt;' and includes navigation links for 'Partner Management' and 'Message Tracking'. The bottom section, titled 'Message Part Data', displays the XML content of the message part, which is a SOAP-ENV:Envelope containing a SOAP-ENV:Header with an eb:MessageHeader. The header includes fields for From (PartyId: urn:duns.com:ACME-id/), To (PartyId: urn:duns.com:BEA-id/), CP:Id (http://www.openuri.org/opac/eb:CP:Id), ConversationId (QuoteService-ACME-id-1056903979060-6), and Service (text:QuoteService).



# System Configuration

This section provides the information you need to use the *System Configuration* module of the WebLogic Integration Administration Console to:

- View or set the archive and purge (or purge only) schedule.
- Request immediate archive and purge (or purge only).
- View or set the JNDI name for the datastore used to archive tracking data.
- View or set the default tracking level and archiving policy for processes.
- View or set the default tracking level for worklist tasks.
- Create, view, or change password aliases.
- Configure the JMS connection factory, repository root, and debug level for application integration.
- Configure the role authorized to create worklist tasks.

**Note:** You must be logged in as a member of the Administrators or IntegrationAdministrators group to make any changes to the system configuration. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About System Administration](#)
- [Overview of the System Configuration Module](#)

- [Viewing the Archive and Purge Configuration](#)
- [Configuring the Archive and Purge Process](#)
- [Configuring the Archive Datastore](#)
- [Configuring the Tracking and Archive Defaults](#)
- [Manually Starting the Archive and Purge Process](#)
- [Adding Passwords to the Password Store](#)
- [Listing and Locating Password Aliases](#)
- [Changing the Password for a Password Alias](#)
- [Deleting Passwords from the Password Store](#)
- [Configuring the Server for Application Integration](#)

## About System Administration

The following sections provide background information related to system administration:

- [Process Tracking Data](#)
- [Archiving and Purging Tracking Data](#)
- [Password Aliases and the Password Store](#)

## Process Tracking Data

Each process instance generates events that contain information about process execution such as information about the node that is executing, timings, and associated data.

The following types of events can be tracked:

- *Global events*  
Events such as start process, end process, suspend, and resume.
- *Node transitions*  
Events generated by each node (a start node event and an end or abort node event).
- *Data*  
Data logged as a result of invoking `JpdContext.trackData()`.



Administrators can set the tracking level for processes to optimally tune their system to meet their reporting needs and performances requirements. The tracking levels are:

- *Full*  
Global events, node transitions, and data are tracked.
- *Node*  
Global and node transitions are tracked.
- *Minimum*  
Global events are tracked.
- *None*  
No events or data are tracked.

The system default tracking level is set from the System Configuration module. The tracking level for each process type is set from the Process Configuration module. The administrator has the option of either:

- Setting the tracking level for a process to the system default.
- Overriding the system default by setting the tracking level for a process to full, node, minimum, or none.

To learn more about:

- Setting the system default tracking level, see [“Configuring the Tracking and Archive Defaults” on page 9-11](#).
- Setting tracking level for a process type, see [“Viewing and Changing Process Details” on page 2-11](#).

## Worklist Tracking Data

Each worklist task instance generates events that can be logged in worklist history tables in the runtime repository. The following types of events can be tracked:

- *Changes in task state and associated values*  
The type of transition and associated values. For example, a task is reassigned or claimed. In this case, the change in state and identity of the new assignee or claimant can be tracked.
- *Expiration of task claim or complete due date*  
The task is unclaimed or incomplete on the due date for claiming or completing.

- *Changes in task owner or assignees*  
The type of change and new values can be tracked.
- *Task requests and task responses*  
The request and response XML.

The tracking levels are:

- *Full*  
All transitions and changes, including task requests and responses, are logged.
- *Basic*  
Transitions and changes are logged. Task requests and responses are not logged.
- *None*  
No task history is tracked.

The tracking level applicable to all worklist tasks is set from the System Configuration module.  
To learn more about:

- Setting the default tracking level for worklist tasks, see [“Configuring the Tracking and Archive Defaults” on page 9-11.](#)
- Contents of the worklist history tables, see [Advanced Worklist Topics](#) in *Building Integration Applications* in the WebLogic Workshop help.

## Archiving and Purging Tracking Data

Tracking data includes:

- Process instance history (see [“Process Tracking Data”](#) above for tracking levels).
- Task instance history (see [“Worklist Tracking Data”](#) above for tracking levels).
- Trading partner message history (see [“Configuring the Mode and Message Tracking” on page 8-9](#) for tracking levels).

In order to optimize performance, the amount of tracking data stored in the runtime database should be kept to a minimum. To help ensure this, the archive and purge process is configured to run at regular intervals set by the administrator. In addition to configuring the schedule, the administrator can enable or disable the archiver:

- When the archiver is enabled, the process copies the data to an offline database, then purges it from the runtime database.
- When the archiver is disabled, the process purges the data from the runtime database without copying it.

**Note:** You cannot disable the purge process.

To provide a greater level of control, the administrator also configures the following:

- *Archive policy for each process type*  
If the archive policy for a process is **On**, instance data is archived if the archiver is enabled. If it is **Off**, instance data for the process is not archived; it is only purged. If it is set to **Default**, the system default archive policy (described below) is used.
- *System default archive policy for processes*  
The system default archive policy can be set to **On** or **Off**. If the archive policy for a process is set to **Default**, the process inherits the system default setting. Instance data for the process is, or is not, archived prior to purge.
- *Purge Delay*  
The amount of time after the following events that must pass before the data is subject to purge by the archive and purge process:
  - Completion or termination of a process instance.
  - Completion or cancellation of a worklist tasks.
  - Receipt or delivery of message.

For example, suppose the archive policy for a process is **On**, the purge delay is set to 5 days, and the archive and purge process is configured to archive and purge data every hour. In that case, the data for an instance completing on day 1 would be archived according to the regular schedule, but the data would not be purged until day 5.

The administrator can reset the archive and purge schedule at any time, enable or disable the archiver (thus configuring the process to purge only), or can request the process to run on demand.

Only data for completed or terminated process instances, or completed or cancelled worklist tasks is subject to the archive and purge process. The data associated with frozen, suspended, or aborted process instances remains in the runtime database. Before this data can be purged:

- An aborted instance must be terminated.
- A suspended instance must be resumed and completed, or terminated.
- A frozen instance must be unfrozen and completed, or terminated.

To learn more about:

- Managing process tracking data, see [“Managing Process Tracking Data” on page 2-2](#).
- Configuring the archiver, see [“Configuring the Archive and Purge Process” on page 9-10](#).
- Setting the system default archive policy level, see [“Configuring the Tracking and Archive Defaults” on page 9-11](#).
- Setting the archive policy for a process, see [“Viewing and Changing Process Details” on page 2-11](#).

## Password Aliases and the Password Store

The password store provides for the secure storage of the passwords used by controls, event generators, and other WebLogic Integration components. Each required password is defined in the password store and associated with a password alias. This alias can then be referenced in the annotations of process definitions (\*.jpd), control extensions (\*.jcx), and event generator configuration files (wliconfig/\*EventGen.xml).

For example, when configuring an email event generator, rather than specifying the password required to access a user’s email account in plain text, the password would be defined and associated with a password alias in the password store. The password alias, rather than the password, can then be referenced in the event generator configuration file.

To learn how to add passwords and aliases, see [“Adding Passwords to the Password Store” on page 9-13](#).

## Overview of the System Configuration Module

The following table lists the pages you can access from the System Configuration module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
<b>Archive and Tracking Policy</b>		
Current Archive Process Policy Settings	View the system-level settings for archiving and purging. The current status of the archiver (enabled or disabled), archive and purge schedule, purge delay, archive datastore (if the archiver is enabled), default archiving policy, and default tracking level are displayed.	<a href="#">“Viewing the Archive and Purge Configuration” on page 9-9</a>
WebLogic Integration Archive Policy Settings	Enable or disable the archiver.	<a href="#">“Configuring the Archive and Purge Process” on page 9-10</a>
	Edit the archiving and purging start time and repeat interval.	
	Edit the purge delay.	
Edit Data Store Configuration Settings	Change the JNDI name of the database used for archiving data (when the archiver is enabled).	<a href="#">“Configuring the Archive and Purge Process” on page 9-10</a>
Default Tracking Level and Archiving Policy	Change the default tracking level or default archiving policy for processes.	<a href="#">“Configuring the Tracking and Archive Defaults” on page 9-11</a>
Edit Worklist Task Tracking Parameter	Change the default tracking level for worklist tasks.	<a href="#">“Configuring the Tracking and Archive Defaults” on page 9-11</a>
<b>Archive</b>		
Archive and Purge Process Data	Request an immediate archive and purge cycle.	<a href="#">“Manually Starting the Archive and Purge Process” on page 9-12</a>
	View the number of records in the runtime database for completed or terminated process instances.	
	View the time the last archive and purge cycle completed.	

Page	Associated Tasks	Topics
<b>Password Store</b>		
View and Edit Password Aliases	View a list of password aliases.	<a href="#">“Listing and Locating Password Aliases” on page 9-14</a>
	Filter the list by alias name. Use ? to match any single character or * to match zero or more characters.	
	Delete one or more password aliases.	<a href="#">“Deleting Passwords from the Password Store” on page 9-15</a>
Add New Password Alias	Add a password by assigning a unique alias and defining the password.	<a href="#">“Adding Passwords to the Password Store” on page 9-13</a>
Edit Password Alias	Change the password associated with a password alias.	<a href="#">“Changing the Password for a Password Alias” on page 9-14</a>
<b>Application Integration</b>		
View Application Integration Configuration	View the application integration configuration. Debug status (enabled or disabled), JMS connection factory, and repository root directory are displayed.	<a href="#">“Configuring the Server for Application Integration” on page 9-15</a>
Edit Application Integration Configuration	Edit the application integration debug status, JMS connection factory, or repository root directory.	<a href="#">“Configuring the Server for Application Integration” on page 9-15</a>
<b>Worklist</b>		
View Worklist Configuration	View current setting for the worklist task creation role.	<a href="#">“Configuring the Worklist Task Creation Role” on page 9-16</a>
Edit Worklist Configuration	Edit the worklist task creation role.	<a href="#">“Configuring the Worklist Task Creation Role” on page 9-16</a>

## Viewing the Archive and Purge Configuration

The Current Archive Process Policy Settings Page allows you to view the archive and purge configuration.

### To view the archive and purge configuration:

- From the home page, select the **System Configuration** module.

The following table describes the properties displayed on the page.

Property	Description
<b>Schedule</b>	
The Archiver Process Is	Status of the archiver process (enabled or disabled): <ul style="list-style-type: none"> <li>• When the archiver is enabled, the tracking data is copied to an offline database, then purged from the runtime database according to the configured schedule.</li> <li>• When the archiver is disabled, the tracking data is purged from the runtime database according to the configured schedule.</li> </ul>
Archiving and Purging Start Time	The start date and time for the archive and purge (or purge only) process.
Repeat Every	Intervals from the start time that the archive and purge (or purge only) process runs.
Purge Delay	The amount of time after completion or termination before process and task instance data is subject to purge.
<b>Archive Datastore</b>	
Archive Datastore JNDI Name	JNDI name of the database used to archive data when the archiver process is enabled.
<b>Default Archiving Policy and Tracking Level</b>	
Default Tracking Level	The system default tracking level (full, node, minimum, or none). If the <b>Tracking Level</b> for a process is set to <b>Default</b> , the process inherits this setting. To learn how to set the archive policy for a process see <a href="#">“Viewing and Changing Process Details” on page 2-11</a> .

Property	Description
Default Archiving Policy	The system default archive policy (on or off). If the <b>Archive Policy</b> for a process is set to <b>Default</b> , the process inherits this setting. Instance data for the process is, or is not, archived accordingly. To learn how to set the archive policy for a process see <a href="#">“Viewing and Changing Process Details” on page 2-11</a> .
<b>Worklist Task Tracking Level</b>	
Task Tracking Level	Tracking level for worklist tasks.
	<b>Full</b> All transitions and changes, including task requests and responses, are logged.
	<b>Basic</b> Transitions and changes are logged. Task requests and responses are not logged.
	<b>None</b> No task history is tracked.

# Configuring the Archive and Purge Process

The WebLogic Integration Archive Policy Settings page allows you to enable or disable the archiver process, update the schedule for archive and purge (or purge only), and set the purge delay.

**To configure the archive and purge process:**

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Archiving and Tracking Policy**.
3. In the Archive Schedule section, click the **Configure** link.
4. Do one or more of the following:
  - To enable or disable the archiver, check or uncheck the **Enable the Archiver Process** check box.
  - To update the **Archiving and Purging Start Time**, select the hour, minute, month, day, and year from the drop-down lists.
  - To update the repeat interval, enter a new value in the **Repeat Every** field, then select **mins**, **hours**, or **days** from the drop-down list.



- To update the purge delay, enter a new value in the **Purge Delay** field, then select **mins**, **hours**, or **days** from the drop-down list.
5. Click **Submit** to save your changes and return to the Current Archive Process Policy Settings page.

## Configuring the Archive Datastore

The Edit Datastore Configuration Settings page allows you to specify the database used to archive data.

### To configure the archive datastore:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Archiving and Tracking Policy**.
3. In the Archive Datastore section, click the **Configure** link.
4. In the **Archive Datastore JNDI Name** field, enter the JNDI name for the datastore.
5. Click **Submit** to save your changes and return to the Current Archive Process Policy Settings page.

## Configuring the Tracking and Archive Defaults

In addition to allowing you to configure the archive and purge process, the Current Archive Process Policy Settings page allows you to configure:

- The default tracking level and archive policies for processes.
- The tracking level for worklist tasks.

See [“Viewing the Archive and Purge Configuration” on page 9-9](#) for a description of all the properties displayed on the Current Archive Process Policy Settings page.

