BEA WebLogic Integration™

Managing WebLogic Integration Solutions

Version 8.1 Service Pack 5
Revised: October 2005

Copyright

Restricted Rights Legend

Trademarks or Service Marks

Contents

4. Process Instance Monitoring

5. Message Broker

6. Event Generators

7. Worklist Administration

8. Application Integration

9. Trading Partner Management

10.System Configuration

11.User Management

12.Business Calendar Configuration

13.XML Cache

A. Configuring a Production Database

B. Querying WebLogic Integration Reporting Data

C. Accessing Process Graphs from HTTP Clients

D. Using the Trading Partner Bulk Loader

E. TPM Schema

CHAPTER 1

Managing WebLogic Integration Solutions: Tools and Tasks

This section provides an overview of the tools and tasks involved in managing WebLogic Integration™ solutions. The following topics are provided:

- WebLogic Integration Management Tools
- WebLogic Managed Beans
- WebLogic Integration Management Task Reference

Note: Throughout this section, the focus is on administrative tasks and tools that are specific to WebLogic Integration. For an introduction to WebLogic Platform™ administration, see *Introducing Administration in WebLogic Platform 8.1* at the following URL: http://edocs.bea.com/platform/docs81/admin/admin.html

WebLogic Integration Management Tools

The following tools are available to support WebLogic Integration administration:

- *WebLogic Configuration Wizard*

  A WebLogic Server® domain is a collection of WebLogic Server resources managed as a single unit. Every domain includes one and only one administration server; any other WebLogic Server instances in the domain are managed servers. The WebLogic Configuration Wizard can be used to assist you in creating and configuring domains to support the development and deployment of WebLogic Integration solutions. See "Creating or Extending Server Domains" on page 1-6 for a quick reference guide to the tasks and related documentation.

- *WebLogic Server Administration Console*
  The WebLogic Server Administration Console is a Web application hosted by the administration server in a domain. You access the console from any machine on the local network that can communicate with the administration server through a Web browser. The console allows administrators to perform WebLogic Server configuration and monitoring tasks without having to learn the JMX API or the underlying management architecture.

- WebLogic Integration Administration Console
  Like the WebLogic Server Administration Console, the WebLogic Integration Administration Console is a Web application hosted on the administration server. Once you have created a domain that supports WebLogic Integration, it is used to perform tasks that are specific to managing WebLogic Integration solutions. A list of all the tasks that can be performed from the console is provided in "Introducing the WebLogic Integration Administration Console" on page 2-1.

- *WebLogic Integration 8.1 SNMP Agent*
  This utility allows you to update key WebLogic Integration information using a standard SNMP Manager. You can obtain a package containing the agent software and the WebLogic Integration MIB from the dev2dev.com site at the following URL:

  http://dev2dev.com/resourcelibrary/utilitiestools/adminmgmt.jsp#snmp

  Instructions for installing and configuring the SNMP Agent and a description of the WebLogic Integration MIB items are included in the package.

- *WLShell*
  This utility provides simplified access to MBeans in WebLogic Server through a scripting language (see the following section, "WebLogic Managed Beans"). It provides a shell-like interface to MBeans in the active WebLogic domain and a GUI explorer for inspecting MBeans. Using WLShell, you can easily navigate the MBean hierarchy, view configuration and runtime properties, and execute operations such as get, set, invoke, mkdir, and rmdir. The script support includes loops and conditionals. To learn more about this freeware tool, visit http://www.wlshell.com. You can also obtain WLShell from the dev2dev.com site at the following URL:

  http://dev2dev.com/resourcelibrary/utilitiestools/adminmgmt.jsp#wlshell

- *Trading Partner Management Bulk Loader*
  This utility allows is a command line tool that allows you to import, export, and delete trading partner management (TPM) data. To learn more about this utility, see Appendix D, "Using the Trading Partner Bulk Loader."

In addition to the above, WebLogic Server provides a number of tools with which you should be familiar. See "System Administration Tools" in the Overview of WebLogic Server System Administration section of *Configuring and Managing WebLogic Server* at the following URL:

http://edocs.bea.com/wls/docs81/adminguide/overview.html

Note: Items or tools on http://dev2dev.com are listed for your convenience and are not supported by BEA Customer Support.

WebLogic Managed Beans

Resources within a domain use Java Management Extensions (JMX) Managed Beans (MBeans) to expose their management functions. An MBean is a concrete Java class that is developed per JMX specifications. It can provide getter and setter operations for each management attribute within a managed resource along with additional management operations that the resource makes available. MBeans that expose the configuration data of a managed resource are called *Configuration MBeans,* while MBeans that provide performance metrics and other information about the runtime state of a managed resource are called *Runtime MBeans*.

To learn more about WebLogic Server managed resources and MBeans, see Overview of WebLogic JMX Services in *Programming WebLogic Management Services with JMX* at the following URL:

http://edocs.bea.com/wls/docs81/jmx/overview.html

To learn more about the WebLogic Integration MBeans, refer to the following packages in the WebLogic Integration Javadoc:

- com.bea.wli.management.configuration
- com.bea.wli.management.runtime
- com.bea.wli.tpm.management.configuration
- com.bea.wli.tpm.management.runtime
- com.bea.wlai.management.deployment
- com.bea.wlai.management.runtime

Programmatically Accessing WebLogic Integration MBeans

The `weblogic.management.MBeanHome` interface is the most convenient way to access the JMX MBean Server that resides on each WebLogic Server in a domain. You can access the

Administration `MBeanHome` interface from the JNDI tree of the Administration Server as described in "Using JNDI to Retrieve an MBeanHome Interface" in Accessing WebLogic Server MBeans at the following URL:

http://edocs.bea.com/wls/docs81/jmx/basics.html

The following example shows how you can access the `ProcessRuntimeMBean` interface:

Listing 1-1 Programmatically Accessing ProcessRuntimeMBean

```
Environment env = new Environment();
env.setSecurityPrincipal("weblogic");
env.setSecurityCredentials("weblogic");
Context ctx = env.getInitialContext();
MBeanHome home = (MBeanHome)ctx.lookup(MBeanHome.ADMIN_JNDI_NAME);
System.out.println("Got the Server-specific MBeanHome: " + home);
Set s = home.getMBeansByType("ProcessRuntime");
Iterator it = s.iterator();

try    {
       while (it.hasNext()){
        ProcessRuntimeMBean bean = (ProcessRuntimeMBean)it.next();
        ProcessInstanceQuery query = new ProcessInstanceQuery();
        query.setServiceURI(context.getService().getURI());
        ProcessInstanceQueryResult info = bean.getProcessInstances(query);
        String[] instances = info.getInstanceIds();
        System.out.println(instances[0]);
        }
   } catch (Exception ex) {
       System.out.println(ex);
       ex.printStackTrace();
   }
```

WebLogic Integration Management Task Reference

This section provides references to the instructions and background information required to perform the most common WebLogic Integration administrative tasks:

- Creating or Extending Server Domains
- Managing Database Resources
- Deploying Integration Solutions
- Securing WebLogic Integration Resources
- Managing Process Types
- Monitoring Process Instances
- Monitoring Message Broker Channels
- Creating and Managing Event Generators
- Managing WebLogic Integration Tracking and Reporting Data
- Creating Business Calendars and Assigning them to Users or Groups
- Managing or Monitoring Worklist Tasks
- Managing Application Views and Adapters
- Managing Trading Partner Integration
- Managing XML Cache Instances

Although a majority of the tasks can be performed using the WebLogic Integration Administration Console, some must be performed using other tools, and in some cases, you must directly edit a configuration file. You can use this section as a roadmap to the task-specific information that can be found in the following resources:

Document Title	URL
This guide, *Managing WebLogic Integration Solutions*	http://edocs.bea.com/wli/docs81/manage/index.html
Deploying WebLogic Integration Solutions	http://edocs.bea.com/wli/docs81/deploy/index.html

Configuring and Managing WebLogic Server	http://e-docs.bea.com/wls/docs81/adminguide/index.html
Creating WebLogic Configurations Using the Configuration Wizard	http://edocs.bea.com/platform/docs81/confgwiz/index.html
Managing WebLogic Platform Database Resources	http://e-docs.bea.com/platform/docs81/db_mgmt/db_resource_mgmt.html
Security in WebLogic Platform 8.1	http://edocs.bea.com/platform/docs81/secintro/index.html
Introducing Trading Partner Integration	http://edocs.bea.com/wli/docs81/tpintro/index.html
Introducing Application Integration	http://edocs.bea.com/wli/docs81/aiover/index.html
Building Integration Applications in the WebLogic Workshop® Help	http://edocs.bea.com/workshop/docs81/doc/en/integration/navIntegration.html
Using the Worklist	http://edocs.bea.com/wli/docs81/worklist/index.html

Note: URLs are provided in the preceding table to assist those using a printed version of the documentation to locate the information referenced in the following sections. If you are viewing an HTML or PDF version of the documentation, the references in the following sections are active links.

Throughout this reference section, it is assumed that the WebLogic Integration Administration Console is to be used as the primary management tool. As described in "WebLogic Integration Management Tools" on page 1-1, alternative utilities, such as the SNMP Agent or WLShell, can be used to perform many tasks.

Creating or Extending Server Domains

A domain includes one or more instances of WebLogic Server and may include WebLogic Server clusters. WebLogic Integration is a collection of applications and resources—EJBs, Web applications, JDBC connection pools, and so on—that are deployed in a domain to provide a unified platform for developing and deploying comprehensive business integration solutions. A first step in the development or deployment of a WebLogic Integration solution is to create a suitable domain.

The following table provides a roadmap to the information you need to create or extend a development or production (running in "noniterativedev" mode) domain.

To . . .	Refer to . . .	The reference provides . . .
Create a basic single server or clustered domain	The following sections of *Creating WebLogic Configurations Using the Configuration Wizard:* • Overview of the WebLogic Configuration Wizard and Configuration Template Builder • Template Reference: Basic WebLogic Integration Domain • Template Reference: WebLogic Integration Extension Template • Tutorials: Using the Configuration Wizard • Creating a New WebLogic Domain • Configuring Managed Servers, Clusters, and Machines • Extending Domains • How Do I? . . . Creating XA Domains Using Configuration Templates	The overview provides general information about WebLogic Server domains and how to use the Configuration Wizard. The template reference sections provide information about the default WebLogic Integration templates provided by the Wizard. The remaining sections provide procedural information.
Prepare a production domain	The following sections of *Deploying WebLogic Integration Solutions*: • Introduction • Understanding WebLogic Integration Clusters • Configuring a Clustered Deployment Related tasks and references are provided in "Deploying Integration Solutions" on page 1-8 and "Securing WebLogic Integration Resources" on page 1-8.	The introduction describes key domain resources and deployment tasks. A discussion of the roles played by system administrators, deployment specialists, and database administrators is also provided. "Understanding WebLogic Integration Clusters" provides background and "Configuring a Clustered Deployment" provides step-by-step procedures.
Create the database tables required by WebLogic Integration	Appendix A, "Configuring a Production Database." Additional references are provided in the following section, "Managing Database Resources."	Describes the scripts provided to create the tables required by WebLogic Integration.

Managing Database Resources

For general information about managing database resources for WebLogic Platform, see *Managing WebLogic Platform Database Resources*.

For information about creating the tables required by WebLogic Integration, see Appendix A, "Configuring a Production Database."

Deploying Integration Solutions

For information about deploying an integration application from the Workshop environment (running in iterative development mode), see Building and Deploying WebLogic Integration Applications in *Building Integration Applications*.

For the background information and procedures required to configure a production environment and deploy integration solutions, see *Deploying WebLogic Integration Solutions*.

Securing WebLogic Integration Resources

Note: This section focuses on security tasks and references that are specific to WebLogic Integration. For an overview of WebLogic Platform security see *Security in WebLogic Platform 8.1*.

The following table provides a roadmap to the information you need to secure WebLogic Integration resources.

To . . .	Refer to . . .	The reference provides . . .
Verify security provider requirements	"Security Provider Requirements for User Management" on page 11-9	Requirements.
Manage users, groups, and roles	Chapter 11, "User Management"	Step-by-step procedures for adding, deleting, or updating users, groups, and roles.
Learn about users, groups, and roles in WebLogic Integration	"About WebLogic Integration Users, Groups, and Roles" on page 11-2	Brief overview.
	"Default Groups, Roles, and Security Policies" on page 11-3	Description of built in groups, roles, and security policies.

To . . .	Refer to . . .	The reference provides . . .
Configure the role required to invoke process operations	"Process Security Policies" on page 3-4.	WebLogic Integration Administration Console procedures.
Configure the roles required to subscribe or publish to message broker channels	"Setting Channel Security Policies" on page 5-8.	WebLogic Integration Administration Console procedures.
Configure the roles required to execute application view services or subscribe for events	"Managing Application Integration Security" on page 8-7	WebLogic Integration Administration Console procedures.
Configure the role authorized to create worklist tasks	"Configuring the Worklist Task Creation Role" on page 10-20	WebLogic Integration Administration Console procedures.
Manage the password store	The following sections of Chapter 10, "System Configuration." • "Password Aliases and the Password Store" on page 10-6 • "Adding Passwords to the Password Store" on page 10-16 • "Listing and Locating Password Aliases" on page 10-17 • "Changing the Password for a Password Alias" on page 10-18 • "Deleting Passwords from the Password Store" on page 10-19	WebLogic Integration Administration Console procedures.
Securing resources for trading partner integration	The following sections of *Introducing Trading Partner Integration*: • Trading Partner Integration Security • Example: ebXML Security Configuration • Example: RosettaNet Security Configuration	Trading partner security

Managing Process Types

Process types can be monitored from the WebLogic Integration Administration Console. For a description of the Process Configuration module, and step-by-step procedures for the various management tasks, see Chapter 3, "Process Configuration."

You can also access the graphical view of a process type from other HTTP clients. See Appendix C, "Accessing Process Graphs from HTTP Clients."

Monitoring Process Instances

Process instances are monitored from the WebLogic Integration Administration Console. For a description of the Process Instance Monitoring module, and step-by-step procedures for the various monitoring tasks, see Chapter 4, "Process Instance Monitoring."

You can also access the graphical view of a process instance from other HTTP clients. See Appendix C, "Accessing Process Graphs from HTTP Clients."

Monitoring Message Broker Channels

Message broker channels are monitored from the WebLogic Integration Administration Console. For a description of the Message Broker module, and step-by-step procedures for the monitoring tasks, see Chapter 5, "Message Broker."

Creating and Managing Event Generators

WebLogic Integration provides native event generators, including JMS, Email, File, and Timer event generators. These event generators are typically used to start a business process based on events, such as the receipt of email or a new file appearing in a directory. WebLogic Integration also works with Application View event generators, which work with J2EE-CA connectors.

The following table provides a roadmap to the information you need to manage event generators.

To . . .	Refer to . . .	The reference provides . . .
Learn about the JMS, Email, File, Timer, MQ Series, RDBMS, and HTTP event generators.	"About the Event Generators" on page 6-2	Introduction to the event generators (which publish messages to Message Broker channels in response to system events).
	"Message Broker Resources" and "Event Generator Resources" in Introduction in *Deploying WebLogic Integration Solutions*.	

To . . .	Refer to . . .	The reference provides . . .
Learn about the application integration event generators	"Events" section of "Application Integration Capabilities and Clients" in Introduction in *Deploying WebLogic Integration Solutions*.	Information about event processing in application integration.
	"Processing Event Notifications at Run-Time" in Understanding Application Integration in *Introducing Application Integration*	
	"Events" section of "Load Balancing Application Integration Functions in a Cluster" in *Deploying WebLogic Integration Solutions*.	
Create and deploy a File, Email, JMS, Timer, MQ Series, RDBMS, or HTTP event generator	"Creating and Deploying Event Generators" on page 6-14	WebLogic Integration Administration Console procedures.
	"Deploying Event Generators" in Understanding WebLogic Integration Clusters in *Deploying WebLogic Integration Solutions*.	Information about event generator targeting and error handling.
Manage the JMS, Email, File, Timer, MQ Series, RDBMS, or HTTP event generators	Chapter 6, "Event Generators"	Procedures for updating channel rules, or deleting suspending, or resuming an event generator.
Configure JMS event generators to consume the first element under the `<SOAP:Body>` element.	The description of the `wli.jmseg.EatSoapActionElement` element in wli-config.properties Configuration File in *Deploying WebLogic Integration Solutions.*	Configuration property description.

Managing WebLogic Integration Tracking and Reporting Data

The following table provides a roadmap to the information you need to manage WebLogic Integration tracking and reporting data.

To . . .	Refer to . . .	The reference provides . . .
Learn about the tracking data	• "Process Tracking Data" on page 10-3 • "Worklist Tracking Data" on page 10-4 • "Reporting and Purging Policies for Tracking Data" on page 10-5 • "Managing Process Tracking Data" on page 3-3	Descriptions of the tracking data available, the tracking levels that can be set, and the related management tasks, such as configuring a reporting database for offline storage or defining the schedule for purging the data from the runtime database.
Query the reporting data tables	• Appendix B, "Querying WebLogic Integration Reporting Data"	Descriptions of key tables and example queries.
Set the system-level policies for purging tracking data from the runtime database.	• "Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9 • "Configuring the Reporting Data and Purge Processes" on page 10-12 • "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-13	WebLogic Integration Administration Console procedures.
Configure the Reporting Data Datastore	"Configuring the Reporting Datastore" on page 10-13	WebLogic Integration Administration Console procedure.
Configure the tracking level for a process	"Viewing and Changing Process Details" on page 3-13	WebLogic Integration Administration Console procedure.
Configure the tracking level for business messages	"Configuring the Mode and Message Tracking" on page 9-10	WebLogic Integration Administration Console procedure.
Set the tracking level for worklist tasks	"Configuring the Default Tracking Level and Reporting Data Policy" on page 10-13	WebLogic Integration Administration Console procedure.

Creating Business Calendars and Assigning them to Users or Groups

Most of the management tasks associated with business calendars are completed from the WebLogic Integration Administration Console. For a description of the Business Calendar Configuration module, and step-by-step procedures for the various management tasks, see Chapter 12, "Business Calendar Configuration."

Managing or Monitoring Worklist Tasks

Most of the management tasks associated with the worklist can be completed from the WebLogic Integration Administration Console. For a description of the Worklist Administration module, and step-by-step procedures for the various management tasks, see "Worklist Administration" on page 7-1.

Custom worklist interfaces can also provide administrative and management functionality. Refer to Worklist User Interface and Enterprise JavaBeans API in *Using the Worklist*.

Detailed information regarding worklist operations is provided in the following sections of *Using the Worklist*.

- Introduction
- Creating and Managing Worklist Tasks

Managing Application Views and Adapters

Most of the application integration management tasks are completed from the WebLogic Integration Administration Console. For a description of the Application Integration module, and step-by-step procedures for the various management tasks, see Chapter 8, "Application Integration."

For background information, refer to the following sections of *Introducing Application Integration*:

- Introduction to Application Integration
- Understanding Application Integration
- Roles, Responsibilities, and Tasks

Managing Trading Partner Integration

Most of the trading partner integration management tasks are completed from the WebLogic Integration Administration Console. For a description of the Trading Partner Management module, and step-by-step procedures for the various management tasks, see Chapter 9, "Trading Partner Management."

You can also use the Bulk Loader command line utility to import and export trading partner management data. To learn more, see Appendix D, "Using the Trading Partner Bulk Loader.".

See "Securing WebLogic Integration Resources" on page 1-8 for additional references on securing trading partner integration applications.

Managing XML Cache Instances

The XML Cache stores XML metadata documents. When you are designing a business process, you use the XML Cache Control to retrieve the XML documents stored in the XML Cache. You use the XML Cache module to create and maintain the XML metadata documents stored in the XML Cache. For a description of the XML Cache module, and step-by-step procedures for the various management tasks, see Chapter 13, "XML Cache."

CHAPTER 2

Introducing the 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	Listing and Locating Process Types Listing and Locating Dynamic Controls Viewing and Changing Process Details Viewing an Interactive or Printable Process Type Graph Managing Process Versions 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
Process Instance Monitoring	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
Message Broker	Listing and Locating Channels Viewing Channel Details and Subscriptions Setting Channel Security Policies Viewing Global Message Counts Resetting the Message Counts
Event Generators	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 Defining Channel Rules for an MQ Series Event Generator Defining Channel Rules for an HTTP Event Generator Defining Channel Rules for a RDBMS 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

Module	Associated Tasks
Worklist Administration	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 State or Deleting Tasks Updating Task Comment, Owner, or Due Dates from the Summary Page Adding a Substitute Routing Rule Changing a Substitute Routing Rule Deleting a Substitute Routing Rule
Application Integration	Listing and Locating Application Views Listing and Locating Adapter Instances Viewing Application View Instance Statistics Viewing Adapter Instance Statistics Viewing Connection Factory Pool Statistics for a Service Connection Viewing Dependent Application Views for an Adapter Instance Viewing and Changing Application View Details 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 Adapter Instance 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 Enabling or Disabling Container-Managed Sign-On Updating Security Policies Suspending or Resuming an Application View or Adapter Instance Redeploying an Adapter Instance Resetting the Counters

Module	Associated Tasks
Trading Partner Management	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
System Configuration	Viewing the Configuration for Tracking, Reporting, and Purging Data Configuring the Reporting Data and Purge Processes Configuring the Reporting Datastore Configuring the Default Tracking Level and Reporting Data Policy Manually Starting and Stopping the 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 Configuring the Worklist Task Creation Role

Module	Associated Tasks
User Management	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
Business Calendar Configuration	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
XML Cache	Adding XML Documents to the XML Cache Updating an XML Document in the XML Cache Viewing the Code for an XML Document Deleting an XML Document from the XML Cache Viewing All XML Documents in the XML Cache

Starting the 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 11-3. 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.

CHAPTER 3

Process Configuration

The *Process Configuration* module allows you 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 reporting data policy.
- View or update the security policies for a process.
- Activate or deactivate a non-versioned 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 11-3.

The following topics are provided:

About Process Configuration

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

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.
- Transmitting 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
Default Tracking Level	Set the system default tracking level.	System Configuration. See "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12.
Tracking Level	Set or verify the tracking level for each process. The administrator can set the level for a process to: • **Default** (the system default tracking level) • **Full**, **Node**, **Minimum**, or **None** (setting overrides the system default tracking level)	Process Configuration. See "Viewing and Changing Process Details" on page 3-12.
Reporting Data Stream	Enable or disable the reporting data stream. If the reporting data stream is enabled, the specified reporting database is populated by a near real-time data stream.	System Configuration. See "Configuring the Reporting Data and Purge Processes" on page 10-11.
Purge Schedule	Enable or disable the purge process and set the regular intervals at which process runs to purge the data from the runtime database.	System Configuration. See "Configuring the Reporting Data and Purge Processes" on page 10-11.

Property	Configuration Task	Task Type and Reference
Purge Delay	Set the amount of time after completion or termination before the instance data is subject to purge by the purge process.	System Configuration. See "Configuring the Reporting Data and Purge Processes" on page 10-11.
Default Reporting Data Policy	Set the system default reporting data policy to **On** or **Off**.	System Configuration. See "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12.
Reporting Data Policy	Set or verify the reporting data policy for each process: • **On** indicates that the instance data is transmitted to the reporting database if the reporting data stream is enabled. If the reporting data stream is disabled, no processes data is transmitted, regardless of the policy set. • **Off** indicates that the instance data is not subject to transfer to the reporting database, even if the reporting data stream is enabled (that is, the data is only purged). • **Default** indicates that the system default reporting data policy (described below) is used.	Process Configuration. See "Viewing and Changing Process Details" on page 3-12

To learn more, see the following topics:

- "Process Tracking Data" on page 10-2.
- "Reporting and Purging Policies for Tracking Data" on page 10-4

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 identify 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 3-23.

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 3-12.

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 Business Processes
- 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 "Managing Process Versions" on page 3-20.

Note: Processes that are not versioned can also be enabled and disabled. See "Viewing and Changing Process Details" on page 3-12. A process, whether versioned or not, is only executable if the **Is Enabled** property is set to true, and the current time is later than the **Activation Date** and earlier than the **Deactivation Date**.

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 help topics associated with each are provided.

Page	Associated Tasks	Help Topics
Process Types		
Process Property Summary	View a list of process types. Display name, public URI, state (stateful or stateless), tracking level, reporting data policy, and SLA are displayed.	"Listing and Locating Process Types" on page 3-10
	Access the Process Type Details page.	
Process Type Details	View process properties. Identifying information (such as service URI and application name), configurable properties (display name, tracking level, reporting data policy, SLA), dynamic client callback properties, execution and authorization policies, variables, and active version are displayed.	"Viewing and Changing Process Details" on page 3-12
	Access an interactive or printable graph of the process.	"Viewing an Interactive or Printable Process Type Graph" on page 3-18
	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 display name, SLA, SLA warning threshold, tracking level, and reporting data policy for the selected process type.	"Viewing and Changing Process Details" on page 3-12
Edit Process Versioning	Enable, disable, or set the activation date and time for the selected version.	"Managing Process Versions" on page 3-20

Page	Associated Tasks	Help Topics
Add New Client Callback Properties	Add a selector value and properties, which can be used to dynamically configure the callback to the client.	"Adding or Changing Dynamic Client Callback Selectors" on page 3-21
Edit Client Callback Properties	Edit the properties used to dynamically configure the callback to the client.	"Adding or Changing Dynamic Client Callback Selectors" on page 3-21
Edit Process Execution Policy	Specify the **run as** identity for the process operations, and whether or not a single principal is required.	"Updating Security Policies" on page 3-23 "Process Security Policies" on page 3-4
Edit Process Authorization Policy	Set the minimum authorized roles for the methods (client requests) in the process.	"Updating Security Policies" on page 3-23 "Process Security Policies" on page 3-4
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.)	"Updating Security Policies" on page 3-23 "Process Security Policies" on page 3-4
Edit Call Back Authorization Policy	Set the authorized roles for the selected callback.	"Updating Security Policies" on page 3-23 "Process Security Policies" on page 3-4
Dynamic Controls		
View Dynamic Control Properties	View a list of dynamic controls. Control name, type, and selector value are displayed.	"Listing and Locating Dynamic Controls" on page 3-11
	Delete a selector from the control.	"Deleting Dynamic Control Selectors" on page 3-29
	Access the Add New or Edit page for the control to define properties for a new selector, or edit properties for an existing selector.	"Adding or Changing Dynamic Control Selectors" on page 3-25

Page	Associated Tasks	Help Topics
Add New Process Control Selector	Define the properties for a new selector.	"Defining Process Control Properties for a Selector" on page 3-25
Edit Process Control Selector	Update the properties for an existing selector.	"Defining Process Control Properties for a Selector" on page 3-25
Add New Service Broker Control Selector	Define the properties for a new selector.	"Defining Service Broker Control Properties for a Selector" on page 3-26
Edit Service Broker Control Selector	Update the properties for an existing selector.	"Defining Service Broker Control Properties for a Selector" on page 3-26

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 3-12.

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

Property	Description
Display Name	Display name assigned to the process. The name is a link to the **Process Type Details** page. **Note:** 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.
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 (**Stateful** or **Stateless**).
Tracking Level	The tracking level set for the process.

Property	Description
Reporting Data Policy	The reporting data 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 to locate a specific process type. 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.

Related Topics

- "Viewing and Changing Process Details" on page 3-12
- "Updating Security Policies" on page 3-23
- "Adding or Changing Dynamic Control Selectors" on page 3-25

Listing and Locating Dynamic Controls

The **View Dynamic Control Properties** page displays the dynamic controls (Process and Service Broker controls) referenced by deployed processes. For each control, the selector values for any dynamic bindings are displayed. To learn how to add or change control selectors, see "Adding or Changing Dynamic Control Selectors" on page 3-25.

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.

Related Topics

- "Dynamic Controls" on page 3-7
- "Adding or Changing Dynamic Control Selectors" on page 3-25

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 3-10.
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** 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 "Managing Process Versions" on page 3-20.
5. To configure dynamic client callback properties, see "Adding or Changing Dynamic Client Callback Selectors" on page 3-21.
6. To update the execution policy, process authorization policy, or method authorization policy, see "Updating Security Policies" on page 3-23.

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 (**Stateful** or **Stateless**.) To learn more about how stateful and stateless processes are created, see Building Stateless and Stateful Business Processes in *Building Integration Applications* in the WebLogic Workshop Help.	No
Description	User-friendly description of the process.	No
Version Group URI	For versioned processes, the URI for the version group.	No
Process Graph	Links to an interactive or printable view of the process. See "Viewing an Interactive or Printable Process Type Graph" on page 3-18.	No
Configurable Properties		
Display name	Display name assigned to the process. **Note:** 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.	Yes

Property	Description		Administrator Can Set (Yes/No)
Tracking Level	The tracking level set for the process. 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 executed node (a start node event and an end or abort node event).		Yes
	Full	Global events, node transitions, and data are tracked.	
	Node	Global events and node transitions are tracked.	
	Minimum	Global events, such as start process, end process, suspend, and resume, are tracked.	
	Default	Tracking level is set to the current system-wide setting (Full, Node, Minimum, or None). See "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12.	
	None	No events or data are tracked.	
Reporting Data Policy	The reporting data policy set for tracking data.		Yes
	On	Reporting data is enabled. The tracking data available for this process is transmitted to an offline database.	
	Off	Reporting data is disabled for this process.	
	Default	The reporting data policy is set to the system default reporting data policy. See "Reporting and Purging Policies for Tracking Data" on page 10-4.	

Property	Description		Administrator Can Set (Yes/No)
Save Process Variable Values on Completion	The process variable values policy set for tracking variables.		Yes
	On	Process variable tracking is enabled. After process completion, the variable values available for this process are stored in the run-time database. The process variable values are archived in the archive database as two new event types: one each for variable summary and for variable detail. For information about how to access archived data, see http://e-docs.bea.com/wli/docs81/manage/archive.html	
	Off	Process variable tracking is disabled.	
	Default	The process variable tracking policy is set to the system default policy. See "Reporting and Purging Policies for Tracking Data" on page 10-4.	
SLA	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. 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. To learn more about the SLA, see "Service Level Agreements" on page 3-5.		Yes
SLA Warning Threshold	A percent of the total SLA time. When this threshold has been reached, a warning flag is displayed for the process instance.		Yes
Is Enabled	For non-versioned processes, indicates whether the process is enabled (**true**) or disabled (**false**). For versioned processes, see the **Version Group** section.		Yes
Activation Time	For non-versioned processes, the date and time the process became, or is to become, active.		Yes
Deactivation Time	For non-versioned processes, the date and time the process is to become inactive.		Yes
Dynamic Client Callback Properties			

Property	Description		Administrator Can Set (Yes/No)
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.	
Version Group			
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 (**true**) or disabled (**false**).	Yes
	Activation Date	Date and time the process version became, or is to become, active.	Yes
	Deactivation Date	Date and time the process version is to become inactive.	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 "Managing Process Versions" on page 3-20.	

Property	Description		Administrator Can Set (Yes/No)
Security Policies			
Execution Policy	Run As	The identity the operations in the process assume while executing. Options are **caller's identity** or **start user**.	Yes
	Single Principal Required	**Yes** or **No**. If set to **Yes**, 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
Variables			
Variables	Name and declared type for each variable defined.		No

Related Topics

- "Viewing an Interactive or Printable Process Instance Graph" on page 4-17
- "Updating Security Policies" on page 3-23
- "Adding or Changing Dynamic Control Selectors" on page 3-25

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 4-17.

Note: The interactive process graph requires Adobe SVG Viewer Version 3.0. To learn more, see "Requirements for the Interactive Graph" on page 4-3. The printable graph requires a PDF viewer such as Adobe Acrobat.

To view a printable graph for a process type:

Note: You must have Adobe Acrobat Reader installed to view the printable graph.

1. Locate the process to view. See "Listing and Locating Process Types" on page 3-10.
2. Click the process name to display the **Process Type Details** page.
3. Click **Printable View**.

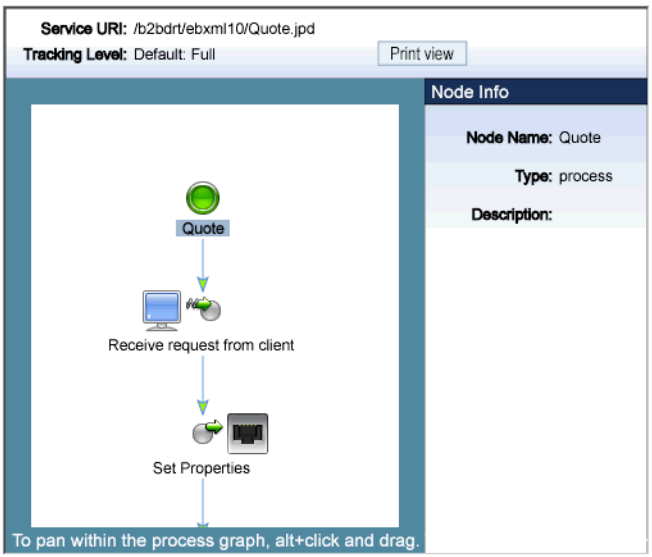
   The process graph is displayed as a PDF document.

To view the interactive graph for a process type:

1. Verify that your browser meets the requirements. See "Requirements for the Interactive Graph" on page 4-3.
2. Locate the process to view. See "Listing and Locating Process Types" on page 3-10.
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.

Related Topics

- "Requirements for the Interactive Graph" on page 4-3

- "Viewing an Interactive or Printable Process Instance Graph" on page 4-17

Managing Process Versions

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

Note: If you are running with `noiterativedev`, running instances will not be terminated when you redeploy an EAR. In production it is recommended that you use the following flags when starting WebLogic Server:

```
production noiterativedev nodebug notestconsole
```

See "Run-Time Tuning Issues" in the Performance Tips section of the *WebLogic Integration Solutions Best Practices FAQ*.

To enable, disable, or activate a version:

1. Locate the process to view. See "Listing and Locating Process Types" on page 3-10.
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.

   The **Edit Process Versioning** page is displayed.
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 **Is Enabled** check box.
   - To enable the version, check the **Is 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.

Related Topics

- "Process Versions" on page 3-6
- "Viewing and Changing Process Details" on page 3-12

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 Type 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 3-10.
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:
   - To add a new selector, click the **Add a new callback property** link.

     The **Add New Client Callback Properties** page is displayed.
   - 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 **Selector Value** field, enter the look up key.	The value used to select and dynamically set control attributes at runtime. **Note:** This field cannot be edited on the **Edit Client Callback Properties** page.	Required
Select the **No Dynamic Authentication**, **Basic Authentication,** or **Certificate Based Authentication** option button.	Type of authentication.	Optional
In the **User Name** field, enter the user name.	If **Basic Authentication** is selected, the required user name.	Required if **Basic Authentication** is selected.
In the **Password Alias** field, enter the password alias.	The password alias used to look up the user password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Client Certificate Alias** field, enter the certificate alias.	Certificate alias for **Certificate Based Authentication**.	Required if **Certificate Based Authentication** is selected.
In the **Client Certificate Password Alias** field, enter the password alias.	Password alias to look up the certificate password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Keystore Location** field, enter the keystore location.	The keystore location.	
In the **Keystore Password Alias** field, enter the password alias.	The password alias used to look up the keystore password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Keystore Type** 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 3-10.
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.

Related Topics

- "Viewing and Changing Process Details" on page 3-12

Updating Security Policies

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

Note: If an authenticator that implements the required MBeans is not configured, the options for configuring the process, method, and callback authorization policies are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

To set security policies:

1. Locate the process to view. See "Listing and Locating Process Types" on page 3-10.
2. Click the process name to display the **Process Type Details** page.
3. To configure the execution policy for the process:
   a. In the **Execution Policy** section, click **Configure**.

      The **Edit Process Execution Policy** page is displayed.

   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, in the **Process Authorization Policy** section, click **Configure**.

     The **Edit Process Authorization Policy** page is displayed.

     Note: If no roles are specified, everyone is authorized.
   - To configure the authorization policy for a method, click the **Configure** link for the method.

     The **Edit Process Method Authorization Policy** page is displayed.

     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.

     The **Edit Callback Authorization Policy** page is displayed.
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**.

Related Topics

- "Process Security Policies" on page 3-4
- "Viewing and Changing Process Details" on page 3-12

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 3-11.
2. Do one of the following:
   - Select the **Add Selector** link.
   - 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 3-25
   - "Defining Service Broker Control Properties for a Selector" on page 3-26
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

Note: The (Dynamic) Selector has now been deprecated. Please use the XML MetaData Cache Control to look up WebLogic Integration Administration Console configured values and then use the `setProperties()` calls of the Process Control to set the endpoint at

runtime. For more information on the XML MetaData Cache Control, see XML MetaData Cache Control in *Using Integration Controls* in the WebLogic Workshop Help, and for more information on the Process Control, see Process Control in *Using Integration Controls* in the WebLogic Workshop Help. For more information on the WebLogic Integration Administration Console, see *Managing WebLogic Integration Solutions*.

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 **Selector Value** field, enter the look up key.	The value used to select and dynamically set control attributes at runtime. **Note:** This field cannot be edited on the **Edit Process Control Selector** page.	Required to Add
In the **Target URI** field, enter the URI for the target process.	The URI for the target process associated with this look up key.	Optional
In the **User Name** field, enter the user name.	The user name (if required) used to invoke the target process.	Optional
In the **Password Alias** field, enter the password alias.	The password alias used to look up the user password in the password store. See "Password Aliases and the Password Store" on page 10-6.	Optional

Related Topics

- "Dynamic Controls" on page 3-7
- "Adding or Changing Dynamic Control Selectors" on page 3-25

Defining Service Broker Control Properties for a Selector

Note: The (Dynamic) Selector has now been deprecated. Please use the XML MetaData Cache Control to look up WebLogic Integration Administration Console configured values and then use the `setProperties()` calls of the Service Broker Control to set the endpoint at

runtime. For more information on the XML MetaData Cache Control, see XML MetaData Cache Control in *Using Integration Controls* in the WebLogic Workshop Help, and for more information on the Service Broker Control see, Service Broker Control in *Using Integration Controls* in the WebLogic Workshop Help. For more information on the WebLogic Integration Administration Console, see *Managing WebLogic Integration Solutions*.

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 **Selector Value** field, enter the look up key.	The value used to select and dynamically set control attributes at runtime. **Note:** This field cannot be edited on the **Edit Service Broker Selector** page.	Required
In the **End Point** field, enter the URI for the target service.	The URI for the service end point associated with this look up key.	Optional
From the **Protocol** drop-down list, select the protocol.	Protocol to use when making the call. Valid values are **http-soap** **http-xml** **jms-soap** **jms-xml** **form-get** **form-post** The default is **http-soap**. **Note:** The WebLogic Integration Administration Console allows you to specify any of the above values, therefore, you must take care to select a protocol that is supported by the process. For example, raw XML (non-SOAP) protocols do not work with conversational web services.	Optional

Setting	Description	Required/ Optional
Select the **No Dynamic Authentication**, **Basic Authentication,** or **Certificate Based Authorization** option button.	Type of authentication. If client certificates are required, select **Certificate Based Authorization** and enter values in the **Keystore Location**, **Keystore Password Alias**, and **Keystore Type** fields.	Optional
In the **User Name** field, enter the user name.	The user name (if required) used to invoke the target process.	Required if **Basic Authentication** is selected.
In the **Password Alias** field, enter the password alias.	The password alias used to look up the user password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Client Certificate Alias** field, enter the certificate alias.	Certificate alias if the remote service requires SSL with two-way authentication or a digital signature.	Required if **Certificate Based Authorization** is selected.
In the **Client Certificate Password Alias** field, enter the password alias.	Password alias to look up the certificate password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Keystore Location** field, enter the keystore location.	The keystore location.	Required if **Certificate Based Authorization** is selected.
In the **Keystore Password Alias** field, enter the password alias.	The password alias used to look up the keystore password in the password store. See "Password Aliases and the Password Store" on page 10-6.	
In the **Keystore Type** field, enter the keystore type.	The keystore type.	

Related Topics

- "Dynamic Controls" on page 3-7
- "Adding or Changing Dynamic Control Selectors" on page 3-25

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 3-11.
2. Click the **Delete** link to the left of the selector value to be deleted.

   The selector is deleted from the list.

CHAPTER 4

Process Instance Monitoring

The *Process Instance Monitoring* module allows you 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 11-3.

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 type of data available. To learn more about how tracking data is managed, see "Managing Process Tracking Data" on page 3-3.

The following topics are provided:

- 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 help topics associated with each are provided.