### To configure the default archiving and tracking policies for processes:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Archiving and Tracking Policy**.
3. In the Default Archiving Policy and Tracking Level section, click the **Configure** link.

4. Do one or both of the following:
  - From the **Default Tracking Level** drop-down list, select **Full**, **Node**, **Minimum**, or **None**.
  - From the **Default Archiving Policy** drop-down list, select **On** or **Off**.
5. Click **Submit** to save your changes and return to the Current Archive Process Policy Settings page.

**To configure the tracking level for worklist tasks:**

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Archiving and Tracking Policy**.
3. In the Worklist Task Tracking Level section, click the **Configure** link.
4. From the **Task Tracking Level** drop-down list, select **Full**, **Basic**, or **None**.
5. Click **Submit** to save your changes and return to the Current Archive Process Policy Settings page.

## Manually Starting the Archive and Purge Process

The Archive and Purge Tracking Data page displays:

- The number of records stored in the runtime database for completed or terminated process instances.
- The time the archiver process last completed.

If the archive and purge process is scheduled to run regularly, tracking data, which includes process history, task history, and trading partner integration message history, is purged from the runtime datastore according to the schedule currently set. If required, you can request that the archive and purge process run immediately, as described in the following procedure.

**Note:** Only the data normally subject to the archive and purge process is archived and purged. (That is, the purge delay, and archive policies currently set are not overridden.) If the archiver is disabled, data is not archived.

**To archive and purge the tracking data:**

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Archive** to display the Archive and Purge Tracking Data page.

3. Click the **Archive and Purge Tracking Data** button.

A confirmation dialog box is displayed.

4. Click **OK** to confirm, or **Cancel** to dismiss the dialog and cancel the action.

## Adding Passwords to the Password Store

The Add a New Password Alias page allows you to create a password and associate it with a password alias.

### To add a password and alias:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Password Store**.
3. From the left panel, select **Create New** to display the Add a New Password Alias page.
4. In the **Password Alias Name** field, enter a unique name.
5. In the **Password** field, enter the password.
6. In the **Confirm Password** field, enter the password again.
7. Do one of the following:
  - To create the password alias, click **Submit**.

The View and Edit Password Aliases page is displayed. The new alias is included in the list. (You may need to page forward to see the new alias.)







**Note:** If there is an error, the Add a New Password Alias page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

- To disregard changes and return to the View and Edit Password Aliases page, click **Cancel**.

## Listing and Locating Password Aliases

The View and Edit Password Aliases page lists the password aliases defined in the password store.

### To list and locate password aliases:

1. From the home page, select the **System Configuration** module.
2. In the left panel, click **Password Store** to display the View and Edit Password Aliases page.
3. To locate a specific password alias, do one of the following:
  - Filter by alias name. Enter the search target, then click **Search**. The password aliases matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Changing the Password for a Password Alias

The Edit Password Alias page allows you to change the password associated with the password alias.

### To view and change the password:

1. Locate the password alias. See [“Listing and Locating Password Aliases” on page 9-14](#).
2. Click the alias name to display the Edit Password Alias page.
3. In the **Current Password** field, enter the current password.
4. In the **New Password** field, enter the new password.
5. In the **Confirm Password** field, enter the new password again.
6. Do one of the following:
  - To update the password, click **Submit**.

The View and Edit Password Aliases page is displayed.

**Note:** If there is an error, the Edit Password Alias page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

- To reset to the last saved values, click **Reset**.
- To disregard changes and return to the View and Edit Password Aliases page, click **Cancel**.

## Deleting Passwords from the Password Store

The View and Edit Password Aliases page allows you to locate and delete selected password aliases.

### To delete password aliases:

1. Locate the password alias or aliases to be deleted. See [“Listing and Locating Password Aliases” on page 9-14](#).
2. Click the check box to the left of the password aliases to be deleted to select them.
3. Click **Delete Selected Aliases**.

## Configuring the Server for Application Integration

The Edit Application Integration page allows you to define the server configuration for application integration.

### To configure the server for application integration:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Application Integration**.
3. On the View Application Integration Configuration page, click **Configure**.
4. Update the configuration as required. The following table summarizes the available settings.

Setting	Description
Check or uncheck the <b>Debug Enabled</b> check box.	When <b>Debug</b> is enabled, additional application integration debug messages are generated. Because these messages are logged using the standard WebLogic Server logging facility, they are only logged if debug messages are also enabled in the WebLogic Server Administration Console.
In the <b>JMS Connection Factory JNDI Name</b> field, enter the name of the required JMS connection factory.	Application views use JMS resources to handle events and asynchronous service invocations, and therefore require access to a JMS Connection Factory. This field specifies the JMS Connection Factory JNDI context.
In the <b>Repository Root Directory</b> field, enter repository root.	Files related to application views are stored in a file repository ( <code>wlai-repository</code> ). This field specifies the root directory for that repository.

## Configuring the Worklist Task Creation Role

The Edit Worklist Task Tracking Parameter page allows you to set the worklist task creation role. This is the role that is authorized to create worklist tasks.

### To set the worklist task creation role:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Worklist**.
3. On the View Worklist Configuration page, click **Configure**.
4. From the **Task Creation Role** drop-down list, select the role.
5. Click **Submit** to update the setting and return to the View Worklist Configuration page.

# User Management

This section provides the information you need to use the *User Management* module of the WebLogic Integration Administration Console. This module allows you to manage the users, groups, and roles defined in the default security realm.

**Note:** You must be logged in as a member of the Administrators or IntegrationAdministrators group to add, delete, or modify a user, group, or role. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About WebLogic Integration Users, Groups, and Roles](#)
- [Overview of the User Management Module](#)
- [Adding a User](#)
- [Adding a Group](#)
- [Adding a Role](#)
- [Constructing a Role Statement](#)
- [Listing and Locating Users](#)
- [Listing and Locating Groups](#)
- [Listing and Locating Roles](#)
- [Viewing and Changing User Properties](#)

- [Viewing and Changing Group Properties](#)
- [Viewing and Setting Role Conditions](#)
- [Deleting Users, Groups, or Roles](#)

## About WebLogic Integration Users, Groups, and Roles

Users are entities that can be authenticated. Each user is assigned a unique identity within the realm. To make it easier to administer a large number of users, users can be organized into named groups. Groups can in turn be assigned membership in other groups.

Like other components of the platform, WebLogic Integration supports role-based authorization. Although the specific users that require access to the components that make up your WebLogic Integration application may change depending upon the deployment environment, the roles that require access are typically more stable. Authorization involves granting an entity permissions and rights to perform certain actions on a resource.

In role-based authorization, security policies define the roles that are authorized to access the resource. In addition to the built-in roles that are associated with certain administrative and monitoring privileges, security policies that control access to the following resources can be configured from the WebLogic Integration Administration Console:

- *Process operations*  
Policies define the role required to invoke the process operations. See [“Process Security Policies” on page 2-4](#).
- *Message Broker channels*  
Policies define the roles required to subscribe and publish to a given channel. See [“Setting Channel Security Policies” on page 4-6](#).
- *Application Views*  
Policies define the roles required to execute services and subscribe for events on an application view. See [“Managing Security” on page 7-5](#).

Once the roles required for access are set, the administrator can map users or groups to the roles as required.



Unlike membership in a group, which is directly assigned, membership in a security role is dynamically calculated based on the set of conditions that define the role statement. Each condition specifies user names, group names, or time of day. Conditions are joined by conjunction (and) or disjunction (or) commands. When a principal (user) is “in” a role based on the evaluation of the role statement, the access permissions of the role are conferred on the principal.

A set of default roles are defined for WebLogic Integration system management. Additional roles can be created to control access to implementation-specific resources. The roles created using the WebLogic Integration Administration Console are created as WebLogic Server global roles.

## Default Groups, Roles, and Security Policies

Any domain that supports WebLogic Integration includes a set of default WebLogic Integration roles and groups. Default security policies define the roles authorized to access specific WebLogic Integration resources.

### Default Roles

The following table lists the default WebLogic Integration roles. A brief description and initial condition statement associated with each is provided. To learn more, see “[Default Security Policies](#)” on page 10-5.

Although you can update the role statement associated with a default role, you cannot delete these roles.

**Note:** In addition to the default WebLogic Integration roles, there are also a number of default WebLogic Server roles. See “Default Global Roles” in “Security Roles” at the following URL:

<http://edocs.bea.com/wls/docs81/secwlrsecroles.html>

Default Role	Description	Initial Role Statement
IntegrationAdmin	The WebLogic Integration administrator role. This role has full privileges to all servers in the cluster. This role can create additional roles using the WebLogic Integration Administration Console.	Groups:(IntegrationAdministrators, Administrators)
IntegrationOperator	The WebLogic Integration operator role. This role has nearly all the privileges of the IntegrationAdministrator role. For example, a user in the IntegrationOperator role cannot configure certain security properties, but can otherwise modify resources. See <a href="#">“Default Security Policies” on page 10-5</a> for details.	Groups:(IntegrationOperators, Operators)
IntegrationMonitor	The WebLogic Integration monitor role. This role has read-only access to the WebLogic Integration Administration Console.	Groups:(IntegrationMonitors, Monitors)
IntegrationUser	The default WebLogic Integration user role. When first created, all users are assigned to the IntegrationUser role.	Groups:(IntegrationUsers)

## Default Groups

The following table lists the default groups.

Default Role	Description
IntegrationAdministrators	The WebLogic Integration administrator group. This group is assigned to the role IntegrationAdmin and all members inherit the that role.
IntegrationUsers	The WebLogic Integration user group. This group is assigned to the role IntegrationUser and all members inherit the that role.

Default Role	Description
IntegrationMonitors	The WebLogic Integration monitor group. This group is assigned to the role IntegrationMonitor and all members inherit the that role.
IntegrationOperators	The WebLogic Integration operator group. This group is assigned to the role IntegrationOperator and all members inherit the that role.

## Default Security Policies

The following table summarizes the actions the IntegrationMonitor, IntegrationOperator, and IntegrationAdmin, and IntegrationUser roles can execute.

Resource	Action	IntegrationMonitor	IntegrationOperator	IntegrationAdmin	IntegrationUser
Servers in a Cluster	Start Stop		✓	✓	
Processes	Configure versions, tracking, and archiving policies		✓	✓	
	Configure Security			✓	
	Terminate Suspend Resume Unfreeze		✓	✓	
	Invoke	Configured by the administrator. Until policies are defined, the default is everyone.			
	Monitor	✓	✓	✓	

## User Management

Resource	Action	IntegrationMonitor	IntegrationOperator	IntegrationAdmin	IntegrationUser
Dynamic Control Selectors	Configure		✓	✓	
	View	✓	✓	✓	
Worklist Tasks	Modify Reassign Complete Cancel Claim Delete		✓	✓	✓
	Configure Security			✓	
	View	✓	✓	✓	✓
Message Broker Channels	Subscribe Publish	Configured by the administrator. Until policies are defined, the default is everyone.			
	Reset counts		✓	✓	
	Configure security			✓	
	View	✓	✓	✓	
Event Generators	Create Delete Modify Suspend/Resume		✓	✓	
	View	✓	✓	✓	

Resource	Action	IntegrationMonitor	IntegrationOperator	IntegrationAdmin	IntegrationUser
Users, Groups, and Roles	Create Delete Modify			✓	
	View			✓	
Business Calendars	Create Delete Modify		✓	✓	
	Manage user and group mappings		✓	✓	
	View	✓	✓	✓	
Application Integration	Configure connection parameters and environment variables		✓	✓	
	Configure security			✓	
	Monitor	✓	✓	✓	
Trading Partner and Service Profiles	Create Delete Modify		✓	✓	
	View	✓	✓	✓	

User Management

Resource	Action	IntegrationMonitor	IntegrationOperator	IntegrationAdmin	IntegrationUser
Trading Partner Management Server	Configure		✓	✓	
	View	✓	✓	✓	
System	Configure archiving policies or manually kick off archive and purge process			✓	
	Manage password aliases			✓	
	View repository size	✓	✓	✓	

## Overview of the User Management Module

The following table lists the pages you can access from the User Management module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
<b>Users</b>		
View and Edit Users	View a list of users. User name, email, group membership, and associated business calendar are displayed.	<a href="#">“Listing and Locating Users” on page 10-16</a>
	Filter the list by user name or group membership. Use ? to match any single character or * to match zero or more characters.	
	Delete one or more users.	
Add New User	Add a user by assigning a unique name and password. Optionally, assign a description, email address, group membership, and business calendar.	<a href="#">“Adding a User” on page 10-11</a>
View User Details	View user properties.	<a href="#">“Viewing and Changing User Properties” on page 10-17</a>
Edit User Details	Change user properties. Add a description, assign a calendar, assign or update the user’s email address, update the password, or assign the user to one or more groups.	<a href="#">“Viewing and Changing User Properties” on page 10-17</a>
<b>Groups</b>		
View and Edit Groups	View a list of groups. Group name, description and group membership are displayed.	<a href="#">“Listing and Locating Groups” on page 10-16</a>
	Filter the list by group name. Use ? to match any single character or * to match zero or more characters.	
	Delete one or more groups.	

Page	Associated Tasks	Topics
Add New Group	Add a group by assigning a unique name. Optionally assign a description or assign the group to one or more other groups.	<a href="#">“Adding a Group” on page 10-12</a>
View Group Details	View group properties.	<a href="#">“Viewing and Changing Group Properties” on page 10-19</a>
Edit Group Details	Change group properties. Add a description, or update the group membership.	<a href="#">“Viewing and Changing Group Properties” on page 10-19</a>
<b>Roles</b>		
View and Edit Roles	View a list of roles. Role name is displayed.	<a href="#">“Listing and Locating Roles” on page 10-17</a>
	Filter the list by role name. Use ? to match any single character or * to match zero or more characters.	
	Delete one or more roles.	<a href="#">“Deleting Users, Groups, or Roles” on page 10-20</a>
Add New Role	Add a role by assigning a unique role name and defining the conditions that constitute the role statement.	<a href="#">“Adding a Role” on page 10-13</a>
View Role Details	View or change role conditions. Add, delete, or reorder conditions.	<a href="#">“Viewing and Setting Role Conditions” on page 10-20</a>
Add Role Conditions	Define a condition to be added.	<a href="#">“Constructing a Role Statement” on page 10-13</a>
Sort Role Conditions	Change the order of the conditions in the list.	<a href="#">“Constructing a Role Statement” on page 10-13</a>
Edit Role Conditions Command	Change the command that joins conditions.	<a href="#">“Constructing a Role Statement” on page 10-13</a>



## Adding a User


The Add New User page allows you to create a new user.