Page	Associated Tasks	Help 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.	"Viewing Instance Statistics by Process Type" on page 4-6
	Filter the list by URI or display name. Use ? to match any single character or * to match zero or more characters.	
Process Instance Summary	View a list of process instances. Instance ID, display name, process label, start time, elapse time, and status (running, completed, frozen, aborted, suspended) are displayed.	"Listing and Locating Process Instances" on page 4-7
	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.	"Suspending, Resuming, Terminating, or Unfreezing Process Instances" on page 4-19

Page	Associated Tasks	Help Topics
Advanced Search	Construct an advanced search using process properties such as status, time started or completed, elapsed time, or SLA status.	"Constructing an Advanced Search" on page 4-10
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.	"Viewing System Health Statistics" on page 4-7
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.	"Viewing Process Instance Details" on page 4-12
	Suspend, Resume, Terminate, or Unfreeze the process instance.	"Suspending, Resuming, Terminating, or Unfreezing Process Instances" on page 4-19
	Access an interactive or printable process graph.	"Viewing an Interactive or Printable Process Instance Graph" on page 4-17

Requirements for the Interactive Graph

To view the interactive process graph, Adobe SVG Viewer must be installed on the client system. If the server is running on Solaris, verify that your operating environment is set up to support this feature. The following section provides the information you need:

- Obtaining the SVG Viewer
- Using Adobe SVG Viewer with Netscape 7.0 on Windows
- Server Operating Environment Requirements for Solaris

Obtaining the SVG Viewer

The interactive process graph requires Adobe SVG Viewer Version 3.0x. 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://e-docs.bea.com/platform/suppconfigs/index.html

Note: If you are running in an English locale (for example, `en_US` or `en_AU`), and need to view processes that contain non-latin characters, we recommend that you install the Arial Unicode MS font. To learn more, see http://support.microsoft.com/kb/q287247/

Browser	Operating System	Adobe SVG Viewer 3.0x Availability
Microsoft Internet Explorer 6.x	Windows	Viewer is available from Adobe.
Netscape 7.0x	Windows	Requires a workaround. See "Using Adobe SVG Viewer with Netscape 7.0 on Windows."
	Solaris	3.0 beta 1 version of viewer available from http://www.adobe.com/svg/viewer/install/main.html
	Linux	3.0 beta 1 version of viewer available from http://www.adobe.com/svg/viewer/install/main.html
	HP-UX	Viewer is not available from Adobe.
	AIX	Viewer is not available from Adobe.
Netscape 7.1	Any	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`.

Server Operating Environment Requirements for Solaris

Like many Java platform applications in the Solaris operating environment, the ability to serve up an Interactive Process Graph is dependent on the presence of one of the following:

- X server and hardware graphics adapter.
- Xvfb "virtual frame buffer" X server, which allows applications to render in the main memory of the computer instead of the hardware graphics adapter.
- Xsun, the X display server.

If the server is in an environment where there is no guarantee of an X server running, you will need to install either Xvfb or Xsun to support client access to interactive process graphs.

For a discussion of the issues and instructions, see "Seeing Up Solaris 7, 8, and 9 Operating Environments for Java Servlet Graphics" at
http://developers.sun.com/solaris/articles/solaris_graphics.html

Note: Headless operation doesn't allow the use of Java Foundation Classes (Swing), and therefore does not address the issues.

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.

Note: For stateless processes, N/A is displayed in the running instances column. These processes start and end in a single transaction.

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 4-7.

Related Topics

- "Reporting and Purging Policies for Tracking Data" on page 10-4
- "Viewing Process Instance Details" on page 4-12
- "Service Level Agreements" on page 3-5

Viewing System Health Statistics

The **System Health** page provides an overview of system health by identifying processes that may be experiences problems.

The following indicators are displayed:

- *Highest Average Elapsed Time*
  The process name and average elapsed time for processes with the highest average elapsed time are displayed.
- *Worst SLA Performance*
  The process name and rate for processes with the worst SLA performance are displayed. Both the percentage of instances that exceeded the SLA, and a ratio of the instances that exceeded SLA to the total number of instances, are displayed in the rate column.
- *Lowest Success Rate*
  The process name and rate for processes with the lowest success rate are displayed. Both the percentage of instances that failed, and a ratio of the instances that failed to the total number of instances, are displayed in the rate column.

For each of the above, the data displayed is divided into the following categories:

- Since Last Purge
- Last 24 Hours
- Active instances (not applicable to lowest success rate).

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

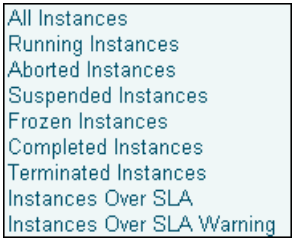
The **Process Instance Summary** page displays the following information for each process instance. For a more detailed description of the properties, see "Viewing Process Instance Details" on page 4-12.

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 "Viewing Process Instance Details" on page 4-12.
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 JpdContext Interface in *Building Integration Applications* in the WebLogic Workshop help.
Start Time	Time this instance started.
Elapsed Time	Time elapsed since instance start. The units reported depend on the duration. • From 0 to 99 msecs, duration is reported in milliseconds. For example, **28 msecs**. • From 99 msecs to one hour, duration is reported to the second. For example, **56 m 48.2 sec**. • From one hour to one week, duration is reported to the minute. For example, **2 d 2 h 6 m**. • From one week to one month, duration is reported to the hour. For example, **25 d 3.5 h**. • Greater than one month, duration is reported to the day. For example, **67 d**.
Status	The current state of the instance (Running, Completed, Suspended, Terminated, Frozen, Aborted). **Note:** Because stateless processes start and finish in a single transaction, these processes are never in the running state.

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**.
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:

   - 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 4-10.

Related Topics

- "Viewing Process Instance Details" on page 4-12
- "Suspending, Resuming, Terminating, or Unfreezing Process Instances" on page 4-19
- "Reporting and Purging Policies for Tracking Data" on page 10-4

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 **Service URI** drop-down list, select the Service URI.	Select from a list of the process types deployed. The default is **any**.
From the **Status** drop-down list, select a the status.	Specify the process status. The options are as follows:  The default is **any**.
In the **Started ...** section, select the **Anytime**, **After**, or **Before** option button. If you selected **After** or **Before**, use the corresponding drop-down lists to specify a time.	Specify the target range for process instance start time.
In the **Completed ...** section, select the **Anytime**, **After**, or **Before** option button. If you selected **After** or **Before**, use the corresponding drop-down list to specify a time.	Specify the target range for process instance completion time.
In the **Elapsed Time** section, specify the **Any**, **More Than**, or **Less Than** option button. If you selected **More Than** or **Less Than**, use the corresponding drop-down lists to specify the time period.	Specify the target time period for process instance elapsed time.

Setting	Description
Select the appropriate **SLA Status** option button.	Specify one of the following options: **Any** **Exceeded SLA** **Exceeded SLA or SLA Warning Threshold** **Exceeded SLA Warning Threshold, but not SLA**
In the **Label Contains** 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. **Note:** This is a containment query. Do not use wildcards.

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 instance.
- Navigate to a parent or child process instance.

Note: If **No Data** is displayed, the process instance details are not available. Either the data is not being captured at the tracking level configured for the process, or the information has been purged. It is possible for an instance ID to be displayed even though the associated instance data has been purged. For example, although the data for an instance may be purged after the instance has completed, the instance ID can remain in the runtime database because it is included as part of the tracking data associated with any parent or child instances that have not yet been purged.

To view process instance details:

1. Locate the process. See "Listing and Locating Process Instances" on page 4-7.
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 "Requirements for the Interactive Graph" on page 4-3. To learn more about the interactive process view, see "Viewing an Interactive or Printable Process Instance Graph" on page 4-17.

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.	
	Running	The process is running. **Note:** Because stateless processes start and finish in a single transaction, these processes are never in the running state.
	Completed	The process finished.
	Suspended	The process was suspended.
	Terminated	The process was terminated.
	Aborted	The process threw an unhandled exception. Aborted processes can only be terminated.
	Frozen	The process failed but can be unfrozen. When a process is unfrozen, it resumes from the point where it failed. See "Suspending, Resuming, Terminating, or Unfreezing Process Instances" on page 4-19. 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 Designing Your Application in *Building Integration Applications*.
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 JpdContext Interface in *Building Integration Applications* in the WebLogic Workshop help.	
SLA Status	If no service level agreements are set, Not Applicable is displayed. If service level agreements are set, this field displays the current status: • If the elapsed time does not exceed the SLA, Not exceeded is displayed. • If the elapsed time exceeds the SLA Warning threshold, the time remaining until the SLA threshold is reached is displayed. • If the elapsed time exceeds the SLA, the time elapsed time since the SLA was reached is displayed. To learn more about the SLA, see "Service Level Agreements" on page 3-5.	
Start Time	Time this instance started.	
Exception	Exception content for a aborted or frozen instance.	

Property	Description
Elapsed Time	Time elapsed since instance start. The units reported depend on the duration. • From 0 to 99 msecs, duration is reported in milliseconds. For example, **28 msecs**. • From 99 msecs to one hour, duration is reported to the second. For example, **56 m 48.2 sec**. • From one hour to one week, duration is reported to the minute. For example, **2 d 2 h 6 m**. • From one week to one month, duration is reported to the hour. For example, **25 d 3.5 h**. • Greater than one month, duration is reported to the day. For example, **67 d**.
Completion Time	Completion date and time for a completed process.
Termination Time	Termination date and time for a process that has been terminated.
Pending Activities	Pending `controlReceive` or `clientRequest` methods. For example: • `waitClientRequest[conditionalWaitClientRequest]` is displayed when the instance is waiting for the following: `<clientRequest name="conditionalWaitClientRequest" method="waitClientRequest" />` • `t1_onTimeout` is displayed when the instance is waiting for the following: `<controlReceive method="t1_onTimeout" />`
Parent Instance	Parent process instance ID, display name, status, start time, and elapsed time for the parent instance is displayed. The instance ID is a link to the **Process Instance Details** page for the instance. To learn more, see "Parent-Child Navigation" on page 4-15. **Note:** The parent or child instance is only displayed if the tracking level for the process is **Minimum**, **Node**, or **Full**.
Child Processes	An entry for each child instance. The instance ID, display name, status, start time, and elapsed time is displayed for each. The instance ID is a link to the **Process Instance Details** page for that process.
Tasks created by this instance	Worklist tasks created by the instance. The task name and ID are displayed. The ID is a link to the **Worklist Task Details** page.
Tasks this instance is listening to	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.

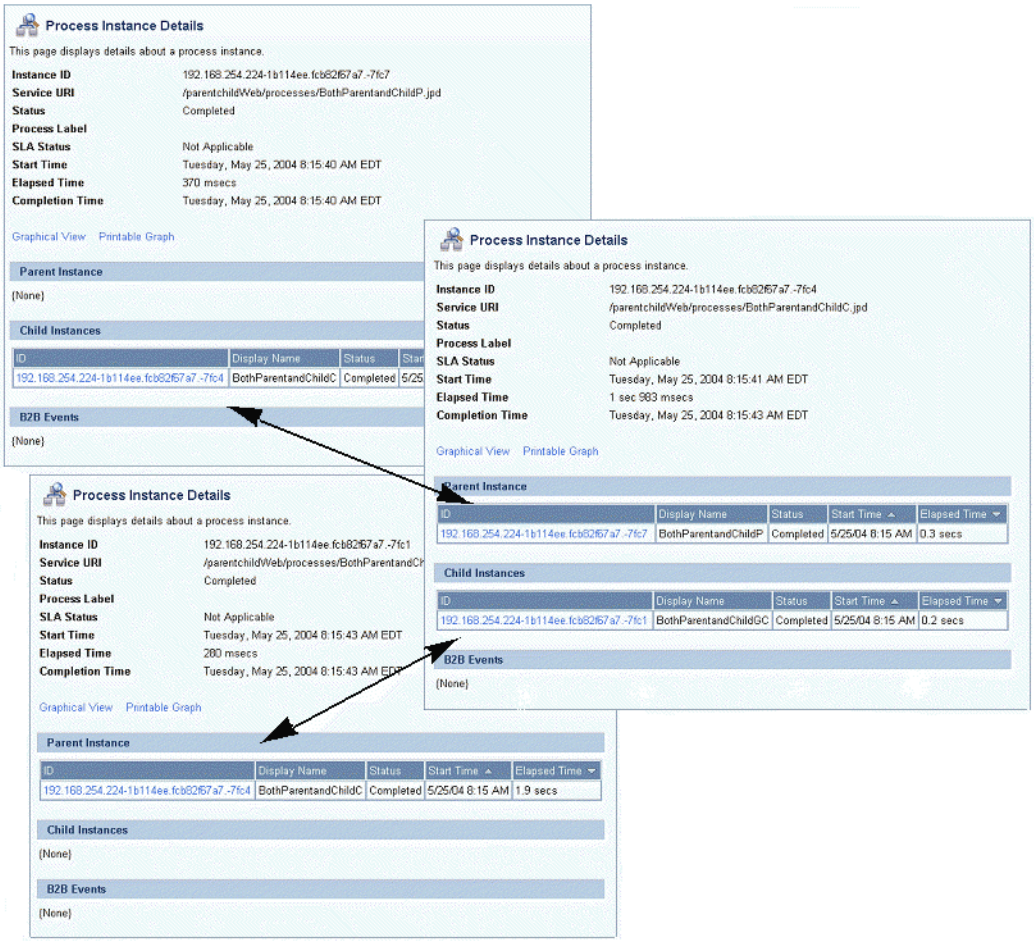
Property	Description
B2B Events	Summary information for any business messages are displayed. The event ID, direction (inbound or outbound), and trading partners (from and to) are displayed. The event ID is a link to the message detail.
Variables	Name, type, and value of each variable defined for the instance. You can view the value of an XML or string variable by clicking it. You can view the value that was assigned to the process variables while the process is running and track the variable values after the process completes, terminates, or aborts. When a process is aborted, behavior of the variable tracking varies for stateless and stateful process. Latest variable values for an aborted stateless process are tracked, even if the transaction in which the variable changed might have been rolled back. For a stateful process, if an exception is thrown in a transaction block, it is rolled back and the variable values are not preserved. However, variable values prior to the transaction roll back are preserved and can be viewed.

Parent-Child Navigation

When a process instance calls another process via the Process control, the process invoked is considered a "child process." In WebLogic Integration 8.1 SP3, information about related processes was added to the **Process Instance Details** page. When you view the detail for an instance that has been called by another, identifying information for the calling process instance is displayed in the **Parent Instance** section. When you view the detail for a process that invokes one or more other instances, the information for each instance invoked is displayed in the **Child Instances** section.

In addition to displaying identifying information for related instances, the console also provides the ability to navigate between related instances. The following figure illustrates the parent-child navigation functionality.

Note: The parent-child navigation functionality is limited to instances invoked via the Process control. Instances started by the Service Control or Service Broker Control are not identified as child instances.



Related Topics

- “Viewing an Interactive or Printable Process Instance Graph” on page 4-17
- “Suspending, Resuming, Terminating, or Unfreezing Process Instances” on page 4-19

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 4-12. 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 4-19.

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:

Note: You must have Adobe Acrobat Reader installed to view the printable graph.

1. Locate the process instance to view. See "Listing and Locating Process Instances" on page 4-7.
2. Click the process name to display the **Process Instance Details** page.

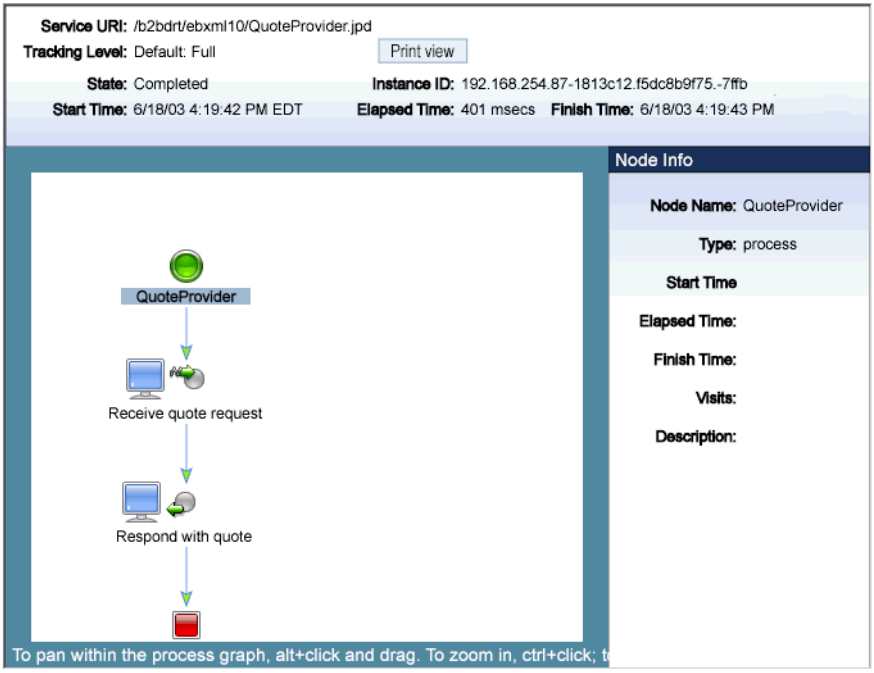
3. Click **Printable Graph**.

   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 "Requirements for the Interactive Graph" on page 4-3.
2. Locate the process instance to view. See "Listing and Locating Process Instances" on page 4-7.
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.

Related Topics

- "Requirements for the Interactive Graph" on page 4-3

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 4-7.
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 4-7.
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 4-7.
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.

CHAPTER 5

Message Broker

The *Message Broker* module allows you 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 11-3.

The following topics are provided:

- Viewing Global Message Counts
- Resetting the Message Counts

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 (if the metadata is typed XML) or message body (if the body is string or typed XML). 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 the following sections of *Building Integration Applications* in the WebLogic Workshop help:

- Publishing and Subscribing to Channels
- "Note About Static and Dynamic Subscriptions" in @jpd:mb-static-subscription Annotation

Overview of the Message Broker Module

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

Page	Associated Tasks	Help Topics
Channel Summary List	View a list of channels. Channel name, message type, message count, subscriber count, and dead letter count are displayed.	"Listing and Locating Channels" on page 5-4
	Filter the list by channel name. Use ? to match any single character or * to match zero or more characters.	
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.	"Viewing Channel Details and Subscriptions" on page 5-5
Edit Channel Subscribe and Publish Properties	View and set the publish roles, subscribe roles, and 'dispatch as' principal defined for the channel.	"Setting Channel Security Policies" on page 5-7
View Message Broker Statistics	View summary statistics, including number of active channels, subscribed channels, dead letter count, message count, and time of last reset.	"Viewing Global Message Counts" on page 5-8
	Reset the counts (published messages and dead letter).	

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.

Related Topics

- "Viewing Channel Details and Subscriptions" on page 5-5

Viewing Channel Details and Subscriptions

The **View Channel Details** page displays the following properties.

Property	Description	Administrator Can Set (Yes/No)
Channel Name	The name of the channel as defined in the channel file. For example, `/myproject/mygroup/mytype/mychannel` is displayed for the following:  	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 process or Web service types that can subscribe to the channel. For example, a JPD with a static subscription counts as one subscription, whether there are zero or many instances running. Similarly, a JPD that uses a Message Broker Subscription control counts as one subscription, whether there are zero or many instances actively subscribed. The identity of each subscriber is listed in the Subscription Rules table.	No
Message Count	The number of messages delivered to this channel.	No
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 appropriate deadletter channel: `/deadletter/xml`, `/deadletter/string`, or `/deadletter/rawData`. The Dead Letter Count reflects the number of messages sent to the dead letter channels since the count was last reset.	No

Property		Description	Administrator Can Set (Yes/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 dynamically subscribe to this channel. If no roles are defined, everyone is authorized. **Note:** When you update the subscribe roles, the new roles are enforced only on subscriptions that occur after you update the value. Existing dynamic subscriptions are maintained.	Yes
Dispatch As		The user under which messages are dispatched to subscribers. If no user is specified, messages are dispatched as `Anonymous`.	Yes
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 5-4.
2. Click the channel name to display the **View Channel Details** page.

Related Topics

- "Setting Channel Security Policies" on page 5-7

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 an authenticator that implements the required MBeans is not configured, the options for configuring the channel security policies are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

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 5-4.
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 restore original settings, click **Reset**.
   - To disregard changes and return to the **View Channel Details** page, click **Cancel**.

Viewing Global 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.
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 appropriate deadletter channel: `/deadletter/xml`, `/deadletter/string`, or `/deadletter/rawData`. The Dead Letter Count reflects the number of messages sent to the dead letter channels 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.

Related Topics

- "Listing and Locating Channels" on page 5-4

Resetting the Message Counts

You can reset the message counts for one or more channels from the Channel Summary List.

To reset the message counts for one or more channels:

1. From the home page, select the **Message Broker** module.

   The Channel Summary List is displayed.

2. Click the check box to the left of the channels to be reset select them.

   Note: You can filter the list as described in "Listing and Locating Channels" on page 5-4.

3. Click **Reset Message Count** to reset the message count for the selected channels.

CHAPTER 6

Event Generators

The *Event Generator* module allows you to:

- Create and deploy new event generators.
- Add channel rules to existing 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 11-3.

The following topics are provided:

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 contents (or a reference to an archived location) to Message Broker channels as XML or binary objects. 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 contents 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.
- *MQ event generator*
  Polls for messages on a WebSphere MQ queue and publishes the messages (MQMD headers as metadata along with the message payload) to Message Broker channels. Content filtering, as well as other handling criteria, are specified in the channel rules for the event generator.
- *HTTP event generator*
  The HTTP event generator is a servlet, which takes HTTP requests, checks for the content type, and then publishes the messages to Message Broker channels.
- *RDBMS event generator*
  Polls the database table to check for added, deleted, or updated rows and publishes the results to Message Broker channels. You can also use this event generator to run custom queries on the database table and publish the results to Message Broker channels.

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.

Additional information regarding the configuration of event generators is also found in the following sections of *Deploying WebLogic Integration Solutions*.