**Note:** All newly created users are included in the IntegrationUsers group. If the user should not be a member of the IntegrationUsers you can remove the assignment by editing the user after it has been created.

### To add a user:

1. From the home page, select the **User Management** module.
2. From the left panel, select **Create New** to display the Add New User page.
3. In the **User Name** field, enter a unique name.
 

**Note:** The name must be unique across users and groups. That is, you cannot create a user that has the same name as a group.
4. In the **Description** field, enter a description for the user (optional).
5. From the **Calendar** drop-down list, select a business calendar for the user (optional).
6. In the **E-mail** field, enter the email address for the user (optional).
7. In the **Password** field, enter the password.
 

**Note:** The password must be at least 8 characters long.
8. In the **Confirm Password** field, enter the password again.
9. Assign the user to one or more groups as follows:
  - a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
  - b. Click the  icon to move the selected groups to the **Current Groups** list.
10. Do one of the following:
  - To create the user, click **Add User**.

The View and Edit Users page is displayed. The new user is included in the list. (You may need to page forward to see the new user.)


**Note:** If there is an error, the Add New User page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

- To disregard changes and return to the View and Edit Users page, click **Cancel**.

## Adding a Group

The Add New Group page allows you to create a new group.

### To add a group:

1. From the home page, select the **User Management** module.
2. From the left panel, select **Groups**.
3. From the left panel, select **Create New** to display the Add New Group page.
4. In the **Group Name** field, enter a unique name.  
**Note:** The name must be unique across users and groups. That is, you cannot create a group that has the same name as a user.
5. In the **Description** field, enter a description for the group (optional).
6. To make this group a member of one or more other groups, do the following:
  - a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
  - b. Click the  icon to move the selected groups to the **Current Groups** list.  
**Note:** To make another group a member of this group, you must update the membership assignments for that group. See [“Viewing and Changing Group Properties” on page 10-19](#).
7. Do one of the following:
  - To create the group, click **Add Group**.  
The View and Edit Groups page is displayed. The new group is included in the list. (You may need to page forward to see the new group.)  
**Note:** If there is an error, the Add New Group page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
  - To disregard changes and return to the View and Edit Groups page, click **Cancel**.

## Adding a Role

The Add New Role page allows you to create a new role.

### To add a role:

1. From the home page, select the **User Management** module.
2. From the left panel, select **Roles**.
3. From the left panel, select **Create New** to display the Add New Role page.
4. In the **Role Name** field, enter a unique name.
5. Click **Add Role**.

The role is created.

6. To add conditions to the role, click **Submit**. To learn more about creating a role statement, see [“Constructing a Role Statement.”](#)

**Note:** Each change to the role statement (adding or deleting conditions, moving the position of a condition in the list, or updating a joining command) becomes effective when it is successfully submitted.

## Constructing a Role Statement

You construct a role statement by adding conditions. See [“Adding Conditions to a Role Statement” on page 10-14](#). Each condition is joined to the previous condition by a conjunction (**and**) or disjunction (**or**) command as shown in the following figure.

**Role Statement:**


<input type="checkbox"/>	Command	Role Conditions
<input type="checkbox"/>		Groups:(Auditors)
<input type="checkbox"/>	and	Hours of Access are Between :(09:00:00,17:00:00)
<input type="checkbox"/>	or	Groups:(Administrators)

After you have added conditions to the statement, you can update the joining commands, move the position of a condition, or delete conditions. See [“Modifying the Role Statement” on page 10-15](#).

## Adding Conditions to a Role Statement


If you are logged in with sufficient privileges, you can add conditions from the View Role Details page.

### To add a Groups condition:

1. Click **Add Condition** to display the Add Role Condition page.
2. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
3. Click the  icon to move the selected groups to the **Current Groups** list.
4. Select the command. This joins the condition to the previous condition in the statement. If this is the first condition, the command setting is ignored.
5. Click **Submit**.

The condition is added to the role statement.

### To add a Users condition:

1. Click **Add Condition** to display the Add Roles Condition page.
2. From the **Available Users** list, select the required users. (To select multiple users, press and hold the **Ctrl** key as you click each additional user.)
3. Click the  icon to move the selected users to the **Current Users** list.
4. Select the command. This joins the condition to the previous condition in the statement. If this is the first condition, the command is ignored.
5. Click **Submit**.

The condition is added to the role statement.

### To add an Hours condition:

1. Click **Add Condition** to display the Add Roles Condition page.
2. Use the **From** drop-down lists to specify the start time.

3. Use the **To** drop-down lists to specify the end time.
4. Select the command. This joins the condition to the previous condition in the statement. If this is the first condition, the command is ignored.
5. Click **Submit**.

The condition is added to the role statement.


## Modifying the Role Statement

If you are logged in with sufficient privileges, you can update the joining command, move the position of the conditions, or delete conditions from the View Role Details page.

### To update the joining command:

1. Click **Edit Role Condition Commands**.
2. Make selections from the **Command** drop-down lists as required.
3. Click **Submit**.

### To sort the role conditions:

1. Click **Sort Role conditions**.
2. Move the position of a condition by clicking the up or down arrow  to the right of the condition.
3. Click **Submit**.

### To delete role conditions:

1. Click the check box to the left of the condition to select it.
2. Click **Delete Condition**.

## Listing and Locating Users

The View and Edit Users page lists the users defined in the default security realm.

### To list and locate users:





1. From the home page, select the **User Management** module to display the View and Edit Users page.
2. To locate a specific user, do one of the following:
  - Filter by user name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **User Name**. The users matching the search criteria are displayed.
  - Filter by group name. Enter the search target (use ? to match any single character or \* to match zero or more characters.), then click **Group Name**. The users assigned to groups matching the search criteria are displayed.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◄, first ◀, or last ▶ page.

## Listing and Locating Groups

The View and Edit Groups page lists the groups defined in the default security realm.

### To list and locate groups:




1. Select the **User Management** module from the home page.
2. Select **Groups** from the left panel to display the View and Edit Groups page.
3. To locate a specific group, do one of the following:
  - Filter by group name. Enter the search target, then click **Group Name**. The groups matching the search criteria are displayed.
  - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.

- Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Listing and Locating Roles

The View and Edit Roles page lists the roles defined in the default security realm.

### To list and locate roles:

1. From the home page, select the **User Management** module.
2. From the left panel, select **Roles** to display the View and Edit Roles page.
3. To locate a specific role, do one of the following:
  - Filter by role name. Enter the search target, then click **Role Name**. The roles matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow  buttons to go to the next or previous page.

## Viewing and Changing User Properties

The View User Details page displays user properties. If you are logged in with sufficient privileges, you can access the Edit User Details page to make changes.

### To view user properties:

1. Locate the user. See [“Listing and Locating Users” on page 10-16](#).
2. Click the user name to display the View User Details page.

The user name, description, calendar, e-mail, and group membership are displayed.

### To change user properties:

1. On the View User Details page, click **Edit User**.
2. In the **Description** field, enter or update the description for the user (optional).

3. From the **User Calendar** drop-down list, do one of the following (optional):

- Select a business calendar for the user.
- Select **No Calendar**.

4. To update the password:


- In the **Current Password** field, enter the current password.
- In the **New Password** field, enter the new password.

**Note:** The password must be at least 8 characters long.


- In the **Confirm Password** field, enter the new password again.

5. Add or remove group assignments as follows:

To add groups:

- From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
- Click the  icon to move the selected groups to the **Current Groups** list.

To remove groups:

- From the **Current Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
- Click the  icon to move the selected groups to the **Available Groups** list.

6. Do one of the following:

- To update the user, click **Submit**.

The View and Edit Users page is displayed.

**Note:** If there is an error, the Edit User Details page is redisplayed. A message indicating the problem is displayed above the input requiring correction.

- To reset to the last saved values, click **Reset**.
- To disregard changes and return to the View and Edit Users page, click **Cancel**.



## Viewing and Changing Group Properties

The View Group Details page displays group properties. If you are logged in with sufficient privileges, you can access the Edit Group Details page to make changes.

### To view group properties:

1. Locate the group. See [“Listing and Locating Groups” on page 10-16](#).
2. Click the group name to display the View Group Details page.


The following table summarizes the information displayed:

Property	Description
Group Name	Name assigned to the group.
Group Membership	Groups that this group is a member of. Each name is a link to the View Group Details page for the group.
Member Groups	Groups that are members of this group. Each name is a link to the View Group Details page for the group.
Member Users	Users that are members of this group. Each name is a link to the View User Details page for the user.


### To change group properties:

1. On the View Group Details page, click **Edit Group**.
2. In the **Description** field, enter or update the description for the user (optional).
3. Add or remove group membership assignments as follows:

To add groups:

- a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
- b. Click the  icon to move the selected groups to the **Current Groups** list.

To remove groups:

- a. From the **Current Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
  - b. Click the  icon to move the selected groups to the **Available Groups** list.
4. Do one of the following:
- To update the group, click **Submit**.  
The View and Edit Groups page is displayed.
- Note:** If there is an error, the Edit Group Details page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
- To reset to the last saved values, click **Reset**.
  - To disregard changes and return to the View and Edit Groups page, click **Cancel**.

## Viewing and Setting Role Conditions

The View Role Details page displays the role statement. If you are logged in with sufficient privileges, you can access the Edit Role Details page to make changes.

**To view and edit role conditions:**

1. Locate the role. See [“Listing and Locating Roles” on page 10-17](#).
2. Click the role name to display the View Role Details page.  
The role name and role statement are displayed.
3. To edit the role statement, see [“Constructing a Role Statement” on page 10-13](#).

## Deleting Users, Groups, or Roles

You can delete users, groups, or roles from the respective View and Edit page.

**To delete users:**

1. Locate the users to be deleted. See [“Listing and Locating Users” on page 10-16](#).
2. Click the check box to the left of the users to be deleted to select them.
3. Click **Remove Selected Users**.

**To delete groups:**

1. Locate the groups to be deleted. See [“Listing and Locating Groups” on page 10-16](#).
2. Click the check box to the left of the groups to be deleted to select them.
3. Click **Remove Selected Groups**.

**To delete roles:**

1. Locate the roles to be deleted. See [“Listing and Locating Roles” on page 10-17](#).
2. Click the check box to the left of the roles to be deleted to select them.
3. Click **Remove Selected Roles**.

User Management

# Business Calendar Configuration

This section provides the information you need to use the *Business Calendar Configuration* module of the WebLogic Integration Administration Console to:

- Create and update business calendars.
- Export and import business calendars.
- Map calendars to users.

**Note:** You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to map, import, or otherwise modify a business calendar. See [“Default Groups, Roles, and Security Policies” on page 10-3](#).

The following topics are provided:

- [About Business Calendars and Business Time Calculations](#)
- [Overview of the Business Calendar Configuration Module](#)
- [Adding a Business Calendar](#)
- [Listing and Locating Business Calendars](#)
- [Viewing and Changing Business Calendars](#)
- [Defining a Time Period Rule](#)
- [Exporting and Importing Business Calendars](#)
- [Assigning Business Calendars to Users and Groups](#)

- [Deleting Business Calendars](#)

# About Business Calendars and Business Time Calculations

Business calendars represent the operating hours of a business. A business calendar specifies a time zone and a set of time period rules. The time period rules determine the days, dates, and hours that are free (available for business activities) and busy (unavailable for business activities). Time period rules are evaluated in sequence as follows:

- Rules that appear later in the list supersede rules that appear earlier in the list.
- Intervals for which there are no rules are busy intervals.

The following examples illustrate how to a business calendar is constructed.

## Example 1

The following is an example of a business calendar for the year 2003:

Time Periods	Free or Busy
Mon, 9:00AM - 5:00PM	Free
Wed, 9:00AM - 5:00PM	Free
Fri, 9:00AM - 5:00PM	Free
Jan 1, 2003	Busy
Oct 13, 2003	Busy
Feb 17, 2003	Busy
May 26, 2003	Busy
Jul 4, 2003	Busy
Sep 1, 2003	Busy

In the above, the first three rules define Mondays, Wednesdays, and Fridays from 9 to 5 as free. By default, all other time is busy. The remaining rules designate the American business holidays which fall on Mondays, Wednesdays, or Fridays as busy, selectively overriding the regular free intervals.

## Example 2

The following is an example of a business calendar for a night-shift worker whose regular hours are from 10 PM to 6 AM three nights a week.

	Time Periods	Free or Busy
	Sun, 10:00PM - 11:59PM	Free
	Mon, 0:00AM - 6:00AM	Free
	Tue, 10:00PM - 11:59PM	Free
	Wed, 0:00AM - 6:00AM	Free
	Thu, 10:00PM - 11:59PM	Free
	Fri, 0:00AM - 6:00AM	Free

Of the calendars defined within WebLogic Integration, one must be designated the system calendar. Initially, the system calendar is a default calendar named **System Calendar**, but you can switch the system calendar designation to a custom calendar at any time.

When allocating worklist tasks to users, the business calendar assigned to a user can be referenced to determine whether or not the user is available. Each user is associated with one of the following:

- *A named calendar*

In this case, the specified calendar is used to determine busy and free time.

- *No calendar*

In this case, the calendar currently designated as the system calendar is used to determine busy or free time.

Calendars can also be assigned to groups, but a group calendar is not “inherited” by users in the group, but rather can be used to determine busy or free time for the group. To learn more about how calendars can be used in determining task dates, see “Understanding Task Dates and Calendars” in [Worklist Controls and WebLogic Integration](#) in *Building Integration Applications*.

In addition to being mapped to users or groups in order to determine user availability, business calendars are used in the calculation of *business time*. When specifying the times that business events are to take place (such as a message being sent or a particular task instance becoming overdue), you may wish to express time intervals in business time by associating the interval with a business calendar. For example, suppose the following:

- A Timer event generator is configured to send a message every 24 hours from January 1 to January 31, 2003.
- The business calendar shown in [Example 1](#) is associated with the 24 hour interval.  
Therefore, the 24 hour interval represents business time calculated against the calendar.

When calculating business time, free time periods are counted to determine when a business time interval has elapsed. Based on the business calendar shown at the beginning of this section, the free days in January fall on the following dates: 3, 6, 8, 10, 13, 15, 17, 22, 24, 27, 29, 31. Since each free day has 8 free hours, a Timer event generator configured to send a message every 24 business hours would send messages at 5 PM on the 8th, 15th, 24th, and 31st.

To learn more about configuring Timer event generators, see [“Defining Channel Rules for a Timer Event Generator” on page 5-16](#).

When calculating business time against a business calendar, if the interval is specified by a mixture of days, hours, and minutes (for example, 3 days, 4 hours, and 5 minutes), the days are accounted for first, then the hours, and finally the minutes. The passage of a day in a business calendar is the passage of any day or date that has any free time defined for it.

For additional information about the methods available for business calendar operations (for example, determining whether or not a user is free or determining a due date based on the passage of a business time interval), see the [com.bea.wli.calendar.api](#) Javadoc.

# Overview of the Business Calendar Configuration Module

The following table lists the pages you can access from the Business Calendar Configuration module. The tasks and topics associated with each are provided.

Page	Associated Tasks	Topics
Business Calendar Management	View a list of business calendars. Calendar name, status (in use: true or false), and type (system calendar: true or false) are displayed.	<a href="#">“Listing and Locating Business Calendars” on page 11-6</a>
	Filter the list by business calendar name. Use ? to match any single character or * to match zero or more characters.	
	Export or import business calendar time period rules and time zone.	<a href="#">“Exporting and Importing Business Calendars” on page 11-9</a>



Page	Associated Tasks	Topics
View Business Calendar Details	View business calendar properties. Business calendar name, time zone, time period rules, and type (indication of whether or not the calendar is the system calendar) are displayed.	<a href="#">“Viewing and Changing Business Calendars” on page 11-6</a>
	Update time period rules by adding, changing, deleting or reordering rules	
Add Business Calendar Time Period	Define a time period rule to be added.	<a href="#">“Defining a Time Period Rule” on page 11-8</a>
Update Business Calendar Time Period	Change an existing time period rule.	<a href="#">“Defining a Time Period Rule” on page 11-8</a>
Sort Calendar Rules	Change the order of the rules in the list.	<a href="#">“Viewing and Changing Business Calendars” on page 11-6</a>
Map Users to a Business Calendar	Select a business calendar and assign the calendar to selected users.	<a href="#">“Assigning Business Calendars to Users and Groups” on page 11-11</a>
	Remove the business calendar assignment from selected users.	
Map Groups to a Business Calendar	Select a business calendar and assign the calendar to selected groups.	<a href="#">“Assigning Business Calendars to Users and Groups” on page 11-11</a>
	Remove the business calendar assignment from selected groups.	

## Adding a Business Calendar

The Create Business Calendar page allows you to add a new calendar.

### To add a business calendar:

1. From the home page, select the **Business Calendar Configuration** module.
2. From the left panel, select **Create New** to display the Create Business Calendar page.
3. In the **Business Calendar Name** field, enter a unique name.

4. Click **Create**.







The business calendar is created with a default set of time period rules.

5. Update the time period rules as required. See [“Viewing and Changing Business Calendars” on page 11-6](#).

## Listing and Locating Business Calendars

The Business Calendar Management page lists the defined business calendars. For each business calendar, the **In Use** and **Is System Calendar** status (true or false) are also displayed.

### To list and locate roles:

1. From the home page, select the **Business Calendar Configuration** module.
2. To locate a specific business calendar, do one of the following:
  - Filter by business calendar name. Enter the search target, then click **Search**. The business calendars matching the search criteria are displayed.
  - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
  - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

## Viewing and Changing Business Calendars

The View Business Calendar Details page allows you to view the business calendar properties. If you are logged in with sufficient privileges, you can:

- Update the time zone or designate a calendar as the system calendar.
- Add a time period rule.
- Change a time period rule.
- Delete one or more time period rules.
- Sort the time period rules.

**To view business calendar properties:**

1. Locate the business calendar. See [“Listing and Locating Business Calendars” on page 11-6.](#)
2. Click the calendar name to display the View Business Calendar Details page.

The calendar name, time zone, type (system calendar true or false), and time period rules are displayed.

**To update the time zone or designate a calendar as the system calendar:**

1. On the View Business Calendar Details page, click **Edit Calendar Details**.
2. Do one or both of the following:
  - To update the time zone, select a new time zone for the **Time Zone** drop-down list.
  - To designate this calendar as the system calendar, check the **Set as system calendar** check box.


**To add a time period rule:**

1. On the View Business Calendar Details page, click **Add a New Rule**.  
The Add Business Calendar Time Period page is displayed.
2. Define the time period as required. See [“Defining a Time Period Rule” on page 11-8.](#)
3. Click **Submit** to add the rule and return to the View Business Calendar Details page.

**To change a time period rule:**

1. From the Time Period Rules table, select the rule to be changed.  
The Update Business Calendar Time Period page is displayed.
2. Define the time period as required. See [“Defining a Time Period Rule” on page 11-8.](#)
3. Click **Submit** to update the rule and return to the View Business Calendar Details page.

**To sort the time period rules:**

1. On the View Business Calendar Details page, click **Sort Calendar Rules**.  
The Sort Calendar Rules page is displayed.
2. Move the position of a rule by clicking the up or down arrow  to the right of the rule.
3. Click **Submit** to update the list and return to the View Business Calendar Details page.

### To delete a time period rule:

1. In the Time Period Rules table, click the check box to the left of the rule or rules to be deleted.
2. Click **Delete Rule**.

## Defining a Time Period Rule

The Add Business Calendar Time Period and Update Business Calendar Time Period pages allow you to define the properties of a time period rule. There are three types of rules:

- Day of the Week
- Calendar Date
- Date Range

### To define a Day of the Week rule:

1. From the **Time Period Type** drop-down list, select **Day of Week**.
2. From the **Day of Month** drop-down list, select **Sun, Mon, Tues, Wed, Thu, Fri, or Sat**.
3. Specify the time period interval in 24 hour time format (also known as military time) as follows:
  - From the **Start hour and minute** drop-down lists, select the time period start hour and minute.
  - From the **End hour and minute** drop-down lists, select the time period end hour and minute.

**Note:** If you do not specify start and end times (that is, if **00:00** is specified for both) the **Free or Busy** status specified in the following step applies to the entire day.

4. From the **Free or Busy** drop-down list, select **Free** or **Busy**.

### To define a Calendar Date rule:

1. From the **Time Period Type** drop-down list, select **Calendar Date**.
2. In the **Year** field, specify the year in **YYYY** format.
3. From the **Month** drop-down list, select the month.
4. From the **Day of the Month** drop-down list, select the date.

5. Specify the time period interval in 24 hour time format (also known as military time) as follows:
  - From the **Start hour and minute** drop-down lists, select the time period start hour and minute.
  - From the **End hour and minute** drop-down lists, select the time period end hour and minute.

**Note:** If you do not specify start and end times (that is, if **00:00** is specified for both) the **Free or Busy** status specified in the following step applies to the entire day.
6. From the **Free or Busy** drop-down list, select **Free** or **Busy**.

#### To define a Date Range rule:

1. From the **Time Period Type** drop-down list, select **Date Range**.
2. In the **Year** field, specify the year in *YYYY* format.
3. Select the time period start date as follows:
  - From the **Start Month** drop-down list, select the month.
  - From the **Start Day of the Month** drop-down list, select the date.
4. Select the time period end date as follows:
  - From the **End Month** drop-down list, select the month.
  - From the **End Day of the Month** drop-down list, select the date.
5. From the **Free or Busy** drop-down list, select **Free** or **Busy**.

## Exporting and Importing Business Calendars

You can export and import business calendars. When you export a business calendar, the calendar name, time zone, and business rules are exported in XML format. When you import a calendar, if the name specified by the `<sch:name>` element in the in the XML file matches an existing calendar, the rules and time zone defined in the existing calendar are overwritten by the rules defined in the XML file. If the name specified by the `<sch:name>` element does not match any existing calendar, a new calendar is created.

If the calendar you are importing has the same name as the calendar currently designated as the system calendar, the system flag element `<sch:systemFlag>` must be set to *y* in the XML file.

If you are importing a new calendar, or updating a calendar that is not currently designated as the system calendar, the system flag is reset to **F** on import, regardless of the setting in the XML file.

### To export a business calendar:

1. Locate the calendar to be exported. See “[Listing and Locating Business Calendars](#)” on [page 11-6](#).
2. Click the check box to the left of the calendar to select it.
3. Click **Export**.

The Export a Calendar page is displayed.

4. To specify a character set other than the default, enter it in the **Encoding** field. See <http://www.iana.org/assignments/character-sets> for values. If a preferred MIME name is indicated for the character set, specify that name.

**Note:** If the **Encoding** field is empty, the default character set is used.

5. Click **Submit** to download the calendar.

You are prompted to open the file or save it to a local directory.

6. Select the save option to display the **Save As** dialog.
7. Navigate to the target directory, specify an appropriate file name, and then click **Save**.

### To import a business calendar:

1. From the home page, select the **Business Calendar Configuration** module.
2. Select **Import** from the left panel.

The Import a Calendar page is displayed.

3. Specify the file in the **Business Calendar File** field. Click **Browse** to browse for the file.
4. To specify a character set other than the default, enter it in the **Encoding** field. See <http://www.iana.org/assignments/character-sets> for values. If a preferred MIME name is indicated for the character set, specify that name.

**Note:** If the **Encoding** field is empty, the default character set is used.

5. Click **Submit** to import the specified calendar file.

The calendar is imported and the Business Calendar Management page is displayed.

## Assigning Business Calendars to Users and Groups

The Map Users to a Business Calendar page allows you to:

- Assign a business calendar to one or more users.
- Remove the business calendar assignment from one or more users.

The Map Groups to a Business Calendar page allows you to:

- Assign a business calendar to one or more groups.
- Remove the business calendar assignment from one or more groups.

**Note:** If a user is not mapped to a calendar, the system calendar is used. A calendar mapped to a group is not “inherited” by users in the group. To learn how a calendar mapped to a user or group can be used in determining worklist task dates, see “Understanding Task Dates and Calendars” in [Worklist Controls and WebLogic Integration](#) in *Building Integration Applications*.

### To assign a business calendar to one or more users:

1. From the home page, select the **Business Calendar Configuration** module.
2. From the left panel, select **Business Calendar Mapping** to display the Map Users to a Business Calendar page.
3. From the **Business Calendar Mapping** drop-down list, select a named calendar, or select **System Calendar** to specify the calendar currently designated as the system calendar.
4. Click the check box to the left of the users to which the calendar is to be assigned.
5. Click **Map** to assign the selected calendar to the selected users.

### To remove the business calendar assignment from one or more users:

1. From the home page, select the **Business Calendar Configuration** module.
2. From the left panel, select **Business Calendar Mapping** to display the Map Users to a Business Calendar page.
3. Click the check box to the left of the users from which the calendar assignment is to be removed.
4. Click **Unmap** to remove the business calendar assignment from the selected users.

**To assign a business calendar to one or more groups:**

1. From the home page, select the **Business Calendar Configuration** module.
2. From the left panel, select **Business Calendar Mapping**.
3. From the left panel, select **Map Groups** to display the Map Groups to a Business Calendar page.
4. From the **Business Calendar Mapping** drop-down list, select a named calendar, or select **System Calendar** to specify the calendar currently designated as the system calendar.
5. Click the check box to the left of the groups to which the calendar is to be assigned.
6. Click **Map** to assign the selected calendar to the selected groups.

**To remove the business calendar assignment from one or more users:**

1. From the home page, select the **Business Calendar Configuration** module.
2. From the left panel, select **Business Calendar Mapping**.
3. From the left panel, select **Map Groups** to display the Map Groups to a Business Calendar page.
4. Click the check box to the left of the groups from which the calendar assignment is to be removed.
5. Click **Unmap** to remove the business calendar assignment from the selected groups.

## Deleting Business Calendars

The Map Users to a Business Calendar page allows you to delete selected calendars.

**Note:** You cannot delete a calendar if it is in use (mapped to a user) or is designated as the system calendar. See [“Assigning Business Calendars to Users and Groups” on page 11-11](#) to update the **In Use** status.

**To delete calendars:**

1. Locate the calendars to be deleted. See [“Listing and Locating Business Calendars” on page 11-6](#).
2. Click the check box to the left of the calendars to be deleted to select them.
3. Click **Delete** to delete the selected calendars.



**Note:** If any of the selected calendars are currently being referenced by a Timer event generator, a warning is displayed. Click **Cancel** to cancel the delete operation, or **OK** to delete the selected calendars anyway.