- "Key Deployment Resources" in the Introduction provides information about event generator resources.
- "Deploying Event Generators" in Understanding WebLogic Integration Clusters provides information about deploying event generators in a clustered environment, including the targeting and error handling issues related to the deployment of JMS event generators.
- wli-config.properties Configuration File provides information about setting the `wli.jmseg.EatSoapActionElement` property for 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 help topics associated with each are provided:

Page	Associated Tasks	Help Topics
File		
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.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the files read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43
Create New File Event Generator	Create and deploy a File event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14

Page	Associated Tasks	Help Topics
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.	"Defining Channel Rules for a File Event Generator" on page 6-17
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
File Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for a File Event Generator" on page 6-17
Email		
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.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the emails read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43

Page	Associated Tasks	Help Topics
Create New Email Event Generator	Create and deploy an Email event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14
Email Event Generator Definition	Access the Email Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	"Defining Channel Rules for an Email Event Generator" on page 6-20
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
Email Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for an Email Event Generator" on page 6-20
JMS		
View All JMS Event Generators	View a list of JMS event generators.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the messages read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43

Page	Associated Tasks	Help Topics
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, and default channel rule.	"Creating and Deploying Event Generators" on page 6-14
JMS Event Generator Details	Update the default channel rule for the event generator.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
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.	"Defining Channel Rules for a JMS Event Generator" on page 6-22
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
JMS Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for a JMS Event Generator" on page 6-22

Page	Associated Tasks	Help Topics
Timer		
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.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the messages read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43
Create New Timer Event Generator	Create and deploy a Timer event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14
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.	"Defining Channel Rules for a Timer Event Generator" on page 6-24
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42

Page	Associated Tasks	Help Topics
Timer Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for a Timer Event Generator" on page 6-24
MQ Series		
View All MQSeries Event Generators	View a list of MQSeries 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.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the messages read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43
Create New MQSeries Event Generator	Create and deploy a MQSeries event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14

Page	Associated Tasks	Help Topics
MQSeries Event Generator Definition	Access the MQSeries Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	"Defining Channel Rules for an MQ Series Event Generator" on page 6-26
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
MQSeries Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for an MQ Series Event Generator" on page 6-26
HTTP		
View All HTTP Event Generators	View a list of HTTP event generators. Generator name, number of channels, HTTP requests read, last reset time, number of errors, error reset time, and status (running or suspended) are displayed.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the messages read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43

Page	Associated Tasks	Help Topics
Create New HTTP Event Generator	Create and deploy a HTTP event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14
HTTP Event Generator Definition	Access the HTTP Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	"Defining Channel Rules for an HTTP Event Generator" on page 6-32
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
HTTP Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for an HTTP Event Generator" on page 6-32
RDBMS		

Page	Associated Tasks	Help Topics
View all RDBMS Event Generators	View a list of RDBMS event generators. Generator name, number of channels, messages read, last reset time, number of errors, and error reset time are displayed.	"Listing and Locating Event Generators" on page 6-38
	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. It is important to note that the suspended status of an event generator is not preserved when the server is restarted. If the event generator is in the suspended state when the server is restarted, the event generator remains suspended and no events are processed. You must resume the event generator from the WebLogic Integration Administration Console.	"Suspending and Resuming Event Generators" on page 6-41
	Reset the messages read or error count.	"Resetting the Counters" on page 6-42
	Delete one or more event generators.	"Deleting Event Generators" on page 6-43
Create New RDBMS Event Generator	Create and deploy a RDBMS event generator. The event generator initially has no channel rules.	"Creating and Deploying Event Generators" on page 6-14
RDBMS Event Generator Definition	Access the RDBMS Event Generator Channel Rule Definition page to add channel rules to a newly created or existing event generator.	"Defining Channel Rules for a RDBMS Event Generator" on page 6-33
	View the channel rules for an existing event generator. Select a channel rule to view or update details.	"Viewing and Updating Event Generator Channel Rules" on page 6-39
	Delete one or more channel rules.	"Deleting Channel Rules" on page 6-42
RDBMS Event Generator Channel Rule Definition	Create a new channel rule or view and update an existing channel rule.	"Defining Channel Rules for a RDBMS Event Generator" on page 6-33

Creating and Deploying Event Generators

The Event Generator module allows you to create and deploy the event generators included as part of WebLogic Integration. When you create a new event generator as described in this section, it is packaged and deployed as an EJB (JMS, File, Email, Timer, MQ, and RDBMS event generators) or Web application module (HTTP event generator) on a single managed server. Once the event generator has been created and deployed, you can suspend, resume, or add additional channel rules as required.

Note: JMS, HTTP, MQ, and RDBMS event generators can be targeted to any number of managed servers in a cluster. For JMS and MQ event generators, it is typical to target the generator to a single managed server when using a physical JMS destination, or to the cluster when using distributed destinations. To deploy to a single managed server, see the procedures in this section.

This section includes the following:

- Creating and deploying a JMS event generator.
- Creating and deploying a File, Email, Timer, MQ Series, HTTP, or RDBMS event generator.

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**.

   The **Create a New JMS Event Generator** page is displayed.
4. In the **Generator Name** field, enter a unique name for the event generator.

   Note: Names are case insensitive. Leading or trailing spaces are removed.
5. From the **Destination Type** drop-down list, select **javax.jms.queue**, **javax.jms.topic**, or **foreign_jms_destination**.
6. Do one of the following:
   - If you selected **javax.jms.queue** or **javax.jms.topic**, select the JNDI name for the topic or queue from the **Destination JNDI Name** drop-down list.

   – If you selected **foreign_jms_destination**, select the Remote JNDI Name from the **Destination JNDI Name** drop-down list, and then select the foreign destination type (**javax.jms.Queue** or **javax.jms.Topic**) from the drop-down list directly below it.

7. In the **Message Selector** field, specify the JMS message selector. See 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 6-22.
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, Timer, MQ Series, HTTP, or RDBMS 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**, **Timer, MQ Series, HTTP**, or **RDBMS**).
3. Select **Create New**.

   The **Create New** page for the selected type is displayed.

4. In the **Generator Name** field, enter a unique name for the event generator. If you selected **HTTP** in step 2, you must also enter the **Web Application Context Root**.
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 6-17
   - "Defining Channel Rules for an Email Event Generator" on page 6-20
   - "Defining Channel Rules for a Timer Event Generator" on page 6-24
   - "Defining Channel Rules for an MQ Series Event Generator" on page 6-26
   - "Defining Channel Rules for an HTTP Event Generator" on page 6-32
   - "Defining Channel Rules for a RDBMS Event Generator" on page 6-33
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.

Related Topics

- "About the Event Generators" on page 6-2
- "Listing and Locating Event Generators" on page 6-38
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

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 **File Type** drop-down list, select **Disk File** or **FTP**.	Type of file event.	Required
From the **Channel Name** 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 **Message Encoding** field, if you do not want to select the default value, enter the name of the character set. **Note:** 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 **Channel Name** is of type string. See http://www.iana.org/assignments/character-sets for valid values.	Optional
In the **FTP Host Location** field, enter the FTP server.	Location of the FTP server (IP address or host name) if the **File Type** is set to **FTP**.	Required if the **File Type** is set to **FTP**
In the **FTP User Name** field, enter the name.	Name required to access the FTP account.	Required if the **File Type** is set to **FTP**
Do one of the following to specify the **FTP User Password**: • Select the **Use Alias** option button, then select the password alias from the drop-down list. • Select the **Use Value** option button, then enter the password in the field.	If you enter the password in the **Use Value** field, it is stored in clear text in the event generator configuration file. To secure the password, add it to the password store. See "Password Aliases and the Password Store" on page 10-6. After the alias has been added to the password store, it is available for selection from the **Use Alias** drop-down list.	Required if the **File Type** is set to **FTP**

Setting	Description	Required/ Optional
In the **FTP Local Directory field,** enter the path.	Specifies the path to a directory to which files from the FTP server are copied.	Required if the **File Type** is set to **FTP**
In the **Directory** field, enter a valid path.	If **File Type** is set to **Disk**, specifies the path to the directory to poll for files. If **File Type** is set to **FTP**, specifies the path on the FTP server to poll for files. Whether the **File Type** is **Disk** or **FTP**, we highly recommend that you specify a location that is writeable. If the **File Type** is **Disk,** the system verifies that the directory is writeable before polling. If it is not writeable, the error count is incremented, and the reading and publishing process is skipped. If the **File Type** is **FTP**, the files in the directory are read and published at each polling interval. If an error is encountered in deleting a file, the error is logged, and the error count is incremented. The inability to delete files will result in the same files being published at every polling interval.	Required
From the **Pass by filename** drop-down list, select **Yes** or **No**.	If set to **Yes**, the file is staged to the Archive directory and is passed as reference in the FileControlPropertiesDocument, which is sent as the payload of the message. If set to **Yes**, you must specify an Archive directory. The default is **No**.	Required
From the **Scan Subdirectories** drop-down list, select **Yes** or **No**.	Specifies whether or not subdirectories are to be scanned.	Optional
In the **File Pattern** field, enter the pattern.	Optional pattern to filter on. Use `?` to match any single character or `*` to match zero or more characters.	Optional

Setting	Description	Required/ Optional
From the **Sort by Arrival** field, select **Yes** or **No**.	If set to **Yes**, the files are sorted by arrival time. This maintains the sequence (files are processed by arrival time). The default is **No**.	Required
Specify the **Polling Interval** 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 **days** field, then select the number of hours, minutes, and/or seconds from the drop-down lists as required.	Required
In the **Read Limit** field, enter the maximum number of files to read per polling sweep.	Maximum number of files to read per polling sweep. Valid values are **0** or greater. If set to **0** all files are read.	Required
From the **Post Read Action** drop-down list, select **Delete** or **Archive**.	Specifies what the event generator does with a file after it has been read. The default is **Delete**.	Required
In the **Archive Directory** field, enter a valid path.	Specifies the path to a directory to which files are archived.	Required if **Post Read Action** is set to **Archive**, or **Pass by filename** is set to **Yes**
In the **Error Directory** 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 **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the file event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

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 **Server Protocol** drop-down list, select **IMAP** or **POP3**.	Server type for the Email account. The default is **POP3**.	Required
From the **Channel Name** 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 **Hostname** field, enter the server name.	The mail server to poll.	Required
In the **Port Number** field, enter the email server port.	The mail server port. The default is **-1**, which indicates the default port number for the mail server (143 for IMAP, 110 for POP3).	Required
In the **Username** 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 **Password**: • Select the **Use Alias** option button, then select the password alias from the drop-down list. • Select the **Use Value** option button, then enter the password in the field.	If you enter the password in the **Use Value** field, it is stored in clear text in the event generator configuration file. To secure the password, add it to the password store. See "Password Aliases and the Password Store" on page 10-6. After the alias has been added to the password store, it is available for selection from the **Use Alias** drop-down list.	Optional

Setting	Description	Required/ Optional
From the **Attachments** field, select **Archive** or **Ignore**.	Specifies how attachments are handled. If **Archive** is selected, attachments are saved to the **Archive Directory**.	Required
In the **Polling Interval** 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 **days** field, then select the number of hours, minutes, and/or seconds from the drop-down lists as required.	Required
In the **Read Limit** 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 **Post Read Action** drop-down list, select **Delete**, **Archive**, or **Move**.	Specifies what the event generator does with a message after it has been read. **Move** is only available with the IMAP protocol. The default is **Delete**.	Optional
In the **IMAP Move Folder** field, enter a valid IMAP folder.	If **Post Read Action** is set to **Move**, the **IMAP Move Folder** specifies the folder to which the message is moved.	Required if **Post Read Action** is set to **Move**
In the **Archive Directory** field, enter a valid path.	If **Post Read Action** is set to **Archive**, the **Archive Directory** specifies the path to the archive location.	Required if **Post Read Action** is set to **Archive**
In the **Error Directory** field, enter a valid path.	Specifies the file system directory path to write the message and any attachments if there is a problem.	Required

Setting	Description	Required/ Optional
In the **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the email event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

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 **Channel Name** 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 **Property Name** field, enter the name of the required JMS property.	If both **Property Name** and **Property Value** (below) are specified, the value of the property must match **Property Value** to trigger a match. If only **Property Name** is specified, then the presence of the property triggers a match. If both **Property Name** and **Property Value** are blank, all message on the JMS queue are a match.	Optional

Setting	Description	Required/ Optional
In the **Property Value** field, enter the required property value.	If **Property Name** is specified, **Property Value** can be used to specify the value required for a match.	Optional
In the **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the JMS event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

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 **Channel Name** 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 **Effective Time** 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, the event generator will not publish an event until the next **Runs Every** interval (see next setting). If the **Runs Once** option is selected, you must enter a valid, future, **Effective Time** or no event will be generated.	Required
Do one of the following: • Select the **Timer handles DST** option button. • Select the **Timer ignores DST** option button.	If you want to create an event that fires at the same time, every day, for the calendar year, you need to consider the impact of Daylight Savings Time (DST). That is, when standard time is switched to the DST and vice versa. To ensure the Timer event is fired as per schedule taking DST into account, select **Timer handles DST**. Select **Timer ignores DST** to ignore the time difference attributed to DST.	Required
Do one of the following: • Select the **Runs Once** option button. • Select the **Runs Every** option button, then specify the interval in days, hours, minutes, and seconds.	Intervals from the **Effective Time** that each event is to be generated. If the **Runs Once** option is selected, the **Effective Time** constitutes the first and last event generated. **Note:** Because the smallest time interval in a business calendar is a minute, if you specify a **Business Calendar** (see setting below), do not include seconds in the **Runs Every** interval.	Required

Setting	Description	Required/ Optional
Do one of the following: • Select the **Never Expires** option button. • Select the **Expires On** option button, then select the month, day, year, and time from the drop-down lists.	The date and time the configured schedule expires. If the **Never Expires** option is selected, the configured schedule remains in effect indefinitely.	Required
In the **Message** 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
From the **Business Calendar** drop-down list, select a business calendar.	If a business calendar is selected, the **Runs Every** interval represents business time calculated against the specified calendar. See "About Business Calendars and Business Time Calculations" on page 12-2. If no calendar is selected, the **Runs Every** interval represents an absolute period (24 hour day, every day). If you want to modify event generator channel rules and the business calendar associated with the channel rules, you must suspend the corresponding timer event generator before you make any changes. For information on suspending a timer event generator, see "Suspending and Resuming Event Generators" on page 6-41.	Optional
In the **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional

Setting	Description	Required/ Optional
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the Timer event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional
Select or clear the **Is Recoverable** check box.	To recover the timer events that were missed because of server shutdown, select the **Is Recoverable** check box.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

Defining Channel Rules for an MQ Series Event Generator

The **MQSeries 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 **Channel Name** 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 **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
Specify the **Polling Interval** in days, hours, minutes, and/or seconds.	How often to poll the specified message queue. Enter the number of days (if the interval is greater than one day) in the **days** field, then select the number of hours, minutes, and/or seconds from the drop-down lists as required.	Required

Setting	Description	Required/ Optional
From the **Connection Type** drop-down list, select **TCP-IP** or **Bindings**.	The connection mode to be used to connect to the WebSphere MQ queue manager. Select **TCP-IP** or **Bindings**. **Bindings** is shared memory protocol that can only be used to connect to queue managers on the local system. If TCP/IP is selected, you must also specify the **MQSeries Server Host Address**, **Queue Manager Channel Name**, and **Queue Manager Port**.	Required
In the **MQSeries Queue Manager** field, enter the name of the queue manager.	Name of the WebSphere MQ queue manager to connect to.	Required
In the **MQSeries Server Host Address** field, enter the IP address or host name.	IP address or host name for the WebSphere MQ server.	Required if the **Connection Type** is set to **TCP-IP**
In the **MQSeries Queue Manager Channel Name,** enter the MQ channel name for the connection.	Specifies the name of the server connection channel used to connect to the WebSphere MQ queue manager.	Required if the **Connection Type** is set to **TCP-IP**
In the **MQSeries Queue Manager Port Number** field, enter the port number of the queue manager.	The TCP/IP port number used to connect to the WebSphere MQ queue manager.	Required if the **Connection Type** is set to **TCP-IP**
In the **MQSeries Queue Manager CCSID** field, enter the CCSID for the locale expected by the application.	Specifies a Coded Character Set Identifier (CCSID) supported by WebSphere MQ. For example, for the **en_US.iso88591** locale, the CCSID is **819**, for the **ja_JP.SJIS** locale, it is **932**. For more information about supported CCSIDs, and about converting between message data from one coded character set to another, see the WebSphere MQ documentation for your platform.	Optional

Setting	Description	Required/ Optional
In the **MQSeries Queue Name** field, enter the name of the queue.	Name of the WebSphere MQ queue to monitor for messages.	Required
In the **MQSeries Error Queue Name** field, enter the name of the queue.	Specifies the name of the queue for messages that cannot be processed due to an error condition. For example, if the message type retrieved from the queue does not match the message type set for the Message Broker channel, an exception would be generated during processing. If you specify the name of an error queue, such errored messages are moved to the specified queue. If you do not specify the name of an error queue, the errored message will remain in the original queue.	Optional
To enable content filtering, enter the fully qualified name of the content filter class in the **Content Filter Class** field.	The fully qualified name of the class implementing the event content filtering logic. As described in "Content Filtering" on page 6-30, this class is an extension of the `com.bea.wli.mbconnector.mqseries.AbstractContentFilter` class.	Optional
Select or clear the **Require MQ Data Conversion** check box.	When checked, the `MQGMO_CONVERT` option is enabled, and directs the queue manager to convert the contents of the message retrieved from the queue. This option must be checked when retrieving messages in a cross platform environment involving mainframes (for example, a mainframe application puts a message on the queue that is retrieved by the event generator on a PC). This option is typically enabled to convert messages to the native character set as specified by the CCSID.	Optional
In the **Specify Number of Threads** field, enter the number of processing threads.	Number of event generator processing threads.	Required

Setting	Description	Required/ Optional
In the **Message Per Poll** field, indicate the number of messages to be retrieved by each thread in each polling cycle.	The number of messages to be retrieved by each event generator thread in each polling cycle. Specify **-1** to retrieve all the messages available on the queue in each polling cycle.	Optional
If WebSphere MQ authorization is enabled, specify the user name in the **MQSeries User Name** field.	The WebSphere MQ user name used to connect to the WebSphere MQ queue manager.	Optional
If WebSphere MQ authorization is enabled, specify the password in the **MQSeries User Password** field.	The WebSphere MQ user password used to connect to the Web sphere MQ queue manager.	Optional
Select the **SSL Required** check box if you want to configure a SSL port for the MQ Series event generator.	When the **SSL Required** check box is selected, the message data from the queue is sent via a secure port. Only one-way SSL is supported.	Optional
Enter the **MQ Cipher Suite**.	The cipher suite algorithm is used to encrypt and decrypt message communication between the MQSeries server and the MQSeries client. You must provide the SSL cipher suite information before you put or get messages from the queue.	Required only for SSL Connection
Enter the **SSL Trust Store**.	This value represents the location of the trust store.	Optional
Enter the **SSL Trust Store Type**	This value represents the type of trust store.	Optional

Setting	Description	Required/ Optional
Enter the **SSL Trust Store Password**	The password used for the SSL trust store.	Required only when SSL trust store location is specified.
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional

Content Filtering

Filtering the messages in a queue based on message contents requires a custom content filter class that extends the `com.bea.wli.mbconnector.mqseries.AbstractContentFilter` class.

Listing 6-1 Content Filter

```
package com.bea.wli.mqseries.eventgen.contentfilter;

import com.bea.wli.mbconnector.mqseries.AbstractContentFilter;

public class ContentFilter extends AbstractContentFilter

{

    public ContentFilter()
    {
    }

    public boolean matchContent(byte abyte[])
    {
```

```
    /*This function always returns true, ensuring that all
       messages generate the event. However the user should
       put in his content filtering logic based on the
       contents of the message here. The abyte[] byte array
       parameter to this function is the byte array
       representation of the message. Return true if the
       message should generate an event, otherwise return
       false*/
   return true;
}
```

The parameter to this function is the byte array representing the message retrieved from the queue by the event generator. You can create content filtering logic by performing required checks on the contents of the message represented by the byte array. Return a Boolean value of **True** from the function if the message should generate an event. Otherwise return a Boolean value of **False**.

Once it is defined, the class implementing the content filtering logic should be bundled in a jar file and included in the WebLogic `CLASSPATH`.

To create a custom content filter class:

1. Extract the `mqegEjbUtil.jar` from the *`WL_HOME`*`\integration\egs\mqEG.ear` file and include it in the `CLASSPATH` variable of the environment where the custom content filter class will be developed.
2. Create the class by extending `com.bea.wli.mbconnector.mqseries.AbstractContentFilter`

   Note: This class is present in the `mqegEjbUtil.jar` file that you extracted in step 1.
3. Write the Code for the Content Filter Class. Listing 6-1 provides an example.
4. Compile the custom content filter class.
5. Extract the `AbstractContentFilter` class from the `mqegEjbUtil.jar` and store in a directory in your file system by maintaining the package structure.
6. Create a JAR, for example, `mycontentfilter.jar`, which contains the `com.bea.wli.mbconnector.mqseries.AbstractContentFilter` class and the custom content filter class compiled in step 4.