# TPM Schema

This section describes the schema for Trading Partner Management (TPM) data that you can exchange with the TPM repository using:

- The WebLogic Integration Administration Console
- The Workshop TPM controls
- The Bulk Loader utility

## TPM Overview

The TPM schema allows you to configure WebLogic Integration to share information among trading partners by defining the following:

- Addresses, phone and fax numbers
- Authentications, encryptions, and certificates
- Protocol transports for RosettaNet, ebXML, and Internet services
- Data unique to your business needs

A trading partner can have one or more service bindings that use different transport protocols for the exchange of documents. Each transport can use a variety of security authentication options, for client, server, signing, and messaging roles. The TPM schema allows you define the complete set of communication and configuration options for all trading partners.

## Architecture: Trading Partners and Services

The root element of the TPM schema is the `trading-partner-management` element. The element provides logging and messaging options, and contains the two essential child elements for any configuration:

- `trading-partner`—a business entity that has authorization to send and receive business messages.

The `trading-partner` element defines the settings for a single trading partner: authentication, security, and protocol options.

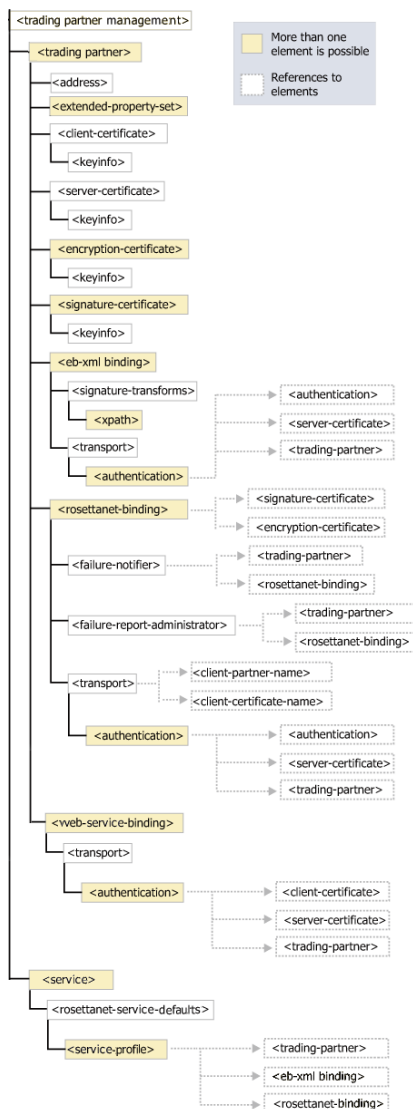
- `service`—a business process a trading partner offers

The `service` element defines settings that describe how pairs of trading partners communicate: message protocols, message tracking, and RosettaNet service options.

The `service` element is rather simple and contains the following elements:

- `rosettanet-service-defaults`—for describing optional RosettaNet settings
- `service-profile`—for describing how pairs of trading partners communicate

The `trading-partner` element is far more complex. The following illustrations present the entity relationships among its elements.



## Protocols and Security

The TPM schema provide configuration options for communication using the following service protocols:

- ebXML
- RosettaNet
- Web services available through JWS and JPD

The TPM schema provide settings for the authentication of trading partners as they send messages using these protocols at runtime for:

- authentication credentials for outbound connections
- mapping of trading partners to WebLogic Integration users for inbound connections
- transport level security with a Secure Sockets Layer (SSL)
- message level encryption and digital signatures

You configure these security and authentication options using:

- The `authentication` elements, that reside within a `transport` element for a given service protocol and allow clients and servers to authenticate.
- The individual service binding elements for each protocol, that provide settings for digital signatures and encryption for messaging.

The individual binding elements for each of the protocol services support non-repudiation by digitally signing outbound messages and acknowledgements based on the attributes that require signatures on messages and acknowledgement receipts. You can securely log message information as well.

The TPM schema supports the use of password aliases so you can refer to the password aliases in the WebLogic Integration password store. To learn more about password security, see [“Password Aliases and the Password Store” on page 9-6.](#)

## Extensibility

You can include custom information unique to your business needs using extended property sets. The extended-property-set allows any XML elements and attributes to be specified as child nodes of the extended-property-set element. To learn more about extending TPM schema, see [“extended-property-set Element” on page A-20.](#)

## Test Mode

You can deploy your TPM options in a development environment without the need to specify explicit service profiles between trading partners. The test mode attribute on the

trading-partner-management element allows you to test and deploy TPM business settings using the default bindings for your trading partners. This mode does not require separate service profiles to be set up for each pair of partners that exchange business messages.

To learn more about using test mode, see [“trading-partner-management Element” on page A-53](#).

## Related Topics

To learn more about using the WebLogic Integration Administration Console for TPM, see [“Trading Partner Management” on page 8-1](#).

To learn more about Workshop TPM controls, see [TPM Control](#) in *Building Integration Applications* in the WebLogic Workshop help.

To learn more about using the Bulk Loader, see [“Using the Bulk Loader” on page B-1](#).

To learn more about XML, see the [W3C Recommendation, XML-Signature Syntax and Processing](#) at the Web site of the W3C.

To learn more about the ebXML protocol, see the [ebXML Collaboration-Protocol Profile and Agreement Specification - Version 2.0](#) at the Oasis Web site.

To learn more about ebXML in general, visit the [ebXML Web site](#).

To learn about the RosettaNet protocol, visit the [RosettaNet Web site](#).

## address Element

This element defines the external business address for a trading partner.

### Syntax

```
<address>partnerMailAddress</address>
```

### Attributes

none

### Type

xs:string

## References

### To

none

### Children

none

## Hierarchy

### Used By

[trading-partner Element](#)

### Children

none

## authentication Element

This element specifies the authentication properties for a remote client that connects to the parent transport endpoint.

## Syntax

```
<authentication>
  client-partner-name="tradingPartnerReference"
  client-authentication=
    "BASIC"
    /NONE
    /SSL_CERT_MUTUAL"
  username="loginName"
  password-alias="clientPassword"
  client-certificate-name="certificateReference"
  server-authentication=
    "NONE"
    /SSL_CERT"
  server-certificate-name="certificateReference"/>
```



## Attributes

Attribute		
<b>client-authentication</b>	<b>Description</b>	Specifies whether to use client authentication, and if so, what kind.
	<b>Allowable Values</b>	BASIC—username and password NONE—no authentication SSL_CERT_MUTUAL—mutual SSL certificates
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	none
<b>client-certificate-name</b>	<b>Description</b>	A reference to the name of the client certificate for mutual SSL authentication.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	reference
	<b>Default Value</b>	none
<b>client-partner-name</b>	<b>Description</b>	The name of the trading partner in the TPM repository to which the authentication applies.
	<b>Allowable Values</b>	any
	<b>Use</b>	required
	<b>Type</b>	reference
	<b>Default Value</b>	none

Attribute		
<b>password-alias</b>	<b>Description</b>	This is a reference to the password alias in the WebLogic Integration password store. The password is retrieved from the password store and is required when BASIC authentication is used.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>server-authentication</b>	<b>Description</b>	Specifies whether to use server authentication, and if so, what kind.
	<b>Allowable Values</b>	NONE—no authentication SSL_CERT—SSL certificate authentication
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	no default value
<b>server-certificate-name</b>	<b>Description</b>	A reference to the name of the server certificate for SSL authentication.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	reference
	<b>Default Value</b>	none

Attribute		
username	Description	The user name for basic client authentication.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none

References

- To
- [client-certificate Element](#)
  - [server-certificate Element](#)
  - [trading-partner Element](#)

From

none

Hierarchy

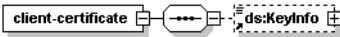
Used By

- [transport Element](#)

Children

none

client-certificate Element



This element defines a digital certificate of a trading partner for client authentication access to a WebLogic Integration communication end point.

# Syntax

```
<client-certificate
  name="certificateName"
  password-alias="keystoreEntryPasswordAlias">
  <ds:KeyInfo
    .
    .
    .
  </ds:KeyInfo>
</client-certificate>
```

# Attributes

Attribute		
name	Description	The name for the client certificate in the TPM repository. The name is also the entry name in the local keystore.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none
password-alias	Description	This is a reference to the entry in the WebLogic Integration password store for the encrypted password. The encrypted password is used for accessing the password-protected keystore entry.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none

## References

### To

none

### From

[authentication Element](#)

## Hierarchy

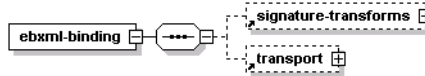
### Used By

[trading-partner Element](#)

### Children

ds:KeyInfo

## ebxml-binding Element



This element defines the ebXML business protocol specific bindings of the parent trading partner.

The ebXML protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the attributes `is-signature-required` and `is-receipt-signature-required`.

## Syntax

```

<ebxml-binding
  business-protocol-name="protocolName"
  business-protocol-version="versionNo"
  delivery-semantics=" [BESTEFFORT
                      /ONCEANDONLYONCE
                      /ATLEASTONCE
                      /ATMOSTONCE]"
  is-default=" [true/false]"
  is-receipt-signature-require=" [true/false]"
  is-signature-required=" [true/false]"
  name="bindingName"

```

```
persist-duration="intervalNo"
retries="retriesNo"
retry-interval="retryIntervalNo"
signature-certificate-name="signatureCertificate">
<signature-transforms
.
.
.
/>
<transport
.
.
.
/>
</ebxml-binding>
```

# Attributes

Attribute		
name	Description	The name for the binding in the TPM repository. A trading partner may have multiple ebxml-binding elements, so the name must be unique to the parent trading-partner element.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none

Attribute		
business-protocol-name	Description	Identifies the business protocol for message exchange.
	Allowable Values	ebXML
	Use	optional
	Type	xs:string
	Default Value	none
business-protocol-version	Description	Identifies the version of the business-protocol name.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none

Attribute		
delivery-antics	Description	This attribute specifies reliable messaging behavior.
	Allowable Values	<p>BESTEFFORT—best effort attempt to deliver messages. No reliable messaging.</p> <p>ONCEANDONLYONCE—Once and only once reliable messaging. Select this option for messaging that requires acknowledgement.</p> <p>ATLEASTONCE—at least once reliable messaging. Select this option for messaging that requires acknowledgement, but not duplicate elimination.</p> <p>ATMOSTONCE—at most once reliable messaging. Select this option for messaging that requires duplicate elimination, but not acknowledgement.</p>
	Use	optional
	Type	xs:NMTOKEN
	Default Value	false
is-default	Description	Identifies the default ebxml-binding for a trading partner in the event it has more than one.
	Allowable Values	<p>false</p> <p>true</p>
	Use	optional
	Type	xs:boolean
	Default Value	none



Attribute		
<b>is-receipt-signature-required</b>	<b>Description</b>	<p>This setting, if true, specifies that the party who receives the ebXML messages from this trading partner through this binding must acknowledge them using the digitally signed receipt messages. The receipt messages must use the certificate of the acknowledging party.</p> <p>You can control the archival of signed receipts in a secure audit log by the global attribute <code>secure-audit-logging</code> in the root element <code>trading-partner-management</code>.</p>
	<b>Allowable Values</b>	<p>false</p> <p>true</p>
	<b>Use</b>	<p>optional</p>
	<b>Type</b>	<p>xs:boolean</p>
	<b>Default Value</b>	<p>none</p>

Attribute		
<b>is-signature-required</b>	<b>Description</b>	<p>This setting, if true, specifies that parties must digitally sign messages they send to the trading partner through this binding.</p> <p>You can control the archival of signed messages in a secure audit log by the global attribute <code>secure-audit-logging</code> in the root element <code>trading-partner-management</code>.</p>
	<b>Allowable Values</b>	<p>false</p> <p>true</p>
	<b>Use</b>	optional
	<b>Type</b>	<code>xs:boolean</code>
	<b>Default Value</b>	none
<b>persist-duration</b>	<b>Description</b>	<p>Specifies the duration for which messages have to be stored persistently for the purpose of duplicate elimination.</p>
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	<code>xs:string</code>
	<b>Default Value</b>	none

Attribute		
<b>retries</b>	<b>Description</b>	Specifies the maximum number of times to attempt to send a reliably delivered message.
	<b>Allowable Values</b>	Any positive Integer
	<b>Use</b>	optional
	<b>Type</b>	xs:nonNegativeInteger
	<b>Default Value</b>	3
<b>retry-interval</b>	<b>Description</b>	This attribute defines the time interval between attempts to send a reliably delivered message. The interval begins after the timeout period for message acknowledgement expires.
	<b>Allowable Values</b>	time duration string
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>signature-certificate-name</b>	<b>Description</b>	References the name of the certificate for digitally signing messages.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional  This setting is required if the if the is-signature-required or is-signature-receipt-required attributes are true.
	<b>Type</b>	reference
	<b>Default Value</b>	none

## Reference

### To

[signature-certificate Element](#)

### From

[service-profile Element](#)

## Hierarchy

### Used By

[trading-partner Element](#)

### Children

[signature-transforms Element](#)

[transport Element](#)

## encryption-certificate Element



This element defines a digital certificate for a trading partner for encrypting and decrypting exchanged messages.

## Syntax

```

<encryption-certificate
  name="certificateName"
  password-alias="keystoreEntryPasswordAlias">
  <ds:KeyInfo
    .
    .
    .
  </ds:KeyInfo>
</encryption-certificate>
  
```

## Attributes

Attribute		
<b>name</b>	<b>Description</b>	The name of the encryption certificate in the TPM repository. This name is also the entry name in the local keystore.
	<b>Allowable Values</b>	any
	<b>Use</b>	required
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>password-alias</b>	<b>Description</b>	This is a reference to the entry in the WebLogic Integration password store for the encrypted password. The encrypted password is used for accessing the password-protected keystore entry.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none

## References

### To

none

### From

[rosettanet-binding Element](#)

## Hierarchy

### Used By

[trading-partner Element](#)

**Children**

ds:KeyInfo

## extended-property-set Element



The `extended-property-set` element allows you to add custom XML nodes to your TPM configuration for your business needs.