7. Include this JAR file in the `CLASSPATH` variable in the WebLogic Start Server script.
8. Start the WebLogic Server.
9. When you create the channel rule for the event generator, specify the fully qualified class name of the content filter. For example, `com.bea.wli.mqseries.eventgen.ContentFilter`.

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

Defining Channel Rules for an HTTP Event Generator

The **HTTP 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 **Channel Name** drop-down list, select a Message Broker channel.	The name of the Message Broker channel to which HTTP events are published.	Required
In the **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
From the **Publish As** drop-down list, select a user name.	The **Publish As** property allows the event generator to publish its messages as a specific user. Setting this property enables messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14
- "Viewing and Updating Event Generator Channel Rules" on page 6-39

Defining Channel Rules for a RDBMS Event Generator

The **RDBMS 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 **Channel Name** drop-down list, select a Message Broker channel.	The name of the Message Broker channel to which messages matching the configuration criteria are published. If you are publishing to an XML or string channel, then an XML schema (`.xsd`) file will be created in the WebLogic domain folder under a directory with the same name as the channel rule definition. You can use this .XSD for validations. If you select a RawData channel type from the **Channel Name** drop-down list, the event generator publishes a serialized `weblogic.jdbc.rowset.WLCachedRowSet` containing the database rows that were polled/processed.	Required
In the **Description** field, enter a description of the channel rule.	A user-friendly description of the channel rule.	Optional
In the **Event Name** field, enter a unique event name.	Identifies a unique event name across channels and across RDBMS Event Generators.	Required
Specify the **Polling Interval** in days, hours, minutes, and/or seconds.	Specifies how often the Database is polled. Enter the number of days (if the interval is greater than one day) in the **days** field, and select the number of **hours**, **minutes**, and/or **seconds** from the drop-down lists provided.	Required
From the **Datasource JNDI Name** drop-down list, select a jndi name.	Identifies the jndi name of the data source connection for the database. The list is populated based on the data sources configured in the Weblogic Server where the event generator is running. For more information on configuring data sources, see the RDBMS Event Generator User Guide.	Required

In the **Max Rows Per Poll** field, enter the number of records to be retrieved by each thread in each polling cycle.	Specifies the number of records to be retrieved by each thread in each polling cycle. This number must be a valid integer greater than 1 and less than 10,000. **Note:** The default value is 1. Please change this value to a value that suits your requirements.	Required
In the **Max Rows Per Event** field, enter the number of records that will be part of the payload of a single event.	For example, if there are 10 records of interest and the **Maximum Rows Per Event** is 3, there will be 3 events with 3 records each, and an event with the remaining record. If there are 2 records of interest and the **Maximum Rows Per Event** is 3, there will still be an event with 2 records.	Required
Event Type Selection: Select the required event type; **Trigger** or **Query/Post Query**.	A **Trigger** event notifies an Insert, Update, or Delete event occurring in a database table. **Query/Post Query** notifies records of interest based on a select query given on a database table and executes the SQL specified in the Post Query for each event posted.	Required
Select a user name from the **Publish As** drop-down list.	The **Publish As** property enables the event generator to publish its messages as a specific user. Setting this property allows messages to be delivered to a secured message broker channel. If **Publish As** is not specified, messages are published as `Anonymous`.	Optional
For a Trigger Event		
From the **Trigger** drop-down list, select Insert, Delete, or Update.	Specifies that an Insert, Update, or Delete event has occurred in a database table using the trigger mechanism. **Note:** While creating Trigger Type Events, the Login ID/Password supplied for the data source must have permission to CREATE/DROP Tables, Triggers, and Sequences (Sequence for Oracle only).	Required (Default is Insert)

In the **Table Name** field, enter the database table name on which the trigger event will be defined.	Enter the name of the database table. Use the corresponding syntax for the following databases: **Oracle**: SCHEMA.TABLENAME **DB2 UDB**: SCHEMA.TABLENAME **Informix Dynamic Server**: Catalog.Schema.Table **SQL Server**: Catalog.Schema.Table **Sybase Adaptive**: Catalog.Schema.Table **Note**: Click the **Table Name** link to view the schemas and table names. Select the radio button next to the table name you require and click **Submit** to confirm your selection.	Required
Select Table Columns to publish	Click this link to browse the columns of the database table entered in the **Table Name** field. Select the desired columns by selecting the check box beside the desired column. Click **Select Columns** to choose the checked columns. Only those columns of the row you select are published when an Event occurs. For example, when 2 of 4 columns are selected for an Update Event, this does NOT mean that the Event is going to listen for updates on those 2 columns alone. The two are not connected. When a Trigger Type Event is configured, it is for an entire Row. An Event will be fired even if only 1 column is chosen and even if it is not one of the updated columns. For **Delete** and **Insert** Trigger Events, the selected columns of the Inserted/Deleted row will be published. If you select **Update** Event, every column chosen will get published along with a similar column with "OLD_" as the prefix. The "OLD_" column will contain the column value before the update occurred. If no columns are selected, all the columns in the table will be published.	Optional

In the **No of Threads** field, enter the number of processing threads.	Specifies the number of event generator processing threads. If the number entered is greater than 1, then the events may not be delivered in the same order as they were in the database. The greater the number of threads, the better the concurrency, as with any concurrent system, order is sacrificed for higher throughput. The maximum number of rows and maximum number of events specified above are related to the number of processing threads. The maximum number of rows per poll is equal to the maximum number of rows per event multiplied by the maximum number of threads.	Required
For a **Query/Post Query** event type		

In the first text area, specify the **SQL Query**.	This **SQL Query** is executed and returns records of interest. The Query must be a Select Query. The Query is not validated for correctness. For example, SELECT FIRST_NAME, LAST_NAME, EMPLOYEE_ID FROM RDBMS_USER.EMP_TBL WHERE STATUS = 'Intern'.	Required
In the **Post Query** text area, specify the Post Query.	Specifies a **Post Query** that will be executed for every row returned by the **SQL Query** above. You must enter the exact names of the columns and the @ prefix to provide runtime values. **Post Query** is not validated for correctness. For example, DELETE FROM RDBMS_USER.EMP_TBL WHERE FIRST_NAME = @FIRST_NAME. "`SELECT *`" will not work if the Post Query refers to a column in the Query. The selected columns must be listed individually. All SQL statements must use fully qualified table names. The **Post Query** is only executed if the Query specified in the **SQL Query** field returns a `ResultSet` and if it contains one or more rows. If you leave the **Post Query** field empty and enter a SELECT query in the **SQL Query** field, the selected row is deleted after it gets published. If `no-op`, meaning "No Operation", is specified in the **Post Query** field, the selected rows are not deleted automatically. If you do not want to specify a Post Query and also do not want the selected rows to be deleted automatically, then you must enter `no-op` in the **Post Query** field. Also, `automatic-delete` only works if a SELECT query refers to a single Table (SELECT DEPT. NAME, EMP.ADDRESS FROM DEPT., EMP WHERE DEPT.NAME = EMP NAME refers multiple tables). `Automatic delete` does not work for DB2 and Informix.	Optional

Related Topics

- "Creating and Deploying Event Generators" on page 6-14

- "Viewing and Updating Event Generator Channel Rules" on page 6-39

Listing and Locating Event Generators

The **View All** page displays the following information for each configured event 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) Emails Read (Email) Messages Read (JMS, Timer, MQ, RDBMS, and HTTP)	Number of items read by the event generator since the read counter was last reset or the server was last restarted. **Note:** Suspending and resuming an event generator also resets the counters.
Last Reset Time	Time the read counter was last reset.
Error Count	Number of errors since the error counter was last reset or the server was last restarted. 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). **Note:** The status for the RDBMS event generator is displayed on the **RDBMS Event Generator Definition** page.

To list and locate File, Email, JMS, or Timer 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.

To list and locate HTTP, MQSeries, or RDBMS event generators:

1. From the home page, select the **Event Generator** module.
2. From the left panel, select the type of event generator (**HTTP**, **MQ Series** or **RDBMS**).
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.

Related Topics

- "Viewing and Updating Event Generator Channel Rules" on page 6-39
- "Suspending and Resuming Event Generators" on page 6-41
- "Deleting Event Generators" on page 6-43

Viewing and Updating Event Generator Channel Rules

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

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

1. Locate the event generator. See "Listing and Locating Event Generators" on page 6-38.
2. Click the event generator name to display the **Event Generator Definition** page.
3. Click **Edit Generator Details**.

   The **JMS Event Generator Details** page is displayed.
4. Select a new channel from the **Default Rule Channel** drop-down list.
5. Click **Submit** to update.

To view channel rules:

1. Locate the event generator. See "Listing and Locating Event Generators" on page 6-38.
2. Click the event generator name to display the **Event Generator Definition** page.

To add or update channel rules:

1. Do one of the following to display the **Generator Channel Rule Definition** page:
   - To add a channel rule, click **Define a New Channel Rule**.
   - To update existing rules, click the value applicable to the generator type (see the following list), and then click **Edit Channel Rule**.

     Timer—Effective time
     File—Channel Directory
     Email—Hostname
     JMS—Property Name
     MQ—Polling Interval
     HTTP—Channel Name

     Note: You cannot update the channel rules for a RDBMS event generator. You must delete the channel and create a new one.
2. 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 6-17.

   "Defining Channel Rules for an Email Event Generator" on page 6-20.

   "Defining Channel Rules for a JMS Event Generator" on page 6-22.

   "Defining Channel Rules for a Timer Event Generator" on page 6-24.

   "Defining Channel Rules for an MQ Series Event Generator" on page 6-26.

   "Defining Channel Rules for an HTTP Event Generator" on page 6-32.
3. Click **Submit** to add or update the channel rule.

To delete channel rules:

1. Click the check box to the left of the channel rules to be deleted.
2. Click **Delete**.

   A confirmation dialog box is displayed.

3. Click **OK** to confirm.

   The selected channel rules are deleted.

To reorder channel rules:

Note: Not available for all event generator types.

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 event generator.

Note: The messages read and error counts are stored in memory only; the counts are not stored to disk or other persistent store. Therefore, when you suspend and resume an event generator, the messages read and error counts are reset to zero.

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

Note: When an event generator is suspended before a server restart, it automatically switches to Running mode on restart. This functionality is uniform across all event generators.

To suspend an event generator:

1. Locate the event generators to be suspended. See "Listing and Locating Event Generators" on page 6-38.
2. Click the check box to the left of the event generators you want to select.
3. Click **Suspend**.

   The selected generators are suspended.

   Note: For all event generators, when an event generator is suspended, the counter resets to 0. However, when you suspend a RDBMS event generator, the event generator resets to 0 AND the message changes to "Last-Reset-Time".

To resume an event generator:

1. Locate the event generators to be resumed. See "Listing and Locating Event Generators" on page 6-38.
2. Click the check box to the left of the event generators you want 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 6-38.
2. Click the check box to the left of the event generators you want 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 *EGType* Event Generators** (where *EGType* is JMS, Timer, MQ Series, HTTP, or RDBMS), 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 6-38.
2. Click the check box to the left of the event generators you want to select.
3. Click **Reset Error Count**.

Deleting Channel Rules

You can delete any 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 6-38.
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.

Note: You cannot delete a RDBMS event generator channel rule if a transaction is inserting rows into the User Table on which the event in question has been configured. You must wait for the transaction to complete before deleting the channel rule.

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 6-38.
2. Click the check box to the left of the event generators you want to delete.
3. Click **Delete**.

   The selected generators are deleted.

CHAPTER 7

Worklist Administration

The *Worklist Administration* module allows you 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 11-3.

The following topics are provided:

- 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 help topics associated with each are provided:

Page	Associated Tasks	Help 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.	Listing and Locating Worklist Tasks
	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.	Updating Task Comment, Owner, or Due Dates from the Summary Page
Update State for Selected Tasks	Update the state for one or more task instances.	"Updating Task State or Deleting Tasks" on page 7-12

Page	Associated Tasks	Help Topics
Update Comment for Selected Tasks	Update the comment for one or more task instances.	Updating Task Comment, Owner, or Due Dates from the Summary Page
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.	Constructing a Custom Query for Task Instances
Worklist Task Details	View task instance properties.	Viewing and Changing Task Details
	Update the state of the task, or delete the task.	Updating Task State or Deleting Tasks
Edit Worklist Task Details	Edit task instance details.	Viewing and Changing Task Details
Work Substitute Routing Table	View the list of substitute routing rules. Rule name, effective date, expiration date, source, and target are displayed.	Listing and Locating Substitute Routing Rules
	Filter the list by rule name. Use ? to match any single character or * to match zero or more characters.	
Add a New Substitute Rule	Define the name, effective date, expiration date, source, and target for a new substitute routing rule.	Adding a Substitute Routing Rule
Edit Substitute Rule	Change the effective date, expiration date, source, or target for an existing substitute routing rule.	Changing a Substitute Routing Rule

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 7-9.

Property	Description
Task ID	Unique task instance ID. This is a link to the **Worklist Task Detail** page. See "Viewing and Changing Task Details" on page 7-9.
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 7-6.

Related Topics

- "Viewing and Changing Task Details" on page 7-9
- "Updating Task Comment, Owner, or Due Dates from the Summary Page" on page 7-14
- "Updating Task State or Deleting Tasks" on page 7-12

Listing and Locating Substitute Routing Rules

The **Work 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.

Related Topics

- Changing a Substitute Routing Rule
- Deleting a Substitute Routing Rule

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 **Enter Task IDs** 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 **Task Name** 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.

Setting	Description
In the **Parent Process IDs** 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 **Parent Process URI** 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 **Task State** check boxes, select one or more states.	Specify one or more of the following states: **assigned**, **claimed**, **started**, **suspended**, **completed**, **aborted**. The search returns tasks in the specified states that also match any other criteria specified.
In the **Description** 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 **Comment** 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 **Priority from** and **to** 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 **Claim Due Date**, do one or both of the following: • Click the **After** check box, then select the target date from the drop-down lists. • Click the **Before** check box, then select the target date from the drop-down lists.	The search returns tasks with a claim due date later than the **After** date (if specified) and earlier than the **Before** date (if specified), that also match any other criteria specified.

Setting	Description
Under **Complete Due Date**, do one or both of the following: • Click the **After** check box, then select the target date from the drop-down lists. • Click the **Before** check box, then select the target date from the drop-down lists.	The search returns tasks with a complete due date later than the **After** date (if specified) and earlier than the **Before** date (if specified), that also match any other criteria specified.
In the **Assignee contains** 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.
If needed, select the **Check to search for tasks with NO assignee field.**	searching for tasks that are not assigned.
In the **Claimant contains** 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 **Owner contains** 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 a message indicating the search is complete is displayed.
5. Click **Close**.

   You are returned to the **Worklist Task Summary** page. The tasks matching the criteria (if any are found) are displayed.

Viewing and Changing Task Details

The **Worklist Task Details** page allows you to view task properties. 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.

Note: If an authenticator that implements the required MBeans is not configured, the options for updating the owner, or assigning or claiming the task are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

The following table summarizes the properties displayed:

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
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: • Any user included in the list of assignees. • A member of any group included in the list of assignees.	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

Property	Description		Administrator Can Set (Yes/No)
State	State of the task.		Yes
	Assigned	The assignees have be designated, but the task has not yet been claimed.	
	Claimed	A user has claimed the task, thus indicating an intent to complete the task.	
	Started	The claimant has started working on the task.	
	Completed	The claimant has completed the task.	
	Suspended	The task is "on hold." An assigned, claimed, or started task can be placed in the suspended state.	
	Aborted	The task has been cancelled. An aborted task can be assigned or deleted.	
Description	Description of the task.		No
Comment	Comment associated with the task.		Yes
Priority	Priority assigned to the task.		Yes
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 7-4.
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 7-12. 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.

   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.

   The **Edit Worklist Task Details** page is displayed.

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 Creating and Managing Worklist Tasks in *Using the Worklist*.

Note: If an authenticator that implements the required MBeans is not configured, the options for updating tasks assigmees or claimant are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

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: • Any user to which it is assigned. • A member of any group to which it is assigned.
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."
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 7-4.
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 7-4.
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 7-4.
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 7-4.
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 7-4.
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 7-4.
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.

Related Topics

- "Updating Task State or Deleting Tasks" on page 7-12

Adding a Substitute Routing Rule

The **Add a New Substitute Rule** 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 New Substitute Rule** 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 New Substitute Rule** 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 Substitute Rule** 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 7-5.
2. Click the name to display the **Edit Substitute Rule** 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 Substitute Rule** 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 7-5.
2. Click the check box to the left of each substitute to be deleted.
3. Click **Delete Selected Substitutes**.

CHAPTER 8

Application Integration

The *Application Integration* module allows you to manage application views and adapter instances. For each application view, you can:

- View and reset event and service statistics.
- View adapter instances used by an application view.
- Set environment variables and security policies.
- Change event and service connections.
- Change auto suspend settings.
- Suspend an application view or resume a previously suspended application view.

For each adapter instance, you can:

- View event and service statistics.
- View application views that depend on an adapter instance.
- Manage principal mappings between WebLogic Server usernames and EIS usernames.
- Change auto suspend settings.
- Suspend, resume, and redeploy an 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 11-3.

The following topics are provided:

- About Application Integration Monitoring and Configuration
- 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 Connection Factory Pool Statistics for a Service Connection
- Viewing Dependent Application Views for an Adapter Instance
- Viewing and Changing Application View Details
- 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 Adapter Instance 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
- Enabling or Disabling Container-Managed Sign-On
- 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

Within WebLogic Integration, *adapters*, *application views* and *controls* are used to expose enterprise resources by providing various levels of abstraction. Adapters provide the detailed low-level APIs required to interact with an enterprise resource (for example, SAP, PeopleSoft, or Siebel). Application views provide the intermediate layer between a *control* and an *adapter*. An application view provides the control with an XML interface into the adapter, as well as basic management capabilities to suspend and resume application view connections. Adapters can be configured to provide *event connections* for event delivery, *service connections* for service invocations, or both.

Note: To learn more 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.

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

About the Statistics Displayed

The following sections provide important information about the statistics displayed:

- Statistics are Reset when MBeans are Recreated
- Statistics for Application Views and Adapters in Testing are Included

Statistics are Reset when MBeans are Recreated

It is important to understand that the statistics displayed do not persist across application view or adapter redeployment. The application integration statistics displayed in the WebLogic Integration Administration Console are derived from the `com.bea.wlai.management.runtime.AppViewSummaryMBean` and the `com.bea.wlai.management.runtime.AdapterSummaryMBean` MBeans. For performance reasons, these MBeans store the statistics in memory only; the statistics are not stored to disk or other persistent store. Therefore, any time these MBeans are destroyed, the statistics they contain are lost.

For example, if the application containing an application view is redeployed, all the MBeans for the application view are destroyed and recreated, and the application view statistics are reset to zero. When the statistics page for the redeployed application view is refreshed, the counts are all reset to zero. Similarly, when adapter instances are redeployed the adapter instance statistics are reset to zero.

In a single server environment, restarting a managed server also resets the application view and adapter statistics to zero.

In the case of a cluster, restarting a managed server can cause confusing counts to be displayed in the WebLogic Integration Administration console. This is because the counts displayed are an aggregate value across all nodes in the cluster. When a single managed server is rebooted, only those MBeans that reside on that managed server are destroyed and recreated. Thus, only the portion of the total statistics represented by the rebooted managed server are lost.

Statistics for Application Views and Adapters in Testing are Included

WebLogic Integration Administration Console includes 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. To assist in distinguishing, the names of application views and adapter instances in the Testing state are preceded by underscore characters (for example, `__myapplicationview`).

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

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 for an Adapter Instance
- 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 Adapter Instance 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
- Enabling or Disabling Container-Managed Sign-On

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 view 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 view.
- If you change the setting for container-managed sign-on, you must redeploy the application view.
- If you change the values of environment variables, you may have to redeploy the adapter instance or the application view that uses them—depending on the design of the adapter.

Note: Because redeploying an adapter instance or application view 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.

Note: When an application view service is invoked, if the adapter instance is suspended, the application is forced into the suspended state. Specifically:

- When a synchronous service is invoked, a check is performed to see if the adapter is suspended. If the adapter instance is suspended, an ApplicationViewSuspendedException is thrown, and the application view is suspended.
- When an asynchronous service is invoked, if the adapter is suspended, the asynchronous processor puts the request back on the request queue and the application view is forced into the suspended state. The suspended application view allows new asynchronous services to be invoked, but does not process them or return a response until the application view and the adapter instance are resumed.

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 Application Integration 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 11-3.) 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
- Enabling or Disabling Container-Managed Sign-On
- 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 help topics associated with each are provided:

Page	Associated Tasks	Help Topics
Application View Management		

Page	Associated Tasks	Help Topics
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.	"Listing and Locating Application Views" on page 8-13
	Filter the list by application view ID. Use ? to match any single character or * to match zero or more characters.	
	Access the Application View Details page for a selected application view.	"Viewing and Changing Application View Details" on page 8-20
	Reset event counts and service counts.	"Resetting the Counters" on page 8-47
Application View Details	View application view properties, including properties of its events and services.	"Viewing and Changing Application View Details" on page 8-20
	Suspend or resume the application view.	"Suspending or Resuming an Application View or Adapter Instance" on page 8-45
	Access one of the following pages to view or update settings: Application View Container Managed Sign-On Settings Application View Auto Suspend Settings Application View Instance Summary Application View Environment Variables Application View Security Application View Event Connection Application View Service Connection	
	Access the Adapter Instance Details page for an application view's adapter.	"Viewing and Changing Adapter Instance Details" on page 8-24

Page	Associated Tasks	Help Topics
Application View Container-Managed Sign-on Settings	Enable or disable container-managed sign-on.	"Enabling or Disabling Container-Managed Sign-On" on page 8-42
Application View Auto Suspend Settings	View and set auto suspend properties. Enable or disable auto suspend. Change auto suspend timeout, or suspended request retry interval.	"Viewing and Changing Application View Auto Suspend Settings" on page 8-32
Application View Instance Summary	For each event type, view a count of events and errors, events per second, and suspended events.	"Viewing Application View Instance Statistics" on page 8-15
	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.	
	Reset event counts and service counts.	"Resetting the Counters" on page 8-47
Application View Environment Variables	View the default and current values for each environment variable defined in the application view. Set or update the current value.	"Viewing and Changing Environment Variable Values for an Application View" on page 8-34
Application View Security	View and change the list of roles authorized to execute services and subscribe for events on an application view.	"Updating Security Policies" on page 8-43
Application View Event Connection	View and change the adapter used by the events for an application view.	"Changing Event Connections for an Application View" on page 8-37
Application View Service Connection	View and change the adapter used by the services for an application view.	"Changing Service Connections for an Application View" on page 8-38

Page	Associated Tasks	Help Topics
Adapter Instance Management		
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.	"Viewing Adapter Instance Statistics" on page 8-17
	Filter the list by adapter instance ID. Use ? to match any single character or * to match zero or more characters.	
	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, auto suspend state (enabled or disabled), auto suspend timeout, and whether or not events connections are enabled.	"Viewing and Changing Adapter Instance Details" on page 8-24
	Suspend or resume the adapter instance.	"Suspending or Resuming an Application View or Adapter Instance" on page 8-45
	Redeploy the adapter instance to activate changes.	"Redeploying an Adapter Instance" on page 8-46
	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: Adapter Instance Auto Suspend Settings Adapter Instance Event Connection Adapter Instance Service Connection	
Adapter Instance Statistics	View event and service statistics for an adapter instance.	"Viewing Adapter Instance Statistics" on page 8-17

Page	Associated Tasks	Help Topics
Dependent Application Views of Adapter Instances	View a list of all application views that depend on an adapter instance.	"Viewing Dependent Application Views for an Adapter Instance" on page 8-20
Adapter Instance Auto Suspend Settings	Enable or disable auto suspend for the adapter instance. Reset the auto suspend timeout.	"Viewing and Changing Adapter Instance Auto Suspend Settings" on page 8-33
Adapter Instance Event Connection	View and change event properties for an adapter's event connection.	"Viewing and Changing Event Connection Properties" on page 8-27
	Set event generation targets.	"Changing Event Generation Targets" on page 8-39
Adapter Instance Service Connection	View a list of connection factories available to handle service invocations.	"Viewing and Changing Service Connection Properties" on page 8-28
	Access the Adapter Instance Service Connection Details page to view properties for a service connection.	
Adapter Instance Service Connection Details	View service connection properties, including the list of roles authorized to obtain connections from the connection pool. Access the Edit Adapter Instance Service Connection Details to update properties.	"Viewing and Changing Service Connection Properties" on page 8-28
	View connection pool settings for a connection factory.	"Viewing and Changing Connection Pool Size Parameters" on page 8-30
	Access WLS to EIS Principal Mapping page.	"Viewing and Changing WebLogic Server to EIS Principal Mappings" on page 8-35

Page	Associated Tasks	Help Topics
Edit Adapter Instance Service Connection Details	Update service properties.	"Viewing and Changing Service Connection Properties" on page 8-28
	Update connection pool settings for a connection factory.	"Viewing and Changing Connection Pool Size Parameters" on page 8-30
	Update the list of roles authorized to obtain connections from the connection pool.	"Updating Security Policies" on page 8-43
WLS to EIS Principal Mapping	View the WebLogic Server usernames mapped to EIS usernames.	"Viewing and Changing WebLogic Server to EIS Principal Mappings" on page 8-35
	Delete entries from the list.	
	Access the WLS to EIS Principal Mapping Detail page to add or update a mapping between a WebLogic Server username and an EIS username.	
WLS to EIS Principal Mapping Detail	Add or update a mapping between a WebLogic Server username and an EIS username.	"Viewing and Changing WebLogic Server to EIS Principal Mappings" on page 8-35

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 "Viewing and Changing Application View Details" on page 8-20.

Property	Description
AppView ID	Application View ID. This is a link to the **Application View Details** page. See "Viewing and Changing Application View Details" on page 8-20. **Note:** Names of application views in the Testing state are preceded by underscore characters.
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, 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.

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 8-24.

Property	Description
ID	Adapter ID. This is a link to the **Adapter Instance Details** page. See "Viewing and Changing Adapter Instance Details" on page 8-24. **Note:** 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, 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 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 (see "Resetting the Counters" on page 8-47). To learn more about what is included in the counts, see "About the Statistics Displayed" on page 8-4.

Property	Description
Event Statistics	
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.
Last Event Count Reset Time	Time event count was last reset.
Service Statistics	
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. **Note:** The Sync Service Count is incremented when the control service method returns. If there is a rollback due to a subsequent failure, the Sync Service Count is not rolled back. If the Sync Service Count is incremented, but there is no corresponding update to the EIS, it is an indication that something downstream failed (for example, an XQuery transform) and caused the rollback.
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.

Property	Description
Async Service Error Count	Number of asynchronous service errors.
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.
Last Service Count Reset Time	Time service count was last reset.
Async Service Average Request Wait Time	Average wait time in milliseconds for asynchronous service invocations.

To view the application view instance statistics:

1. Locate the application view. See "Listing and Locating Application Views" on page 8-13.
2. Click an application view ID to display the **Application View Details** page.
3. In the Main Details section, click **Show Statistics**.

Related Topics

- "Resetting the Counters" on page 8-47
- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45
- "Viewing Adapter Instance Statistics" on page 8-17

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 (See "Resetting the Counters" on page 8-47). To learn more about what is included in the counts, see "About the Statistics Displayed" on page 8-4.

Property	Description
Adapter Instance Statistics	
ID	Adapter instance ID.
Event Statistics	
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.
Service Statistics	
Sync Service Count	Number of synchronous service invocations since the service counter was last reset. **Note:** The Sync Service Count is incremented when the control service method returns. If there is a rollback due to a subsequent failure, the Sync Service Count is not rolled back. If the Sync Service Count is incremented, but there is no corresponding update to the EIS, it is an indication that something downstream failed (for example, an XQuery transform) and caused the rollback.

Property	Description
Sync Service Error Count	Number of synchronous 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 8-14.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Show Statistics**.

Related Topics

- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45
- "Resetting the Counters" on page 8-47
- "Viewing and Changing Adapter Instance Details" on page 8-24

Viewing Connection Factory Pool Statistics for a Service Connection

The **Adapter Instance Service Connection Details** page displays the following connection factory pool statistics for a selected service connection:

- Active Connections Count
- Active Connections High Count
- Free Connections Current Count

- Free Connections High Count
- Connections Created Total
- Connections Destroyed Total
- Connections Matched Total
- Connections Rejected Total
- Connections Recycled Total

The statistics are provided by the WebLogic Server `weblogic.management.runtime.ConnectorConnectionPoolRuntimeMBean`. To learn more about the information provided by the `ConnectorConnectionPoolRuntimeMBean` interface, see the WebLogic Server Javadoc at the following URL:

http://edocs.bea.com/wls/docs81/javadocs/

To view the connection factory pool statistics for a service connection:

1. Locate the adapter instance. See "Viewing and Changing Adapter Instance Details" on page 8-24.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Edit 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 Details** page is displayed. The **Connection Factory Pool** section displays the statistics described in the preceding table.
5. Click Return to go back to the **Adapter Instance Service Connection** page.
6. Select another service connection to view, or click return to go back to the **Adapter Instance Details** page.

Viewing Dependent Application Views for an Adapter Instance

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 8-14.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Dependent Application Views**.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45
- "Redeploying an Adapter Instance" on page 8-46

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 8-13.
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 8-15.
4. To enable or disable the container-managed sign-on setting, see "Enabling or Disabling Container-Managed Sign-On" on page 8-42.

5. To enable or disable auto suspend, see "Viewing and Changing Application View Auto Suspend Settings" on page 8-32.
6. To set environment variables, see "Viewing and Changing Environment Variable Values for an Application View" on page 8-34.
7. To update the security policies, see "Updating Security Policies" on page 8-43.
8. To change the adapter used for event deliveries, see "Changing Event Connections for an Application View" on page 8-37.
9. To change the adapter used for service invocations, see "Changing Service Connections for an Application View" on page 8-38.
10. To suspend or resume the application view, see "Suspending or Resuming an Application View or Adapter Instance" on page 8-45.

The **Application View Details** page displays the following information:

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

Property	Description	
	Suspended	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.
	Resuming	The application view is in the process of returning to the deployed state from the suspended state.
	Undeploying	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.
	Testing	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. For information about testing application views, 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
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.	
	false	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.
	true	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.
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.	
	false	Auto suspend is disabled.
	true	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.
Events		
Adapter Instance	ID of the adapter instance the application view uses for event delivery.	
Event table	Entry for each event defined for the application view.	
	Event Name	Name of the event.
	Description	Description of the event.
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.	

Property	Description	
Services		
Adapter Instance	ID of the adapter instance the application view uses for service invocations.	
Service table	Entry for each service defined for the application view.	
	Service Name	Name of the service.
	Description	Description of the service.
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.	

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Resetting the Counters" on page 8-47

Viewing and Changing Adapter Instance Details

The **Adapter Instance Details** page allows you to:

- View and change auto suspend properties for an adapter instance.
- View statistics for an adapter instance.
- View the application views dependent on an adapter instance.
- 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 8-14.
   - Locate an application view (see "Listing and Locating Application Views" on page 8-13), 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 enable or disable auto suspend for the adapter instance, see "Viewing and Changing Adapter Instance Auto Suspend Settings" on page 8-33.
4. To view statistics for the adapter instance, see "Viewing Adapter Instance Statistics" on page 8-17.
5. To view a list of the application views dependent on the adapter instance, see "Viewing Dependent Application Views for an Adapter Instance" on page 8-20.
6. To view and change the properties of the adapter used for event deliveries, see "Viewing and Changing Event Connection Properties" on page 8-27.
7. To view and change the properties of the adapter used for service invocations, see "Viewing and Changing Service Connection Properties" on page 8-28.
8. To suspend or resume the adapter instance, see "Suspending or Resuming an Application View or Adapter Instance" on page 8-45.
9. To redeploy the adapter instance, see "Redeploying an Adapter Instance" on page 8-46.

The **Adapter Instance Details** page displays the following information:

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.	
	Undeployed	The adapter instance is not available for getting connections or making event deliveries.
	Deploying	The adapter instance is being prepared for getting connections or making event deliveries.
	Deployed	The adapter instance is ready for use. Events are available as the EIS produces them and getting connections is allowed.
	Deploy Failed	The adapter instance could not be deployed and is not available for use.
	Suspending	The adapter instance is in the process of being suspended.
	Suspended	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.
	Resuming	The adapter instance is in the process of returning to the deployed state from the suspended state.
	Undeploying	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 "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
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.	

Property	Description	
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 "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	
Auto Suspend Enabled	**true**	Auto suspend is enabled. The adapter instance will be suspended if WebLogic Integration determines that the EIS instance is temporarily unavailable. The adapter instance will resume automatically if WebLogic Integration determines the EIS instance is available or the auto-suspend timeout has been exceeded.
	false	Auto suspend is disabled.
Auto Suspend Timeout	How long auto suspend should last (in seconds). Valid values are from **0** to **2147483647** seconds, and **-1** to specify an infinite timeout period. The default is **1800**.	

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.

In addition to viewing and updating the adapter-specific event properties, you can also define event generation targets (a list of the managed servers on which the event generator for an adapter instance is to be started). To learn more, see "Changing Event Generation Targets" on page 8-39.

To view and change event connection properties:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Edit Event Connection**.
4. Enter new settings for one or more event properties, as necessary.

5. Do one of the following:
   - To update the event connection properties, click **Submit**.
   - To reset to the last saved values, click **Reset**.
   - 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 8-46.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Changing Event Connections for an Application View" on page 8-37
- "Viewing and Changing Service Connection Properties" on page 8-28
- "Changing Event Generation Targets" on page 8-39

Viewing and Changing Service Connection Properties

The **Adapter Instance Service Connection Details** 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.

Note: The **JdbcDbType** property is a legacy field that is no longer used.

In addition to the adapter-specific service properties, you can also:

- Update connection pool properties for the service connection. See "Viewing and Changing Connection Pool Size Parameters" on page 8-30.
- Update roles authorized to access the service connection. See "Updating Security Policies" on page 8-43.
- View connection factory pool statistics for the service connection. See "Viewing Connection Factory Pool Statistics for a Service Connection" on page 8-18.

To view and change service connection properties:

1. Locate the adapter instance. See "Viewing and Changing Adapter Instance Details" on page 8-24.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Edit 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 Details** page is displayed. For additional information about the statistics displayed in the **Connection Factory Pool Statistics** section, see "Viewing Connection Factory Pool Statistics for a Service Connection" on page 8-18.
5. Click **Edit Properties**.

   The **Edit Adapter Instance Service Connection Details** page is displayed.
6. Enter new settings for one or more service properties, as necessary.

   For additional information about updating the security policies or connection pool size parameters, see "Viewing and Changing Connection Pool Size Parameters" on page 8-30 or "Updating Security Policies" on page 8-43.
7. 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 8-46.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Changing Service Connections for an Application View" on page 8-38
- "Viewing and Changing Event Connection Properties" on page 8-27
- "Viewing Dependent Application Views for an Adapter Instance" on page 8-20

Viewing and Changing Connection Pool Size Parameters

The **Adapter Instance Service Connection Details** 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 **Min Pool Size** field, enter the minimum number of connections.	Minimum connection pool size for the connection factory. Valid values are from **0** to **2147483647**. The default is **1**.	Required
In the **Max Pool Size** 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 **1** to **2147483647**. The default is **10**.	Required
Click the **Allow Pool to Shrink** check box to enable or disable this option.	With **Allow Pool to Shrink** 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 8-14.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Edit 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 Details** page is displayed.

5. Click **Edit Properties**.

   The **Edit Adapter Instance Service Connection Details** page is displayed.

6. Configure the settings as described in the preceding table.

7. 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 8-46.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Viewing and Changing Service Connection Properties" on page 8-28
- "Changing Service Connections for an Application View" on page 8-38
- "Viewing Dependent Application Views for an Adapter Instance" on page 8-20

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 settings are available.

Setting	Description	Required/ Optional
Click the **Auto Suspend** 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 **Auto Suspend Timeout** field, enter the number of seconds.	How long auto suspend should last. Valid values are from **0** to **2147483647** seconds, and **-1** to specify an infinite timeout period. The default is **1800**.	Required
In the **Suspended Request Retry Interval** field, enter the number of seconds.	How long to wait before retrying a suspended request. Valid values are from **0** to **2147483647** seconds. The default is **3**.	Required

To view and change application view auto suspend settings:

1. Locate the application view. See "Listing and Locating Application Views" on page 8-13.
2. Click the application view ID to display the **Application View Details** page.
3. To the right of **Auto Suspend Enabled**, 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**.

Related Topics

- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45
- "Viewing and Changing Adapter Instance Auto Suspend Settings" on page 8-33

Viewing and Changing Adapter Instance Auto Suspend Settings

The **Adapter Instance Auto Suspend Settings** page allows you to enable or disable auto suspend, and to update the auto suspend timeout for an adapter instance. The following settings are available.

Setting	Description	Required/ Optional
Click the **Auto Suspend Enabled** check box to enable or disable auto suspend.	With auto suspend enabled, the adapter instance will be suspended if WebLogic Integration determines that the EIS instance is temporarily unavailable. The adapter instance will resume automatically if WebLogic Integration determines the EIS instance is available or the auto-suspend timeout has been exceeded.	Required
In the **Auto Suspend Timeout** field, enter the number of seconds.	How long auto suspend should last. Valid values are from **0** to **2147483647** seconds, and **-1** to specify an infinite timeout period. The default is **1800**.	Required

To change application view auto suspend settings:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
2. Click the application view ID to display the **Adapter Instance Details** page.
3. Click **Change Settings** to display the **Adapter Instance Auto Suspend Settings** page.

4. Configure the settings as described in the preceding table.
5. To update the settings, click **Submit**.

Related Topics

- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45
- "Viewing and Changing Application View Auto Suspend Settings" on page 8-32

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. To learn more 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 8-13.
2. Click the application view ID to display the **Application View Details** page.
3. In the Main Details section, 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 8-46. 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 Adminstration Console Online Help*, which is available at the following URL:

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

Related Topics

- "Viewing and Changing Application View Details" on page 8-20

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 8-13.
2. Click the adapter instance ID to display the **Adapter Instance Details** page.

3. Click **Edit 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 Details** 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 a WebLogic Server to EIS principal mapping 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 clear the fields, click **Reset**.
   - To disregard the mapping, click **Cancel**.

To edit a WebLogic Server to EIS principal mapping for a service connection:

1. On the **WLS to EIS Principal Mapping** page, click the WLS name for the entry.

   The **WLS to EIS Principal Mapping Detail** page for the entry is displayed.
2. Edit the entry as required.
3. Do one of the following:
   - To save changes, click **Submit**.

- To reset to original values, click **Reset**.
- To disregard changes, click **Cancel**.

Related Topics

- "Enabling or Disabling Container-Managed Sign-On" on page 8-42
- "Updating Security Policies" on page 8-43

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 8-13.
2. Click the application view ID to display the **Application View Details** page.
3. In the **Events** section, click **Change Event Connection** to display the **Application View Event Connection** page.
4. Select an event connection by clicking the option button to the right of the adapter ID.
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 Adminstration Console Online Help*, which is available at the following URL:

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

Related Topics

- "Viewing and Changing Application View Details" on page 8-20

- "Viewing and Changing Event Connection Properties" on page 8-27

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 8-13.
2. Click the application view ID to display the **Application View Details** page.
3. In the **Services** section, click **Change Service Connection** to display the **Application View Service Connection** page.
4. Select a service connection by clicking the option button to the right of the adapter ID.
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 Adminstration Console Online Help*, which is available at the following URL:

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

Related Topics

- "Viewing and Changing Application View Details" on page 8-20
- "Viewing and Changing Service Connection Properties" on page 8-28
- "Changing Event Connections for an Application View" on page 8-37

Changing Event Generation Targets

Application Integration event generators work with event routers and resource adapters to 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.

To learn more about event processing in application integration, see "Processing Event Notifications at Run-Time" in Understanding Application Integration in *Introducing Application Integration*.

The following sections describe basic and advanced event generation targeting, and provide instructions for changing the event generation targets.

Basic Event Generation Targeting

In a single node environment, adapter instance events are triggered on the single node by default; there is no need to specify the target in the **Event Generation Targets** field on the **Adapter Instance Event Connection** page.

In a clustered environment, events are not triggered on any node by default. You must specify one or more targets in the **Event Generation Targets** field on the **Adapter Instance Event Connection** page. In basic targeting, the target servers for the event connection are specified as a comma separated list as follows:

```
servername,servername,servername,...
```

If an adapter provides event generator instance support, more advanced event generation targeting is available. With event generator instance support, event connections can define logical event generator instances that allow system administrators to control the distribution of event generation work within a WebLogic Server cluster. The following section describes the how advanced event generation targeting can be used to improve load balancing and fault tolerance.

Advanced Event Generation Targeting

Some adapters, such as the DBMS sample adapter, provide event generator instance support. This allows for finer control over event generator instance targeting when multiple instances of a event connection are processing events in a cluster. The general syntax for specifying targets in the **Event Generation Targets** field on the **Adapter Instance Event Connection** page is as follows:

```
servername=[instance_specifier instance_specifier ...],servername=[instanc
e_specifier instance_specifier ...],...
```

Here, `instance_specifier` is an adapter-specific instance specifier.