The child elements appear within the repository as sub trees within an XML document, and can be nested.

```

<trading-partner name="ACMECORP" type="REMOTE" business-id="ACME-id">
  .
  .
  .
  <extended-property-set
    name="ACME Corp Extension"
    description="Contact Info"
    notes="the number format is important"/>
    <business-contact>Joe Smith</business-contact>
    <phone type="work">+1 123 456 7654</phone>
    <phone type="cell">+1 321 654 4567</phone>
    <city>Anytown</city>
    <state>California</state>
  </extended-property-set>
</trading-partner>
  
```

## Syntax

```

<extended-property-set
  name="propertyName"
  description="propertyDescription"
  notes="propertyNotes">
  <xmlElement
    .
    .
    .
  </xmlElement>
  
```

</extended-property-set>

## Attributes

Attribute		
name	Description	The name of the property set.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none
description	Description	A text description of the property set that appears in the WebLogic Integration Administration Console.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
notes	Description	Text notes or documentation for the property set.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none

## References

To  
none

**From**  
none

## Hierarchy

**Used By**  
[trading-partner Element](#)

**Children**  
any

## failure-notifier Element

This element represents the RosettaNet PIP failure notifier. It sends notification of failure (PIP0A1) messages to the appropriate trading partner and binding.

## Syntax

```
<failure-notifier
  trading-partner-name=" tradingPartnerReference"
  binding-name=" bindingNameReference" />
```

## Attributes

Attribute		
trading-partner-name	Description	The name of the trading partner in the TPM repository that should receive RosettaNet failure notification.
	Allowable Values	any
	Use	required
	Type	reference
	Default Value	none



Attribute		
<b>binding-name</b>	<b>Description</b>	References the name of the service binding in the TPM repository for the provider.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	reference
	<b>Default Value</b>	none

## References

### To

[rosettanet-binding Element](#)

[trading-partner Element](#)

### From

none

## Hierarchy

### Used By

[rosettanet-binding Element](#)

### Children

none

## failure-report-administrator Element

This element represents the RosettaNet PIP failure report administrator. It sends notification of failure (PIP0A1) messages to the appropriate trading partner and binding.

# Syntax

```
<failure-report-administrator
  trading-partner-name=" tradingPartnerReference"
  binding-name=" bindingReference" />
```

# Attributes

Attribute		
trading-partner-name	Description	The name of the trading partner in the TPM repository that should receive RosettaNet failure notification.
	Allowable Values	any
	Use	required
	Type	reference
	Default Value	none
binding-name	Description	The name of the binding in the TPM repository for the provider.
	Allowable Values	any
	Use	optional
	Type	reference
	Default Value	none

# References

- To
- [rosettanet-binding Element](#)
  - [trading-partner Element](#)

From

none

## Hierarchy

### Used By

[rosettanet-binding Element](#)

### Children

none

## reference simpleType

This references another element in the TPM repository.

## Syntax

```
<reference>referenceName</reference>
```

## Attributes

none

## Type

xs:string

## Hierarchy

### Used By

[authentication Element](#)

[ebxml-binding Element](#)

[failure-notifier Element](#)

[failure-report-administrator Element](#)

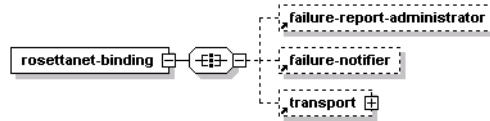
[rosettanet-binding Element](#)

[service-profile Element](#)

### Children

none

## rosettanet-binding Element



This element defines the RosettaNet business protocol specific bindings for the parent trading partner.

The RosettaNet protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the `is-signature-required` and `is-receipt-signature-required` attributes.

## Syntax

```

<rosettanet-binding
  name="bindingName"
  business-protocol-name="businessProtocolName"
  business-protocol-version="businessProtocolVersion"
  is-default="[true/false]"
  encryption-certificate-name="encryptionCertificateName"
  cipher-algorithm="[NONE|RC5|DES|TRIPLE_DES]"
  encryption-level="[NONE|PAYLOAD|ENTIRE_PAYLOAD]"
  is-signature-required="[true/false]"
  is-receipt-signature-required="[true/false]"
  signature-certificate-name="signatureCertificateName"
  retries="noOfRetries"
  retry-interval="retryIntervalNo"
  process-timeout="processTimeoutNo">
  <failure-report-administrator/>
  <failure-notifier
    .
    .
    .
  />
  <transport
    .
    .
  </transport>
</rosettanet-binding>

```

```
.  
/>  
</rosettanet-binding>
```

## Attributes

Attribute		
name	Description	The name for the binding in the TPM repository. A trading partner may have multiple rosettanet-binding elements, so the name must be unique to the parent trading-partner element.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none
business-protocol-name	Description	Identifies the business protocol for message exchange.
	Allowable Values	RosettaNet
	Use	optional
	Type	xs:string
	Default Value	none

Attribute		
<b>business-protocol-version</b>	<b>Description</b>	Identifies the version of the business-protocol name.
	<b>Allowable Values</b>	1.1 2.0
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>is-default</b>	<b>Description</b>	Identifies the default rosettanet-binding for a trading partner in the event it has more than one.
	<b>Allowable Values</b>	false true
	<b>Use</b>	optional
	<b>Type</b>	xs:boolean
	<b>Default Value</b>	false
<b>encryption-certificate-name</b>	<b>Description</b>	The name of the encryption certificate for the encryption and decryption of messages.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	reference
	<b>Default Value</b>	none

Attribute		
<b>cipher-algorithm</b>	<b>Description</b>	The cipher algorithm for encrypting messages.
	<b>Allowable Values</b>	NONE RC5 DES TRIPLE_DES
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	none
<b>encryption-level</b>	<b>Description</b>	This attribute determines how much of a message to encrypt.
	<b>Allowable Values</b>	NONE PAYLOAD ENTIRE_PAYLOAD
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	none

Attribute		
is-signature-required	Description	<p>This setting, if true, specifies that parties must digitally sign messages they send to the trading partner through this binding.</p> <p>You can control the archival of signed messages in a secure audit log by the global attribute <code>secure-audit-logging</code> in the root element <code>trading-partner-management</code>.</p>
	Allowable Values	<code>false</code> <code>true</code>
	Use	optional
	Type	<code>xs:boolean</code>
	Default Value	<code>false</code>



Attribute		
<b>is-receipt-signature-required</b>	<b>Description</b>	<p>This setting, if true, specifies that the party who receives the RosettaNet messages from this trading partner through this binding must acknowledge them using the digitally receipt messages. The receipt messages must use the certificate of acknowledging party.</p> <p>You can control the archival of signed receipts in a secure audit log by the global attribute <code>secure-audit-logging</code> in the root element <code>trading-partner-management</code>.</p>
	<b>Allowable Values</b>	false true
	<b>Use</b>	optional
	<b>Type</b>	xs:boolean
	<b>Default Value</b>	false
<b>signature-certificate-name</b>	<b>Description</b>	References the name of the certificate for digitally signing messages.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
		This setting is required if the <code>is-signature-required</code> or <code>is-signature-receipt-required</code> attributes are true.
	<b>Type</b>	reference
	<b>Default Value</b>	none

Attribute		
retries	Description	Specifies the maximum number of times to attempt to send a reliably delivered message.
	Allowable Values	Any positive Integer
	Use	optional
	Type	xs:nonNegativeInteger
	Default Value	3
retry-interval	Description	This attribute defines the time interval between attempts to send a reliably delivered message. The interval begins after the time-out period for message acknowledgement expires.
	Allowable Values	time duration string
	Use	optional
	Type	xs:string
	Default Value	none
process-timeout	Description	The amount of time a PIP can be active before timing out.
	Allowable Values	time duration string
	Use	optional
	Type	xs:string
	Default Value	none

# References

To [encryption-certificate Element](#)

[signature-certificate Element](#)

**From**

[failure-notifier Element](#)

[failure-report-administrator Element](#)

[service-profile Element](#)

## Hierarchy

**Used By**

[trading-partner Element](#)

**Children**

[failure-report-administrator Element](#)

[failure-notifier Element](#)

[transport Element](#)

## rosettanet-service-defaults Element

This element specifies RosettaNet protocol-specific configuration attributes for a service.

## Syntax

```
<rosettanet-service-defaults
  service-content-schema="schemaFilePath"
  use-dtd-validation=" [true/false]"
  validate-service-content=" [true/false]"
  validate-service-header=" [true/false]" />
```

# Attributes

Attribute		
service-content-schema	Description	<p>The XML schema for content validation.</p> <p>The service uses this schema only if use-dtd-validation is false and validate-service-content is true.</p>
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
use-dtd-validation	Description	<p>Specifies the kind of XML validation to perform. If true, the validation is from a DTD; if false, from XML schema.</p>
	Allowable Values	false true
	Use	optional
	Type	xs:boolean
	Default Value	false
validate-service-content	Description	<p>Determines whether to validate the service content of all messages.</p>
	Allowable Values	false true
	Use	optional
	Type	xs:boolean
	Default Value	false

Attribute		
validate-service-header	Description	Determines whether to validate the service header for all messages.
	Allowable Values	false true
	Use	optional
	Type	xs:boolean
	Default Value	false

## References

### To

none

### From

none

## Hierarchy

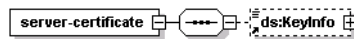
### Used By

[service Element](#)

### Children

none

## server-certificate Element



This element defines a digital certificate for a trading partner to authenticate the identity of a target server for an outbound connection.

## Syntax

```
<server-certificate
  name="serverCertificateName"
```

```
password-alias="password-alias_1">
<KeyInfo
.
.
.
</KeyInfo>
</server-certificate>
```

Attributes

Attribute		
name	Description	The name of the server certificate in the TPM repository. The name is also the entry name in the local keystore.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none
password-alias	Description	This is a reference to the entry in the WebLogic Integration password store for the encrypted password. The encrypted password is used for accessing the password-protected keystore entry.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none

References

To  
none

**From**

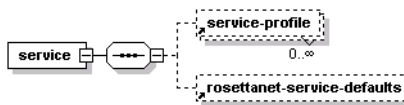
authentication Element

**Hierarchy****Used By**

trading-partner Element

**Children**

ds:KeyInfo

**service Element**

This element represents a business process that a trading partner offers.

**Syntax**

```

<service
  name="serviceName"
  description="serviceDescription"
  notes="serviceNotes"
  service-type=" [WEBSERVICE | PROCESS | SERVICECONTROL] "
  business-protocol=" [WEBSERVICE | EBXML | ROSETTANET] " >
  <service-profile
    .
    .
    .
  />
  <rosettanet-service-defaults
    .
    .
    .
  />
</service>

```

# Attributes

Attribute		
name	Description	The name of the service in the TPM repository. The name corresponds to the name of a component on the local domain.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none
description	Description	A text description of the service that appears in the WebLogic Integration Administration Console.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
notes	Description	Text documentation of the service element.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none



Attribute		
<b>service-type</b>	<b>Description</b>	The kind of service the element represents
	<b>Allowable Values</b>	WEBSERVICE—a JWS file PROCESSS—a JPD file SERVICECONTROL—a service control (JCX file)
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	none
<b>business-protocol</b>	<b>Description</b>	The business protocol for the service, which determines the child service profile bindings.
	<b>Allowable Values</b>	WEBSERVICE EBXML ROSETTANET
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	none

## References

### To

none

### From

none

## Hierarchy

### Used By

[trading-partner-management Element](#)

**Children**[rosettanet-service-defaults Element](#)[service-profile Element](#)

## service-profile Element

This element defines the interactions that two B2B trading partners agree to carry out, along with a specification for the business protocol implementation details such as messaging characteristics, security constraints, transport mechanisms, and workflow processes. Links to appropriate bindings for each trading partner specify these characteristics.

## Syntax

```
<service-profile
  local-trading-partner="localTradingPartner"
  local-binding="localBinding"
  external-trading-partner="externalTradingPartner"
  external-binding="externalBinding"
  status=" [ENABLED|DISABLED] "
  message-tracking=" [NONE|DEFAULT|METADATA|ALL] " />
```

# Attributes

Attribute		
local-trading-partner	Description	<p>This attributes references either:</p> <ul style="list-style-type: none"><li>the name of a local trading partner that hosts a JWS or JPD</li><li>the name of a local trading partner that uses a control to send messages to an external partner</li></ul> <p>If you do not provide a value in the repository for this attribute, at runtime the value for this property comes from the <code>is-default</code> attribute.</p>
	Allowable Values	any
	Use	optional
	Type	reference
	Default Value	none
local-binding	Description	<p>References the name of the binding for the corresponding local trading partner.</p> <p>If you do not provide a value for this attribute, at runtime the value property comes from the binding with the <code>is-default</code> value of <code>true</code>.</p>
	Allowable Values	any
	Use	optional
	Type	reference
	Default Value	none

Attribute		
<b>external-trading-partner</b>	<b>Description</b>	References the name of the trading partner with which the local trading partner interacts.  This attribute can describe: <ul style="list-style-type: none"> <li>• Remote trading partners</li> <li>• Collocated local trading partners</li> </ul>
	<b>Allowable Values</b>	none
	<b>Use</b>	required
	<b>Type</b>	reference
	<b>Default Value</b>	none
<b>external-binding</b>	<b>Description</b>	References the binding name for the corresponding external-external-trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	reference
	<b>Default Value</b>	none
<b>status</b>	<b>Description</b>	The deployed state of the service profile.
	<b>Allowable Values</b>	ENABLED DISABLED
	<b>Use</b>	optional
	<b>Type</b>	xs:NMTOKEN
	<b>Default Value</b>	DIASABLED

Attribute		
message-tracking	Description	Determines whether to track messages, and if so, at what level.
	Allowable Values	NONE—no message tracking DEFAULT—default message tracking options METADATA—track message metadata ALL—track all message data
	Use	optional
	Type	xs:NMTOKEN
	Default Value	DEFAULT

## References

**To**

- [ebxml-binding Element](#)
- [rosettanet-binding Element](#)
- [trading-partner Element](#)
- [web-service-binding Element](#)

**From**

none

## Hierarchy

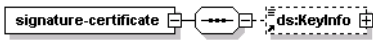
**Used By**

- [service Element](#)

**Children**

none

# signature-certificate Element



This element identifies a digital certificate for a trading partner and digitally signs messages for the associated trading partner.

## Syntax

```
<signature-certificate
  name="signatureCertificateName"
  password-alias="certificatePasswordAlias">
  <KeyInfo
    .
    .
    .
  />
</signature-certificate>
```

## Attributes

Attribute		
name	Description	The name of the signature certificate in the TPM repository. This name is also the entry name in the local keystore.
Allowable Values	any	
Use	required	
Type	xs:string	
Default Value	none	

Attribute		
<b>password-alias</b>	<b>Description</b>	This is a reference to the entry in the WebLogic Integration password store for the encrypted password. The encrypted password is used for accessing the password-protected keystore entry.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none

## References

### To

none

### From

[ebxml-binding Element](#)

[rosettanet-binding Element](#)

## Hierarchy

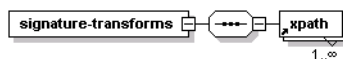
### Used By

[trading-partner Element](#)

### Children

ds:KeyInfo

## signature-transforms Element



This element defines a sequence of optional XML data transformations for a digitally signed message, before WebLogic Integration signs the message. WebLogic Integration computes the message digest after performing transforms on the message.

## Syntax

```
<signature-transforms>  
  <xpath>xpath_expression-1</xpath>  
  <xpath>xpath_expression-2</xpath>  
  <xpath>xpath_expression-3</xpath>  
</signature-transforms>
```

## Attributes

none

## References

### To

none

### From

none

## Hierarchy

### Used By

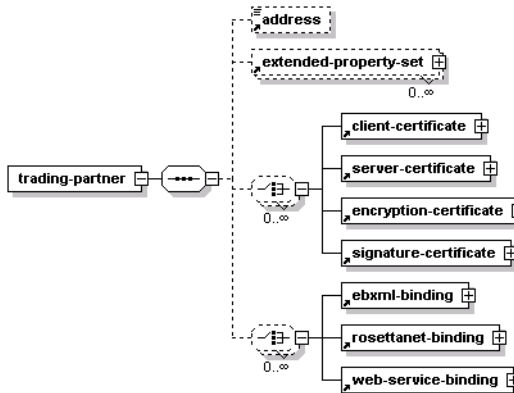
[ebxml-binding Element](#)

### Children

[xpath Element](#)



## trading-partner Element



A trading partner is a business entity with authorization to send and receive business messages in a conversation.

## Syntax

```
<trading-partner
  name="tradingPartnerName"
  description="tradingPartnerDescription"
  notes="tradingPartnerNotes"
  status=" [enabled/ENABLED/disabled/DISABLED] "
  type=" [LOCAL/REMOTE] "
  is-default=" [true/false] "
  business-id-type="businessIdType"
  business-id="businessId"
  email="emailAddress"
  phone="phoneNumber"
  fax="faxNumber"
  username="username">
  <address>partnerAddress</address>
  <extended-property-set>
    .
    .
    .
  </extended-property-set>
```

```
<client-certificate>
.
.
.
</client-certificate>
<server-certificate>
.
.
.
</server-certificate>
<encryption-certificate>
.
.
.
</encryption-certificate>
<signature-certificate>
.
.
.
</signature-certificate>
<ebxml-binding>
.
.
.
</ebxml-binding>
<rosettanet-binding>
.
.
.
</rosettanet-binding>
<web-service-binding>
.
.
.
</web-service-binding>
</trading-partner>
```

## Attributes

Attribute		
<b>name</b>	<b>Description</b>	Name for the trading partner in the repository.
	<b>Allowable Values</b>	any
	<b>Use</b>	required
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>description</b>	<b>Description</b>	A short text description of the trading partner that appears in the WebLogic Integration Administration Console.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>notes</b>	<b>Description</b>	Text notes or documentation of the trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none

Attribute		
status	Description	A string that determines whether the trading partner is enabled to send and receive messages.
	Allowable Values	enabled ENABLED disabled DISABLED
	Use	optional
	Type	xs:NMTOKEN
	Default Value	ENABLED
type	Description	Specifies whether the trading partner resides locally within WebLogic Integration domain or at an external remote location.
	Allowable Values	LOCAL—the trading partner resides within the domain  REMOTE—the trading partner resides outside the domain
	Use	optional
	Type	xs:NMTOKEN
	Default Value	REMOTE

Attribute		
<b>is-default</b>	<b>Description</b>	<p>This setting indicates whether or not the trading partner is the default trading partner for sending and receiving messages for the local host system.</p> <p>This attribute can be set to true for trading partners with a <code>type</code> attribute of <code>LOCAL</code> only. Only one <code>LOCAL</code> <code>type</code> trading partner can have this value set to true.</p>
	<b>Allowable Values</b>	<p>false</p> <p>true</p>
	<b>Use</b>	optional
	<b>Type</b>	<code>xs:boolean</code>
	<b>Default Value</b>	false
<b>business-id-type</b>	<b>Description</b>	<p>Identifies the type for naming convention for the associated <code>business-id</code> attribute. For example, a trading partner that is registered with Dun and Bradstreet might use a value of "DUNS".</p>
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	<code>xs:string</code>
	<b>Default Value</b>	none
<b>business-id</b>	<b>Description</b>	<p>Uniquely identifies the trading partner in message exchanges according to the <code>business-id-type</code>.</p>
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	<code>xs:string</code>
	<b>Default Value</b>	none

<b>Attribute</b>		
<b>email</b>	<b>Description</b>	An email address for the trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>phone</b>	<b>Description</b>	A telephone number for the trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>fax</b>	<b>Description</b>	A fax telephone number for a trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none
<b>username</b>	<b>Description</b>	The username in the WebLogic Integration security configuration that represents the trading partner.
	<b>Allowable Values</b>	any
	<b>Use</b>	optional
	<b>Type</b>	xs:string
	<b>Default Value</b>	none

## References

### To

none

### From

[authentication Element](#)

[failure-notifier Element](#)

[failure-report-administrator Element](#)

[service-profile Element](#)

## Hierarchy

### Used By

[trading-partner-management Element](#)

### Children

[address Element](#)

[extended-property-set Element](#)

[client-certificate Element](#)

[server-certificate Element](#)

[encryption-certificate Element](#)

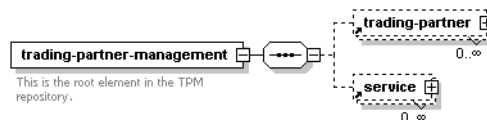
[signature-certificate Element](#)

[ebxml-binding Element](#)

[rosettanet-binding Element](#)

[web-service-binding Element](#)

## trading-partner-management Element



This element is the document root for TPM. It serves as the parent element for all the major elements in the TPM repository.

## Syntax

```
<trading-partner-management
  test-mode=" [true/false]"
  message-tracking-default=" [NONE/METADATA/ALL]"
  message-trace=" [true/false]"
  message-trace-directory="directoryLocation"
  secure-audit-logging=" [true/false]">
</trading-partner-management>
```

## Attributes

Attribute		
message-tracking-default	Description	The default global setting for the message tracking level. The message tracking attribute of the service-profile element overrides this attribute.
	Allowable Values	NONE—no tracking METADATA—tracking message metadata ALL—all message data
	Use	optional
	Type	xs:NMTOKEN
	Default Value	NONE



Attribute		
<b>message-trace</b>	<b>Description</b>	Toggles message tracing on and off.
	<b>Allowable Values</b>	false true
	<b>Use</b>	optional
	<b>Type</b>	xs:boolean
	<b>Default Value</b>	false
<b>message-trace-directory</b>	<b>Description</b>	The directory location where messages logs reside.
	<b>Allowable Values</b>	false true
	<b>Use</b>	optional
	<b>Type</b>	xs:boolean
	<b>Default Value</b>	none
<b>secure-audit-logging</b>	<b>Description</b>	Specifies whether signed messages reside in a secured audit log.
	<b>Allowable Values</b>	true, false
	<b>Use</b>	optional
	<b>Type</b>	xs:boolean
	<b>Default Value</b>	false

Attribute		
test-mode	Description	Specifies whether the repository is running in a test or production environment. In test-mode, you can send and recieve messages between collocated trading partners without using service profiles.
	Allowable Values	false true
	Use	optional
	Type	xs:boolean
	Default Value	true

## References

To  
none

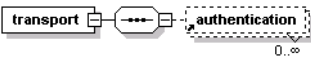
From  
none

## Hierarchy

Used By  
none

Children  
trading-partner Element  
service Element

## transport Element



This element specifies the transport level properties and receiving endpoint for a binding.

## Syntax

```
<transport
  protocol=" [http/HTTP/https/HTTPS/jms/JMS] "
  protocol-version=" [1.1/none] "
  endpoint="URL"
  timeout=" timeoutNo">
  <authentication
    .
    .
    .
  />
</transport>
```

## Attributes

Attribute		
protocol	Description	The protocol for sending and receiving messages. A value of JMS / jms is possible only when the transport is a child of the web-service-binding element.
	Allowable Values	http HTTP https HTTPS jms JMS
	Use	required
	Type	xs:NMTOKEN
	Default Value	none

Attribute		
protocol-version	Description	The version of the transport protocol.  This attribute is required for only HTTP/HTTPS protocols. The only supported version is 1.1.
	Allowable Values	"1.1" or no value
	Use	optional
	Type	xs:string
	Default Value	none
endpoint	Description	The URL of the transport endpoint
	Allowable Values	any
	Use	optional
	Type	xs:anyURI
	Default Value	none
timeout	Description	The period that the transport waits until indicating that the transport of a message failed.
	Allowable Values	time duration string
	Use	optional
	Type	xs:string
	Default Value	none

References

To  
none

From  
none

## Heirarchy

### Used By

[ebxml-binding Element](#)

[rosettanet-binding Element](#)

[web-service-binding Element](#)

### Children

[authentication Element](#)

## web-service-binding Element



This element and its child elements provide messaging properties such as transport endpoints, and authentication parameters for trading partners hosting or calling Web services.

## Syntax

```

<web-service-binding>
  <transport
    .
    .
    .
  />
</web-service-binding>
  
```

# Attributes

Attribute		
name	Description	The name for the binding in the TPM repository. A trading partner may have multiple <code>web-service-binding</code> elements, so the name must be unique to the parent <code>trading-partner</code> element.
	Allowable Values	any
	Use	required
	Type	xs:string
	Default Value	none

# References

To

none

From

[service-profile Element](#)

# Heirarchy

Used By

[trading-partner Element](#)

Children

[transport Element](#)

# xpath Element

This element defines an Xpath expression that may be one of a sequence of optional XML data transformations on a message that it is to be digitally signed. The message digest is computed after any transforms are performed on the message.

## Syntax

`<xpath>xpath-expression</xpath>`

## Attributes

none

## References

### To

none

### From

none

## Heirarchy

### Used By

[signature-transforms Element](#)

### Children

none





# Using the Bulk Loader

The Bulk Loader is a command line tool that you can use to import, export, and delete trading partner (TPM) data. This data includes trading partner profiles, certificates from keystores, service definitions, and service profiles. The Bulk Loader imports an XML representation of TPM data and it exports an XML file. Validation of the XML input documents is performed using the XSD schemas. The Bulk Loader uses an XML configuration file (`blconfig.xml`) to obtain parameters for connecting to the database and certificate keystores. If the Bulk Loader detects any errors during this procedure, it creates an error log.

The following sections provide information on using the Bulk Loader:

- [About Using the Bulk Loader](#)
- [Schemas](#)
- [Configuring the Bulk Loader Configuration File](#)
- [Using the Bulk Loader Command Line Options](#)
- [Importing and Exporting Management Data](#)
- [Deleting Management Data](#)

## About Using the Bulk Loader

The Bulk Loader command line tool should only be used when the WebLogic Integration server is *not* running. If the WebLogic Integration server is running, all configuration changes to TPM data in the database should be performed through the WebLogic Integration Administration

Console. The WebLogic Integration Administration Console also supports import, export, and bulk delete operations. Using the WebLogic Integration Administration Console for these operations ensures that the running servers in a WebLogic Integration domain have consistent TPM data in their internal TPM memory cache.

To learn about using the WebLogic Integration Administration Console to import, export, and delete management data, see the following:

- [Importing Management Data](#)
- [Exporting Management Data](#)
- [Deleting Trading Partner Profiles and Services Using Bulk Delete](#)

## Schemas

When importing and exporting repository data and trading partner configuration, two XSD schemas are used by the Bulk Loader to validate the imported or exported XML documents. The `TPM.xsd`, which specifies the trading partner information and the `BulkLoaderConfig.xsd`, which specifies database and keystore information and the transaction processing options. These schemas are based on the 2001 XML Schema Definition (XSD).

Both the `TPM.xsd` and `BulkLoaderConfig.xsd` schemas are in the `schema/src` directory inside the `wli.jar` file. These files are located in the following directory:

```
BEA_HOME/weblogic81/server/lib
```

In the preceding line, `BEA_HOME` represents the WebLogic Platform home directory.

To learn about the entities and elements that comprise trading partner management data in the `TPM.xsd` file, see [Appendix A, “TPM Schema.”](#)

To learn about setting up keystore information and the transaction processing options in the `BulkLoaderConfig.xsd`, see [“Transaction Processing Options” on page B-5](#) and [“Importing or Exporting Certificate Elements” on page B-6](#).

## Configuring the Bulk Loader Configuration File

The Bulk Loader uses an configuration file (`blconfig.xml`) to get parameters for connecting to the database and certificate keystores. Before using the Bulk Loader, you must modify this file to match your database installation.