For example, for the DBMS sample adapter:

instance_specifier=instance_id/number_of_instances

Here,

- *instance_id* is a numeric identifier for the DBMS sample event generator instance. Valid values are any integer from 1 to the *number_of_instances*.
- *number_of_instances* is the total number of DBMS sample event generator instances in the cluster. Depending upon how the instances are deployed, the total number of instances can be greater than or less than the number of nodes in the cluster.

For example, you might enter the following in the **Event Generation Targets** field for a DBMS sample adapter instance:

```
myserver1=[1/4],myserver2=[2/4],myserver3=[3/4],myserver4=[4/4]
```

Here, 1/4 (instance 1 of 4), 2/4 (instance 2 of 4), and so on, each represent an *instance_specifier* in the format required by the DBMS adapter.

With event generator instance support, if a managed server in your cluster fails, you can move an event generator instance from the failed server to a live server—potentially configuring multiple instances to operate on a single live server. For example, continuing the preceding DBMS adapter example, suppose myserver2 fails. The following target specification would move the load to myserver1:

```
myserver1=[1/4 2/4],myserver3=[3/4],myserver4=[4/4]
```

In this case, the event connection on myserver1 consumes events destined for instance 1 of 4 and instance 2 of 4. The event connection on myserver3 consumes events destined only for instance 3 of 4. When myserver2 is back in operation, you could return to the original configuration.

Note: Although the definition for *instance_specifier* is adapter-specific, the list of instances is always enclosed in square brackets [], and each instance is separated from the others by one more space characters.

A description of how event generator instance support is provided in the DBMS sample adapter can be found in "Step 3e: Implement Event Generator Instance Support" in Developing an Event Adapter in *Developing Adapters*.

To learn more about application integration event generation targeting, load balancing, and error handling, see the following sections of *Deploying WebLogic Integration Solutions*:

- "Events" section of "Application Integration Capabilities and Clients" in Introduction
- "Events" section of "Load Balancing Application Integration Functions in a Cluster" in Understanding WebLogic Integration Clusters.
- "Deploying Event Generators" in Understanding WebLogic Integration Clusters.

To change event generation targets:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
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 field, enter a comma-separated list of server names using the following syntax:

     ```
     servername,servername,servername,...
     ```

     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 the mapping for servers and event generator instances using the following syntax:

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

     ```
     servername=[instance_specifier instance_specifier ...],servername=[i
     nstance_specifier instance_specifier ...],...
     ```

     Here:

     servername is the name of a server whose event connection you want to target,

     instance_specifier is adapter-specific instance specifier for the instance whose events you want to target to the specified server. See "Advanced Event Generation Targeting" on page 8-39.

5. Do one of the following:
   - To update event targets, click **Submit**.
   - To reset to original values, click **Reset**.
   - 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 8-46.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Viewing and Changing Event Connection Properties" on page 8-27
- "Changing Event Connections for an Application View" on page 8-37
- "Viewing Dependent Application Views for an Adapter Instance" on page 8-20

Enabling or Disabling Container-Managed Sign-On

The **Application View Container Managed Signon Settings** page allows you to enable or disable container-managed sign-on for an application view.

In order for the container managed sign-on setting to take affect, you must redeploy the application using the WebLogic Server Administration Console. If security policy settings are not edited and deployed in the correct order, application view security policy settings may be lost when the application is redeployed.

To learn more about container-managed sign-on, see "Managing Application Integration Security" on page 8-7.

To change the container-managed sign-on setting:

1. Locate the application view. See "Listing and Locating Application Views" on page 8-13.
2. Click the application view ID to display the **Application View Details** page.
3. To the right of **Container Managed Sign-On Enabled**, click **Change Settings**.

   The **Application View Container Managed Signon Settings** page is displayed.

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**.
6. When you change the container-managed sign-on setting, you must perform the following tasks so that the container managed sign-on setting takes affect:
   a. Redeploy the application using the WebLogic Server Administration Console.
   b. Edit the security policy for the application view using the WebLogic Integration Administration Console.

Note: 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 Adminstration Console Online Help*, which is available at the following URL:

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

Related Topics

- "Viewing and Changing Application View Details" on page 8-20
- "Viewing and Changing WebLogic Server to EIS Principal Mappings" on page 8-35

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 Details** page allows you to specify a list of roles that can obtain service connections from the connection factory for an adapter instance.

Note: If an authenticator that implements the required MBeans is not configured, the options for configuring the security policies for applications views and adapter instances are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

To view security policies for an application view:

1. Locate the application view. See "Listing and Locating Application Views" on page 8-13.

2. Click the application view ID to display the **Application View Details** page.
3. In the Main Details section, click **Set Security Policy** to display the **Application View Security** page.
4. To update, see "To update security policies," below.

To view security policies for an adapter instance:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
2. Click the adapter instance ID to display the **Adapter Instance Details** page.
3. Click **Edit 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 Details** page is displayed.
5. At the bottom of the page, click **Edit Properties**.

   The **Edit Adapter Instance Service Connection Details** page is displayed. You set authorized roles in the **Security Policy** section at the bottom of the page.
6. To update, see "To update security policies," below.

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**.

Related Topics

- "Viewing and Changing WebLogic Server to EIS Principal Mappings" on page 8-35
- "Enabling or Disabling Container-Managed Sign-On" on page 8-42

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 as described in "Suspending, Resuming, and Redeploying Application Views and Adapter Instances" on page 8-6.

To suspend or resume an application view instance:

1. Locate the application view. See "Listing and Locating Application Views" on page 8-13.
2. Click the application view name to display the **Application View Details** page.
3. Click **Suspend Application View** or **Resume Application View**, as required.

To suspend or resume an adapter instance:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
2. Click the adapter ID to display the **Adapters Instance Details** page.
3. Click **Suspend Adapter Instance** or **Resume Adapter Instance**, 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.

Related Topics

- "Viewing and Changing Application View Details" on page 8-20
- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Viewing Dependent Application Views for an Adapter Instance" on page 8-20

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.

Note: You can also use the redeploy function to deploy an adapter that is currently in the undeployed state.

To redeploy an adapter instance:

1. Locate the adapter instance. See "Listing and Locating Adapter Instances" on page 8-14.
2. Click an adapter ID to display the **Adapter Instance Details** page.
3. Click **Redeploy**. A dialog box displays the following message:

This action will redeploy all application views dependent on this adapter instance. Do you wish to proceed?

4. Do one of the following:
   - Click **OK** to proceed and redeploy the adapter and the application views dependent on the adapter instance.

     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.
   - Click **Cancel** to return to the **Adapter Instance Details** page without redeploying. The adapter continues to operate without applying changes to its configuration.
   - To view the application views dependent on the adapter before redeploying, click **Cancel**, then see "Viewing Dependent Application Views for an Adapter Instance" on page 8-20.

Related Topics

- "Viewing and Changing Adapter Instance Details" on page 8-24
- "Viewing Dependent Application Views for an Adapter Instance" on page 8-20
- "Suspending or Resuming an Application View or Adapter Instance" on page 8-45

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 A**pplication View Summary page** as described in "Listing and Locating Application Views" on page 8-13.
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 8-13.
2. Do one or both of the following:
   - Click **Reset Event Count**.
   - Click **Reset Service Count**.

Related Topics

- "Viewing and Changing Application View Details" on page 8-20
- "Viewing Application View Instance Statistics" on page 8-15
- "Viewing Adapter Instance Statistics" on page 8-17

CHAPTER 9

Trading Partner Management

The *Trading Partner Management* module allows you 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 11-3.

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

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 TPM Schema in *Managing WebLogic Integration Solutions.*
- How trading partner management data is used to support business transactions, see *Introducing Trading Partner Integration*.
- Building RosettaNet and ebXML solutions, see *Tutorials for Trading Partner Integration*.

- Building participant processes for ebXML or RosettaNet, see the Building ebXML Participant Business Processes or Building RosettaNet Participant Business Processes topic in *Building Integration Applications* in the WebLogic Workshop help.
- Security in Trading Partner Integration, see:
  - Using WebLogic Integration Security in *Deploying WebLogic Integration Solutions*.
  - Example: ebXML Security Configuration and Example: RosettaNet Security Configuration in *Introducing Trading Partner Integration*.
- Trading partner integration controls, see TPM Control, RosettaNet Control, and ebXML Control in *Building Integration Applications* in the WebLogic Workshop help.
- WebLogic Integration – Business Connect, the lightweight trading partner software for WebLogic Integration, see the WebLogic Integration – Business Connect documentation.

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 help topics associated with each are provided.

Page	Associated Tasks	Help 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 Trading Partner Management from the navigation bar.	"Trading Partner Management" on page 9-1

Page	Associated Tasks	Help Topics
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 9-44
	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 9-78
	Enable or disable the trading partner profile.	"Enabling and Disabling Trading Partner and Service Profiles" on page 9-70
Add a New Trading Partner	Add a trading partner.	"Adding Trading Partner Profiles" on page 9-13
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.	"Viewing and Changing Trading Partner Profiles" on page 9-47
	View summary information for the protocol bindings associated with the trading partner. Add a new binding or select a binding for edit.	"Viewing and Changing Bindings" on page 9-52
	View summary information for the certificates associated with the trading partner. Add a new certificate or select a certificate for edit.	"Viewing and Changing Certificates" on page 9-50
	View summary information for a custom extension. Update the existing custom extension, or add a new custom extension if one does not exist.	"Viewing and Changing a Custom Extension" on page 9-64
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.	"Viewing and Changing Trading Partner Profiles" on page 9-47

Page	Associated Tasks	Help Topics
Profile Management: Bindings		
Add Binding	Add a new protocol binding to the selected trading partner.	"Adding Protocol Bindings to a Trading Partner" on page 9-18
View Binding Details	View the properties of a binding.	"Viewing and Changing Bindings" on page 9-52
Edit Binding	Edit the properties of a binding.	"Viewing and Changing Bindings" on page 9-52
Profile Management: Certificates		
Add Certificate	Add a new certificate to the selected trading partner.	"Adding Certificates to a Trading Partner" on page 9-14
View and Edit Trading Partner Certificate	View the properties of a certificate or update a certificate.	"Viewing and Changing Certificates" on page 9-50
Edit Certificate	Update a certificate by importing certificate files.	"Viewing and Changing Certificates" on page 9-50
Profile Management: Custom Extension		
Add Custom Extension	Add custom properties to the trading partner.	"Adding a Custom Extension to a Trading Partner" on page 9-19
View and Edit Custom Extension	View the custom properties for a trading partner.	"Viewing and Changing a Custom Extension" on page 9-64
Edit Custom Extension	Change the custom properties for a trading partner.	"Viewing and Changing a Custom Extension" on page 9-64

Page	Associated Tasks	Help Topics
Service Management: Services		
View and Edit Services	View a list of services. Service name, business service name, description, type, business protocol, and description are displayed.	"Viewing and Changing Services" on page 9-65
	Filter the list by service name. Use ? to match any single character or * to match zero or more characters.	
	Delete a service.	"Deleting Services" on page 9-81
Add Service	Add a service definition for a newly deployed service. Assign the name, type, and business protocol. Optionally assign a description.	"Adding Services" on page 9-21
View and Edit Service Details	View service properties. The type, business protocol, description, version, and associated service profiles are displayed.	"Viewing and Changing Services" on page 9-65
	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.	"Viewing and Changing Services" on page 9-65
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.	"Adding Service Profiles to a Service" on page 9-23
View Service Profile	View the properties of a service profile.	"Viewing and Changing Service Profiles" on page 9-68
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.	"Viewing and Changing Service Profiles" on page 9-68
Add Authentication	Add authentication to a service profile.	"Adding Authentication to a Service Profile" on page 9-25

Page	Associated Tasks	Help Topics
Message Tracking		
View Messages	View the list of messages. Event ID, time of event, direction (inbound or outbound), and status are displayed.	"Monitoring Messages" on page 9-84
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.	"Filtering the Messages Displayed" on page 9-85
Message Details	View message properties and link to detail, such as header, status, or message part data.	"Filtering the Messages Displayed" on page 9-85
Import/Export		
Import Trading Partner Management Data	Select a trading partner management file for import, and set the import properties.	"Importing Management Data" on page 9-73
Export Trading Partner Management Data	Select trading partners and services for export, and set the export properties.	"Exporting Management Data" on page 9-75
Bulk Delete	Select trading partner profiles and services to delete and set the delete properties.	"Deleting Trading Partner Profiles and Services Using Bulk Delete" on page 9-77
Statistics		
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.	"Viewing Statistics" on page 9-82

Page	Associated Tasks	Help Topics
Configuration		
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.	"Configuring the Mode and Message Tracking" on page 9-10
	Set the trading partner integration mode (test or production).	
Proxy Configuration	Configure a proxy host.	"Configuring a Proxy Host" on page 9-11
Audit Log Configuration	Enable or disable secure audit logging. If enabled, specify the secure audit logging class.	"Configuring Secure Audit Logging" on page 9-11
Secure Timestamp Configuration	Specify the Java class used for secure time stamping.	"Configuring Secure Audit Logging" on page 9-11
Refresh Keystore	Refresh the KeyStores (identity and trust) in memory from the disk.	"Refreshing the Keystore" on page 9-12
Certificate Verification Provider	Specify the certificate verification provider.	"Specifying the Certificate Verification Provider" on page 9-13

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 9-10
- "Configuring a Proxy Host" on page 9-11
- "Configuring Secure Audit Logging" on page 9-11
- "Refreshing the Keystore" on page 9-12
- "Specifying the Certificate Verification Provider" on page 9-13

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 **Message Tracking Level** drop-down list, select **All**, **Metadata**, or **None**.	The default message tracking level for trading partner integration. If the tracking level for a service profile is set to **Default** (see "Adding Service Profiles to a Service" on page 9-23), the tracking level for the service profile defaults to the setting specified here. The options are: **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. **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 or history is stored in repository and no information is available for view in the Message Tracking module of the console.	Required
From the **Mode** drop-down list, select **Test** or **Production**.	The trading partner integration mode. In **Test** 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

Setting	Description	Required/ Optional
In the **Directory** field, enter the path.	The path to a directory used to store messages.	Required if **Trace Raw Message** is set to **Yes**.
Select the **Trace Raw Messages Yes** or **No** option button.	When set to **Yes**, 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**.

   The **Secure Timestamp Configuration** page is displayed.
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 to 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 9-31 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 9-14.
   - To add bindings to the trading partner, see "Adding Protocol Bindings to a Trading Partner" on page 9-18.
   - To add a custom extension to the trading partner, see "Adding a Custom Extension to a Trading Partner" on page 9-19.

Related Topics

- "Adding Certificates to a Trading Partner" on page 9-14
- "Adding Protocol Bindings to a Trading Partner" on page 9-18
- "Adding a Custom Extension to a Trading Partner" on page 9-19
- "Adding Service Profiles to a Service" on page 9-23
- "Viewing and Changing Trading Partner Profiles" on page 9-47
- "Importing Management Data" on page 9-73
- "Listing and Locating Trading Partners" on page 9-44

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 **Add Certificate** link to the right 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 9-44, 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.

   The Add Certificate (Step 1 of 2) page is displayed.
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 9-15
   - "Creating and Importing the Files for a Certificate" on page 9-16
   - "Creating a Reference to an Existing Certificate" on page 9-18

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 10-6.

   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 identity 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. If you are importing a certificate for a local trading partner, select the alias for the password associated with the keystore entry from the **Password Alias** drop-down list. This alias is used to retrieve the required password from the password store. See "Password Aliases and the Password Store" on page 10-6.

   Note: This step only applies if you are importing a certificate for a local trading partner.

   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 10-6.

   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 **Add**.

   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 9-44, 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.

The **Add Binding (Step 1 of 2)** page is displayed.

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 9-33 for a description of the available settings.
6. Click **Add Binding**.

   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 9-60.
   - A RosettaNet 1.1 or 2.0 binding, you can configure the notification of failure roles as described in "Configuring PIP Notification of Failure Roles for RosettaNet Bindings" on page 9-62.

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”>
              <myxmlelement>
                     <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>
              </myxmlelement>
       </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 9-73.

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 9-44, 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.

   The **Add Custom Extension** page is displayed.

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 9-20 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.

Related Topics

- "Adding Trading Partner Profiles" on page 9-13
- "Importing Management Data" on page 9-73

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 **Add Service.**

   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 9-23.
9. If the Business Protocol is **ROSETTANET**, you can define the RosettaNet service defaults as described in the following section.

Adding Defaults to a RosettaNet Service

Once you have created a the service definition for a RosettaNet service, you can add service defaults from the **View and Edit Service Details** page.

To add RosettaNet Service Defaults:

1. Locate the service as described in "Listing and Locating Services" on page 9-46.
2. Click the service name to select it.

   The **View and Edit Service Details** page is displayed.
3. Click Add Defaults.
4. Define the defaults as required. The following table describes the available settings.

Service Content Schema Location	Location of the schemas on the file system You must enter a valid path.	
Use DTD for Validation	**True**	Use DTD over schemas for validating documents received and sent.
	False	Do not use DTD for validation.
Validate Service Content	**True**	Validate service content for each message
	False	No validation is performed. Selecting **False** improves performance.
Validate Service Header	**True**	Validate service header for each message
	False	No validation is performed. Selecting **False** improves performance.

5. Click **Set Defaults** to save the settings and return to the **View and Edit Service Details** page.

Related Topics

- "Listing and Locating Services" on page 9-46

Adding Service Profiles to a Service

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

To add service profiles to a service:

1. Locate the service as described in "Listing and Locating Services" on page 9-46.
2. Click the service name to select it.

   The **View and Edit Service Details** page is displayed.
3. Click the **Add Service Profile** button.

   The **Add Service Profile** page is displayed.
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 9-10.
- **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 9-25.
   - Click **No**. You can configure authentication later as described in "Adding Authentication to a Service Profile" on page 9-25.

   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 9-58.

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	**Client Trading Partner:** RemoteTP	**Client Trading Partner:** LocalTP **Username and Password Alias:** RemoteTP username and password (the password alias for the password is specified). The username and password required to access the RemoteTP transport endpoint.
HTTPS	One-Way	**Client Trading Partner:** RemoteTP	**Client Trading Partner:** LocalTP **Server Certificate:** RemoteTP server certificate to be used for SSL authentication.
	One-Way with Basic	**Client Trading Partner:** RemoteTP	**Client Trading Partner:** LocalTP **Username and Password Alias:** RemoteTP username and password (the password alias for the password is specified). The username and password required to access the RemoteTP transport endpoint. **Server Certificate:** RemoteTP server certificate to be used for SSL authentication.
	Mutual	**Client Trading Partner:** RemoteTP **Client Certificate:** RemoteTP client certificate to be used for SSL mutual authentication.	**Client Trading Partner:** LocalTP **Client Certificate:** LocalTP client certificate to be used for SSL mutual authentication. **Server Certificate:** RemoteTP server certificate to be used for SSL authentication.

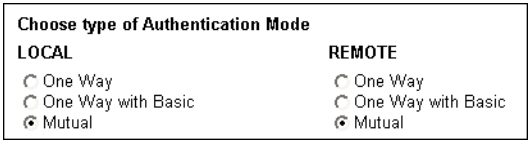
To add HTTPS authentication to a service profile:

1. Locate the service as described in "Listing and Locating Services" on page 9-46.
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:



   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 **Server Certificate** from the drop-down list.
One-Way with Basic	Enter the **Username** required to access the remote endpoint. Select the **Password Alias** from the drop-down list.	Select the **Server Certificate** from the drop-down list.
Mutual	Select the **Client Certificate** from the drop-down list.	Select the **Client Certificate** from the drop-down list. Select the **Server Certificate** 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 9-14 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 10-15 for instructions. Once the alias has been added, it is available for selection.

9. To preview to the configuration, click **Preview config**. To learn more about the preview function, see "Previewing the Authentication Configuration:" on page 9-29.
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 9-46.
2. Click the service name to select it.

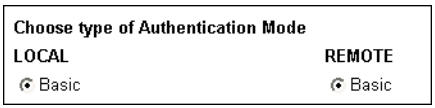
   The **View and Edit Service Details** page is displayed.

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:



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 10-15 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 9-29.