The `blconfig.xml` configuration file is located in the following directory:

```
BEA_HOME\weblogic81\integration\bin
```

In the preceding line, *BEA\_HOME* represents the WebLogic Platform 8.1 home directory.

#### Listing B-1 blconfig.xml

---

```
<?xml version="1.0" encoding="UTF-8"?>
<bulkloader-config
  xmlns="http://www.bea.com/2003/03/wli/tpm/bulkloader"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.bea.com/2003/03/wli/tpm/bulkloader
BulkLoaderConfig.xsd">
  <database-info>
    <!-- Modify the following to match your database installation -->
    <url>jdbc:pointbase://localhost:9093/workshop</url>
    <driver>com.pointbase.jdbc.jdbcUniversalDriver</driver>
    <userid>weblogic</userid>
    <password>weblogic</password>
  </database-info>
  <encoding>UTF-8</encoding>
</bulkloader-config>
```

---

## Using the Bulk Loader Command Line Options

The Bulk Loader is located in the following directory:

```
BEA_HOME\weblogic81\integration\bin
```

In the preceding line *BEA\_HOME* represents the WebLogic Platform 8.1 home directory.

The Bulk Loader usage is as follows:

```
bulkloader [-verbose] [-config <blconfig.xml>] [-wlibc]
-import <data.xml>
-export <data.xml> [-select <selector.xml>]
-delete <selector.xml>
```

The following table summarizes the options for the Bulk Loader commands.

**Table B-1 Bulk Loader Commands**

Option	Description
<code>[-verbose]</code>	Optional. Use verbose mode to help you troubleshoot problems in your import, export, or delete process.
<code>[-config &lt;blconfig.xml&gt;]</code>	Optional. Use to designate an explicit configuration file. Default is <code>blconfig.xml</code> . If not using the default, specify the full path of the configuration file.
<code>[-wlibc]</code>	Optional. Use when you import and export an XML file for use by a trading partner using WebLogic Integration - Business Connect.
<code>-import &lt;data.xml&gt;</code>	Use to import data. Specify the full path of the TPM file you want to import.  To learn more about importing, see <a href="#">“Importing and Exporting Management Data” on page B-4</a> .
<code>-export &lt;data.xml&gt;</code> <code>[-select &lt;selector.xml&gt;]</code>	Use to export data. Specify the full path of the TPM file you want to export. The <code>-select</code> option specifies the selector file and <code>selector.xml</code> specifies the type of data to be exported. You can use the <code>selector.xml</code> file to export all or just selected Trading Partners. This file can also designate that all or selected Services for export. This file must conform to the <code>TPM.xsd</code> schema.  To learn more about exporting, see <a href="#">“Importing and Exporting Management Data” on page B-4</a> .
<code>-delete &lt;selector.xml&gt;</code>	Use to delete data. Specify the full path of the TPM file used for selecting the elements to be deleted.  Use <code>selector.xml</code> to specify the elements that you want to delete. This file must conform to the <code>TPM.xsd</code> schema.  To learn more about deleting, see <a href="#">“Deleting Management Data” on page B-10</a> .

## Importing and Exporting Management Data

You can import or export management information including certificate data using the Bulk Loader. The Bulk Loader imports an XML representation of the TPM data and it exports an XML file. Before importing or exporting certificates you need to modify the `blconfig.xml` file as

described in [“Importing or Exporting Certificate Elements” on page B-6](#). How to import and export trading partner information is described in the following topics:

- [Transaction Processing Options](#)
- [General Procedure for Importing and Exporting](#)
- [Importing or Exporting Certificate Elements](#)

## Transaction Processing Options

In case of errors or when working with large repositories, you can use two attributes contained in the `BulkLoaderConfig.xsd` schema to control transaction processing. These attributes are `transaction-level="all"` and `transaction-level="default"`. They are under the `<bulkloader-config>` root element. These options provide the same functionality available in the WebLogic Integration Administration Console.

The attribute `transaction-level="all"` performs the following:

- Imports the data in a single transaction. If invalid data is detected the entire transaction is rolled back.
- Exports all trading partner management entities.
- Deletes the data in a single transaction. If invalid data is detected the entire transaction is rolled back.

The attribute `transaction-level="default"` performs the following:

- Imports data using multiple transactions. The import initiates a transaction for each trading partner or service. If invalid data is detected during a transaction for any entity, the import is rolled back for the current transaction only; importing stops with the rolled back transaction.
- Exports the data specified in the `selector.xml` file. (This file must conform to the `TPM.xml` schema.)
- Deletes the data using multiple transactions. A delete transaction is initiated for each trading partner or service. If an error is encountered during the transaction for any entity, the transaction is rolled back; deleting stops with the rolled back transaction.

## General Procedure for Importing and Exporting

This section contains information about importing and exporting trading partner management data.

### To import or export trading partner management data:

Before importing or exporting a TPM file, make sure of the following is true:

- The TPM file conforms to the `TPM.xsd` schema.
  - When importing or exporting a file for use with WebLogic Integration - Business Connect, only a single trading partner profile is specified.
1. On a Windows system, open a command window.
  2. In both Windows and UNIX, go to the following directory:

```
BEA_HOME/weblogic81/integration/bin
```

In the preceding line, *BEA\_HOME* represents the WebLogic Platform home directory.

3. Execute the import or export by entering the appropriate commands:

```
bulkloader [-verbose] [-config <blconfig.xml>] [-wlibc]  
-import <data.xml>  
-export <data.xml> [-select <selector.xml>]
```

The following shows an example of importing a trading partner XML file that was exported from WebLogic Integration - Business Connect:

```
bulkloader -wlibc -import  
d:\tradingpartners\profiles\WorldWideTrading.xml
```

This example shows exporting services offered by a remote trading partner:

```
bulkloader -config myconfig.xml -export  
exports\NationalTradingServices.xml -select  
selectors\NationalTradingSelector.xml
```

## Importing or Exporting Certificate Elements

**Note:** Only the certificates for remote Trading Partners can be imported; local Trading Partners cannot be imported.

Importing and exporting of certificates, as with other trading partner profile information, is done in XML format. The XML representation of the certificates conforms to the certificate

representation format specified in the W3C XML-Signature Syntax and Processing recommendation, which is available at the following URL:

<http://www.w3.org/TR/xmlsig-core/#sec-KeyInfo>

The Bulk Loader only supports import or export of certificate data and public keys. The Private Key of certificates is not imported or exported; an administrator must manually perform the transfer of the Private Key. The keystore related information is read from the Bulk Loader configuration file (blconfig.xml).

**Note:** To learn more about the WebLogic Server Keystore, see “[WebLogic Keystore Provider-->General](#)” in the Administration Console Online Help.

When the input XML file has certificate elements for a trading partner with <ds:KeyInfo> sub-elements, the specified certificate-key data is added to the appropriate keystore as designated by the Bulk Loader configuration file.

The Bulk Loader configuration schema (BulkLoaderConfig.xsd) includes keystore configuration information. This is an optional element in the schema. The following extract is from the schema definition for the keystore-info element:

```
<xs:element name="keystore-info">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="path" type="xs:string"/>
      <xs:element name="password" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="encoding" type="xs:string"/>
```

Passwords for the database and keystore can be initially entered in the blconfig.xml file in clear text. After the operation successfully completes, the Bulk Loader encrypts the passwords and re-writes the blconfig.xml file with the encrypted form of the passwords.

The path element is the absolute file path to the Java KeyStore. The password element is the keystore password.

The following is an example of the Bulk Loader configuration file that includes keystore information.

---

#### **Listing B-2 blconfig.xml with Keystore Information**

```
<?xml version="1.0" encoding="UTF-8"?>
<bulkloader-config
```

## Using the Bulk Loader

```
xmlns="http://www.bea.com/2003/03/wli/tpm/bulkloader"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.bea.com/2003/03/wli/tpm/bulkloader
BulkLoaderConfig.xsd">
<database-info>
  <url>jdbc:pointbase://localhost:9094/WLIDB</url>
  <driver>com.pointbase.jdbc.jdbcUniversalDriver</driver>
  <userid>PBPUBLIC</userid>
  <password>PBPUBLIC</password>
</database-info>
<keystore-info>
  <path>D:\test\peer1KeyStore.pks</path>
  <password>peer1</password>
</keystore-info>
</bulkloader-config>
```

---

The following is an example of trading partner information with a client certificate in import-export format.

### Listing B-3 Trading Partner with Client Certificate

---

```
<trading-partner
  name="ebxml-sender"
  type="REMOTE"
  status="ENABLED">
  <client-certificate name="peer1-en">

<KeyInfo>
  <KeyName>1.2.840.113549.1.9.1=#160d7065657231406265612e636f6d,
    CN=localhost.peer1-en.crt,OU=ECI Division,O=BEA Systems,
    ST=California,C=US
  </KeyName>
  <KeyValue>
    <RSAKeyValue>
      <Modulus>t/kDK6Jezk2e31k2nMQMagPuXsC56df18YW0KRqQa89Q7o/
        H8O8m6LdOH5H0GyYEUBD+jN08lgZqCQMDAZCG6w==</Modulus>
```



```

        <Exponent>AQAB</Exponent>
    </RSAKeyValue>
</KeyValue>
<X509Data>
<X509SubjectName>1.2.840.113549.1.9.1=#160d7065657231406265612e6366fd,
    CN=localhost.peer1-en.crt,OU=ECI Division,O=BEA Systems,
    ST=California,C=US</X509SubjectName>
<X509IssuerSerial>
<X509IssuerName>1.2.840.113549.1.9.1=#1610676172696d656c73406265612e6366f6,
    CN=luke.bea.com,OU=WLC Luke,O=ECI Division\, BEA Systems Inc,
    L=San Jose,ST=California,C=US</X509IssuerName>
    <X509SerialNumber>DQ==</X509SerialNumber>
</X509IssuerSerial>
<X509Certificate>MIICQzCCAe2gAwIBAgIBDTANBgkqhkiG9w0BAQQFADCBqDELMAkGA1UEB
hMCMVVMxEzARBgNVBAGTCkNhbg1mb3JuaWEwETAPBgNVBACTCFZhbnB3N1lMSYwJAYDVQQKE1
FQ0kgRG12aXNpb24sIEJFQSBTeXN0ZW1zIEluYzERMA8GA1UECzMIV0xDIEEx1a2UxFTATBgNVB
AMTDGx1a2UuYmVhLmNvbTEfMB0GCSqGSIb3DQEJARYQZ2FyaW1lbHNAYmVhLmNvbTAeFw0wMjA
xMDEwMDAwMDBaFw0wMzAxMDEwMDAwMDBaMIGOMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fsa
WZvcms5pYTEUMBIGA1UEChMLQkVBIFN5c3RlbXMxFTATBgNVBAsTDDEVDSSEBaXZpc2l1b2JfEjMB0
GA1UEAxMwBg9jYXxob3N0LnBlZXIxLWVuLmNydDEcMBoGCSqGSIb3DQEJARYNcGV1c2FAYmVhL
mNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC3+QMrol7OTZ7fWTacxAxqA+5ewLnpl/XxhbQ
pGpBrz1Duj8fw7ybot04fkfQbJgRQEP6M3TyWBmoJAwMBkIbrAgMBAAGjGjAYMAkGA1UdEwQCM
AAwCwYDVR0PBAQDAGXgMA0GCSqGSIb3DQEBAUAA0EAA8QAs20bOFvebMd6mU6ui7lAYZd+5+d
OhTU0R03VgY35ZQXzyaOH7GtMHN0omFqKaRdckwAi75FZTuAfKVYJfw==</X509Certificate
>
    </X509Data>
</KeyInfo>

</client-certificate>
</trading-partner>

```

---

**Note:** The Bulk Loader also imports certificates from an WebLogic Integration - Business Connect export file and exports certificates in the format that Business Connect can consume.

## Deleting Management Data

The Bulk Loader provides the ability to bulk delete management data. The delete operation removes trading partners information based on an input selector file. It deletes each selected leaf element and all linked child elements associated with that element. For example, if you delete a particular Trading Partner from the repository, all child certificate, binding, transport, and authentication elements are also deleted.

### To delete management data using the Bulk Loader, take the following steps

1. Create an input file that specifies the data elements to be deleted from the repository, as shown in the following example.

#### **TpmDelete.xml**

```
<?xml version="1.0" encoding="UTF-8"?>
<trading-partner-management
  xmlns="http://www.bea.com/2003/03/wli/tpm"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.bea.com/2003/03/wli/tpm TPM.xsd">
  ... elements to be deleted are specified here in XML ...
</trading-partner-management>
```

2. On a Windows system, open a command window.
3. In both Windows and UNIX, go to the following directory:

*BEA\_HOME*/weblogic81/integration/bin

In the preceding line, *BEA\_HOME* represents the WebLogic Platform home directory.

4. Execute the bulk delete by entering:

```
bulkloader [-verbose] [-config <blconfig.xml>] [-wlibc] -delete
<selector.xml>
```

For a description of these options, see [Table B-1](#).

# Production Database

In preparation for running WebLogic Integration in production mode, database tables must be created manually. This section contains information about these procedures:

- [Creating the WebLogic Integration Tables](#)

## Creating the WebLogic Integration Tables

The database tables used by WebLogic BPM (business process management) can be found in the directory:

`BEA_HOME/weblogic81/integration/dbscripts/vendor/`

In this path, *BEA\_HOME* represents the WebLogic Platform home directory, and *vendor* represents the vendor of the database you will be using in production mode. In that directory are the SQL scripts you will need to create needed tables. The following table describes these scripts.

Script filename	Description
wli_archive.sql	SQL that creates tables involved in WebLogic Integration data archive activity.
wli_runtime.sql	SQL that creates tables involved in WebLogic Integration runtime activity.

Use your preferred SQL tool to run these scripts to create the WebLogic BPM tables in your production database.

## Production Database

After the tables have been created, you must use the bulkloader to initialize the tables. Refer to [Appendix B, “Using the Bulk Loader.”](#)