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
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	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
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	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 ----->

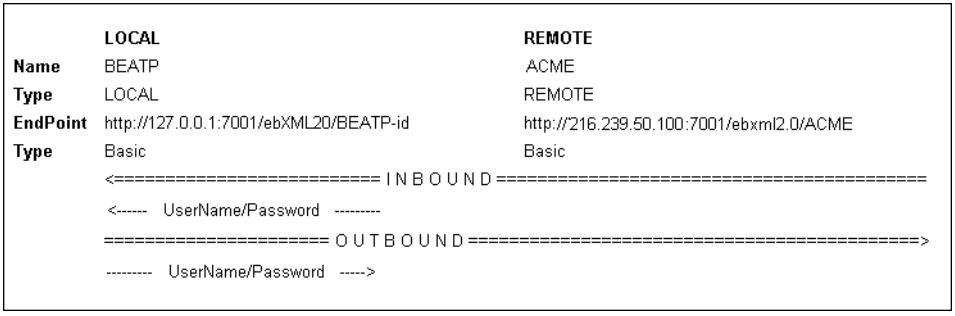
<------ Client Cert (ACME-client) ---------

========== 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 **Name** field, enter the name.	The name used to identify the trading partner within the system. Do not use spaces. **Note:** This field is only available on the **Add Trading Partner Profile** page. It cannot be edited on the **Edit Trading Partner Profile** page.	Required
In the **Description** field, enter a description.	An optional description. This value is for administrative purposes only. It is not included in messages.	Optional
In the **Business ID** field, enter an appropriate identifier.	Identifier for the trading partner. The value is used to identify the partner in message exchanges.	Required
In the **Business ID Type** field, enter the type of **Business ID**.	The type or naming convention for the **Business ID**. For example, if the value entered for **Business ID** is a D-U-N-S number, enter **DUNS** for the **Business ID Type**.	Optional

Setting	Description	Required/ Optional
Check or uncheck the **Default Trading Partner** check box.	When checked, the trading partner is designated the default trading partner for sending or receiving messages for the local host system. **Default Trading Partner** can only be checked if **Type** is set to **LOCAL**. Only one **LOCAL** trading partner can be designated the default. The default is unchecked.	Optional
From the **Type** drop-down list, select **LOCAL** or **REMOTE**.	Specifies whether the trading partner is hosted locally or represents an external, remote trading partner. The default is **LOCAL**.	Optional
From the **Status** drop-down list, select **ENABLED** or **DISABLED**.	Specifies whether or not to allow business messages to be sent or received by the partner You cannot set the **Status** to **DISABLED** until all service profiles associated with the partner are disabled. If you attempt to set the **Status** to **DISABLED**, you are prompted to disable any enabled service profiles before the change takes effect. Setting the **Status** to **ENABLED** 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 "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70. The default is **ENABLED**.	Optional
In the **Email** field, enter an email address.	A contact email address for the trading partner.	Optional
In the **Address** field, enter a mailing address.	A mailing address for the trading partner.	Optional
In the **Phone** field, enter a telephone number.	A contact telephone number for the trading partner.	Optional

Setting	Description	Required/ Optional
In the **Fax** field, enter a fax number.	A fax number for the trading partner.	Optional
In the **WLS User Name** 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 "Listing and Locating Users" on page 11-17. The value applies only if **Type** is set to **Remote**.	Optional

Related Topics

- "Adding Trading Partner Profiles" on page 9-13
- "Viewing and Changing Trading Partner Profiles" on page 9-47

Defining Protocol Bindings

The **Add Binding and Edit Binding** pages allow you to define the properties for a protocol binding. The following sections describe the available settings for each protocol type and a special case regarding Trading Partner Endpoint definition:

- Defining an ebXML 1.0 or 2.0 Binding
- Defining a RosettaNet 1.1 or 2.0 Binding
- Defining a Web Service Binding
- Defining Endpoints for Projects Containing Multiple JPDs Having the Same Name

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.

Note: When exchanging ebXML messages with a trading partner that uses WebLogic Integration - Business Connect, you can only use one version of ebXML Message Service protocol (either ebXML 1.0 or ebXML 2.0). WebLogic Integration - Business Connect uses the same HTTP endpoint for a given trading partner regardless of the ebXML version. You cannot configure more than one protocol binding for a given partner in WebLogic Integration that uses the same HTTP endpoint.

Setting	Description	Required/ Optional

In the **Name** field, enter the binding name.	The name used to identify the binding within the system. The name must be unique within the trading partner profile. When you add a new binding, a default name is automatically generated using the following convention:
	`<partner>-<protocol>-<qualifier>`
	For example:
	`acme-ebxml20-4`
	If you choose to change the default name, make sure the name you choose is unique.
	Note: This field is only available on the **Add Binding** page. It cannot be edited on the **Edit Binding** page.
		Required

Check or uncheck the **Default Binding** check box.	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. The default is unchecked.	Optional
Transport Configuration		
From the **Transport Protocol** drop-down list, select the **HTTP** or **HTTPS**.	The transport protocol for sending and receiving messages. The default is **HTTP**.	Optional
From the **Transport Protocol Version**, select the version.	The version of the transport protocol. If **HTTP** is selected for the Transport Protocol, select **1.0** or **1.1**. The default is **1.0**. If **HTTPS** is selected for Transport Protocol, **1.1** is currently the only option.	Optional
In the **Endpoint** field, enter the **URL** for the transport endpoint.	The URL or URI for the transport endpoint. For information about specifying an endpoint as a URI, see "Defining Endpoints for Projects Containing Multiple JPDs Having the Same Name" on page 9-44.	Required

Setting	Description	Required/ Optional
In the **Timeout** field, enter the transport timeout.	The transport timeout for the specified Endpoint. The default value is **0**, which indicates **no timeout**.	Optional
Quality of Service		
From the **Delivery Semantics** drop-down list, do one of the following: • For **ebXML 1.0**, select **BESTEFFORT** or **ONCEANDONLYONCE** • For **ebXML 2.0**, select **BESTEFFORT**, **ONCEANDONLYONCE**, **ATLEASTONCE**, or **ATMOSTONCE**	The reliable message service behavior: **BESTEFFORT** Best effort. No reliable messaging. **ONCEANDONLYONCE** Once and only once reliable messaging. Select this option for messaging that requires acknowledgement and duplicate elimination. **ATLEASTONCE** At least once reliable messaging. Select this option for messaging that requires acknowledgement, but not duplicate elimination. **ATMOSTONCE** At most once reliable messaging. Select this option for messaging that requires duplicate elimination, but not acknowledgement.	Required
In the **Retry Count** field, enter the number of retries.	The maximum number of retries for sending a reliably delivered message. The default is **0**. The value is ignored if **BESTEFFORT** or **ATMOSTONCE** is selected for **Delivery Semantics**. If **ONCEANDONLYONCE** or **ATLEASTONCE** is selected, the message is retried until the acknowledgement is received or the number of retries specified in the **Retry Count** field is exhausted.	Required if **ONCEANDONLYONCE** or **ATLEASTONCE** is selected,

Setting	Description	Required/ Optional
In the **Retry Interval** field, enter the interval.	The time interval before a message is resent following a timeout waiting for a message acknowledgement. The following are examples of 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 Any combination of the above are also valid. For example: 1 d 5 h 1 sec 500 ms The default is **1 min**.	Required if **Retry Count** is 1 or greater.
In the **Persist Duration**, enter the interval.	Specifies the duration for which messages have to be stored persistently for the purpose of duplicate elimination. The following are examples of 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 Any combination of the above are also valid. For example: 1 d 5 h 1 sec 500 ms The default is **0**.	Required if **ONCEANDONLYONCE** or **ATMOSTONCE** is selected,

Note: When defining an ebXML binding for a local trading partner, set the values for **Retry Count**, **Retry Interval**, and **Persist Duration** to the same values as the remote trading partner.

Setting	Description	Required/ Optional
XML Digital Signature Configuration for Non-Repudiation		
From the **Signature Certificate** drop-down list, select an existing certificate or **NONE**. If you have not yet added the certificate, click **Add certificate** and follow the instructions in "Adding Certificates to a Trading Partner" on page 9-14.	The name of the signature certificate used to digitally sign messages. **NONE** indicates no digital signature.	Optional
Check or uncheck the **Signature Required** check box.	When checked, the message is digitally signed using the signature certificate of the trading partner sending the message. The default is unchecked. Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See "Configuring Secure Audit Logging" on page 9-11.	Optional
Check or uncheck the **Signature Receipt Required** check box.	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. Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See "Configuring Secure Audit Logging" on page 9-11.	Optional

Note: Within WebLogic Integration, 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. In addition to the preceding properties:

- 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 *Deploying WebLogic Integration Solutions*.
- Optional XPath filtering transforms can be applied to messages for signing purposes. See "Configuring Signature Transforms for ebXML Bindings" on page 9-60.

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 **Name** field, enter the binding name.	The name used to identify the binding within the system. The name must be unique within the trading partner profile. When you add a new binding, a default name is automatically generated using the following convention:
	`<partner>-<protocol>-<qualifier>`
	For example:
	`acme-rosettanet20-4`
	If you choose to change the default name, make sure the name you choose is unique.
	Note: This field is only available on the **Add Binding** page. It cannot be edited on the **Edit Binding** page.
		Required

Check or uncheck the **Default Binding** 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
Transport Configuration		
From the **Transport Protocol** drop-down list, select the **HTTP** or **HTTPS**.	The transport protocol for sending and receiving messages.	Required
From the **Transport Protocol Version**, select the version.	The version of the transport protocol. If **HTTP** is selected for the Transport Protocol, select **1.0** or **1.1**. If **HTTPS** is selected for Transport Protocol, **1.1** is currently the only option.	Required
In the **Endpoint** field, enter the **URL** for the transport endpoint.	The URL or URI for the transport endpoint. For information about specifying an endpoint as a URI, see "Defining Endpoints for Projects Containing Multiple JPDs Having the Same Name" on page 9-44.	Required

Setting	Description	Required/ Optional
In the **Timeout** field, enter the transport timeout.	The transport timeout for the specified endpoint. The default value is **0**, which indicates **no timeout**.	Required
Quality of Service		
In the **Retry Count** field, enter the number of retries.	The number of times a RosettaNet message should be retried in case of failure. The default is **0**.	Required
In the **Retry Interval** field, enter the interval.	The amount of time to wait between subsequent retries. The default is **1 min**. 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 Any combination of the above are also valid. For example: 1 d 5 h 1 sec 500 ms The default is 60 seconds.	Required for if **Retry Count** is 1 or greater.
In the **Process Timeout**, enter the interval.	Specifies the amount of time a PIP can be active without completion before timing out. The default is **0**.	Optional
Note: The values specified for **Retry Count**, **Retry Interval**, and **Process Timeout** are not directly enforced by the RosettaNet messaging runtime. These values can be accessed from a business process that implements a RosettaNet process.		

Setting	Description	Required/ Optional
Message-Level Encryption (RosettaNet 2.0 Only)		
From the **Encryption Certificate** drop-down list, select an existing certificate or **NONE**. If you have not yet added the certificate, click **Add certificate** and follow the instructions in "Adding Certificates to a Trading Partner" on page 9-14.	The name of the encryption certificate used to encrypt and decrypt messages. **NONE** indicates no message-level encryption. The default is **NONE**.	Optional
From the **Encryption Level** drop-down list, select **NONE**, **PAYLOAD**, or **ENTIRE_PAYLOAD**.	The encryption level specifies how much of the message content is to be encrypted. Select **PAYLOAD** to encrypt only the XML business document(s) part of the message. Select **ENTIRE_PAYLOAD** if you want to encrypt the business documents and all attachments in the message. The default is **NONE**.	Optional

Setting	Description	Required/ Optional
From the **Cipher Algorithm** drop-down list, select **NONE**, **RC5**, **DES**, **3DES**, or **RC2**.	Type of cipher algorithm: If **RC5** is selected, the algorithm object identifier passed to the RSA security code is `RC5-0x10-32-16/CBC/PKCS5Padding`. If the algorithm object identifier is equal to `RC5-0x10-32-16/CBC/PKC5Padding`, then an RC5 in CBC mode, with the PKCS5 padding algorithm, is used to encrypt the message. If **DES** is selected, the algorithm object identifier passed to the RSA security code is `DES/CBC/PKC5Padding`. If the algorithm object identifier is equal to `DES/CBC/PKC5Padding`, then a DES in CBC mode with the PKCS5 padding algorithm, is used to encrypt the message. If **3DES** is selected, the algorithm object identifier passed to the RSA security code is `3DES_EDE/CBC/PKC5Padding`. If the algorithm object identifier is equal to `3DES_EDE/CBC/PKC5Padding`, then a Triple DES in EDE mode, with the PKCS5 padding algorithm, is used to encrypt the message. A domestic license is required. If **RC2** is selected, the algorithm object identifier passed to the RSA security code is `RC2/CBC/PKCS5Padding`. If the algorithm object identifier is equal to `RC2/CBC/PKCS5Padding`, then RC2 in CBC mode, with the PKCS5 padding algorithm at a key size of 40 bits (RC2-40), is used to encrypt the message. The default is **NONE**.	Required if Encryption Level is **PAYLOAD** or **ENTIRE_PAYLOAD**
XML Digital Signature Configuration for Non-Repudiation		
From the **Signature Certificate** drop-down list, select the certificate.	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 "Adding Certificates to a Trading Partner" on page 9-14 for instructions.	
Check or uncheck the **Signature Required** check box.	When checked, the message is digitally signed using the signature certificate of the trading partner sending the message. The default is unchecked. Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See "Configuring Secure Audit Logging" on page 9-11.	Required

Setting	Description	Required/ Optional
Check or uncheck the **Signature Receipt Required** check box.	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. Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. See "Configuring Secure Audit Logging" on page 9-11.	Required
From the **Hash Function** drop-down list, select **None**, **SHA1**, or **MD5.**	Message digest algorithm used for the acknowledgement message. If **SHA1** or **None** is selected, the Secure Hash Algorithm 1 (SHA-1), which produces a 160-bit hash, is used. If **MD5** is selected, the Message Digest 5 (MD5) message hash algorithm, which produces a 128-bit hash, is used. The default is **None**. **Note:** Non-repudiation of receipt requires an acknowledgement of the received RosettaNet business message to be sent. The acknowledgement must be digitally signed and include an MD5 or SHA-1 digest of the message being acknowledged.	Required

Note: Within WebLogic Integration, the RosettaNet protocol supports non-repudiation by digitally signing outbound messages and acknowledgements based on the settings for the **Signature Required**, **Signature Receipt Required**, and **Hash Function** properties of the binding. For all RosettaNet messages, the non-repudiation protocol is **PKCS7**.

In addition to the preceding properties:

- 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 *Deploying WebLogic Integration Solutions*.
- PIP failure notification can also be configured by the administrator. See "Configuring PIP Notification of Failure Roles for RosettaNet Bindings" on page 9-62.

Defining a Web Service Binding

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

Setting	Description	Required/ Optional

In the **Name** field, enter the binding name.	The name used to identify the binding within the system. The name must be unique within the trading partner profile. When you add a new binding, a default name is automatically generated using the following convention:
	`<partner>-<protocol>-<qualifier>`
	For example:
	`acme-webservice-4`
	If you choose to change the default name, make sure the name you choose is unique.
	Note: This field is only available on the **Add Binding** page. It cannot be edited on the **Edit Binding** page.
		Required

Transport Configuration		
From the **Transport Protocol** drop-down list, select the **HTTP** or **HTTPS**.	The transport protocol for sending and receiving messages.	Required
From the **Transport Protocol Version** drop-down list, select the version.	The version of the transport protocol. If **HTTP** is selected for the Transport Protocol, select **1.0** or **1.1**. If **HTTPS** is selected for Transport Protocol, **1.1** is currently the only option.	Required
In the **Endpoint** field, enter the **URL** for the transport endpoint.	The URL or URI for the transport endpoint. For information about specifying an endpoint as a URI, see "Defining Endpoints for Projects Containing Multiple JPDs Having the Same Name" on page 9-44.	Required
In the **Timeout** field, enter the transport timeout.	The transport timeout for the specified endpoint. The default value is **0**, which indicates **no timeout**.	Required

Defining Endpoints for Projects Containing Multiple JPDs Having the Same Name

When you have multiple JPD files with the same name within the same Java package, that is,. in the same project, you should use the actual URI to identify the absolute endpoint of the participant process.

To use this feature, you must first add the `B2B-TransportServletFilter` to your `web.xml` file by adding the following lines of code:

```
<!-- WLI-B2Bi filter-begin. DO NOT EDIT -->
<filter>
<filter-name>TransportServletFilter</filter-name>
<filter-class>com.bea.b2b.transport.http.TransportServletFilter</filter-class>
</filter>

<filter-mapping>
<filter-name>TransportServletFilter</filter-name>
<url-pattern>/*</url-pattern>
</filter-mapping>
<!-- WLI-B2Bi filter-end. -->
```

After you have edited your `web.xml` file, define your trading partner's endpoint URL accordingly.

Related Topics

- "Adding Protocol Bindings to a Trading Partner" on page 9-18
- "Viewing and Changing Bindings" on page 9-52

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 Profil**e page for the partner.
Type	The trading partner type (local or remote).

Property	Description
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	Status of the trading partner: • 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. • 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).

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.

Related Topics

- "Viewing and Changing Trading Partner Profiles" on page 9-47
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70
- "Deleting Trading Partner Profiles" on page 9-78

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 **ebxml-service-name** specified in the @jpd:ebxml Annotation. For a RosettaNet process, this is the **pip-name** specified in the @jpd:rosettanet Annotation. 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.

Related Topics

- "Viewing and Changing Services" on page 9-65

- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70
- "Deleting Services" on page 9-81

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. **Note:** 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: • 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. • 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).	Yes
Description	An optional description. This value is for administrative purposes only. It is not included in messages.	Yes

Property	Description		Administrator Can Set (Yes/No)
Default Trading Partner	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). This field is only displayed for a local trading partner.		Yes
Email	A contact email address for the trading partner.		Yes
Address	A mailing address for the trading partner.		Yes
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 **Delete** link that can be used to delete the entry.	

Property	Description		Administrator Can Set (Yes/No)
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 **Delete** link that can be used to delete the entry.	
Custom Extension			
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 **Delete** 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 9-44.
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 9-31.

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 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 9-14.
   - To add bindings to the trading partner, see "Adding Protocol Bindings to a Trading Partner" on page 9-18.
   - To add a custom extension to the trading partner, see "Adding a Custom Extension to a Trading Partner" on page 9-19.
   - To update a certificate, see "Viewing and Changing Certificates" on page 9-50.
   - To update a binding, see "Viewing and Changing Bindings" on page 9-52.
   - To update a custom extension, see "Viewing and Changing a Custom Extension" on page 9-64.

Related Topics

- "Adding Trading Partner Profiles" on page 9-13
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

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 9-44, 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 Certificates** 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.

Related Topics

- "Adding Certificates to a Trading Partner" on page 9-14
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

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 for RosettaNet bindings.

For example, the **View Binding Details** page for a RosettaNet 2.0 binding is shown in the following figure.

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

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
Name	The name used to identify the binding within the system. **Note:** You cannot update the name, business protocol, or business protocol version of an existing binding. To change the these properties, you must delete the binding, then recreate it with the new values.	All binding types	No
Business Protocol	The business protocol (ebXML, RosettaNet, or Web service).	All binding types	No

Property	Description	Property Applies To	Administrator Can Set (Yes/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	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.	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Transport Configuration			
Transport Protocol	The transport protocol for sending and receiving messages: • For ebXML or RosettaNet, HTTP or HTTPS. • For a Web service, HTTP, HTTPS, or JMS.	All binding types	Yes
Transport Protocol Version	The version of the transport protocol. • For HTTP 1.0 or 1.1. • For HTTPS the value is 1.1.	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
Quality of Service			
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: • 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. • For RosettaNet, the number of times a message should be retried in case of failure.	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

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
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: • Best effort. No reliable messaging. • Once and only once reliable messaging. For messaging that requires acknowledgement and duplicate elimination. • At least once reliable messaging (ebXML 2.0 only). For messaging that requires acknowledgement, but not duplicate elimination. • At most once reliable messaging (ebXML 2.0 only). For messaging that requires duplicate elimination, but not acknowledgement.	ebXML 1.0/2.0	Yes
Digital Signature Configuration for Non-Repudiation			
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
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 message digest hash function (SHA1 or MD5).	RosettaNet 1.1/2.0	Yes
Signature Algorithm	The predefined signature algorithm (RSA).	RosettaNet 1.1/2.0	No

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
Message-Level Encryption Configuration			
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, 3DES, or RC2). See "Defining a RosettaNet 1.1 or 2.0 Binding" on page 9-38 for a description of the values.	RosettaNet 2.0	Yes
Encryption Level	The encryption level specifies how much of the message content is to be encrypted. • PAYLOAD—Only the XML business document(s) part of the message is encrypted. • ENTIRE_PAYLOAD—The business documents and all attachments in the message are encrypted. • NONE—Message is not encrypted.	RosettaNet 2.0	Yes
Authentication			
Authentication table	Entry for each authentication configured for the binding. See "Adding Authentication to a Service Profile" on page 9-25.	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 **Delete** link that can be used to delete the entry.		

Property	Description		Property Applies To	Administrator Can Set (Yes/No)
PIP Failure				
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 **Delete** 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 9-44, 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 Detail**s page, click the name of the binding.

   The **Edit Binding** page is displayed.

2. Update properties as required. See "Defining Protocol Bindings" on page 9-33.

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 9-60.

   – To Configure PIP failure notification to a RosettaNet binding, see "Configuring PIP Notification of Failure Roles for RosettaNet Bindings" on page 9-62.

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 9-1 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 **Username** field or select a new alias from the **Password Alias** drop-down list.
One-Way	No properties can be edited.	You can select a new certificate from the **Server Certificate** drop-down list.
One-Way with Basic	No properties can be edited.	You can enter a new user name in the **Username** field or select a new alias from the **Password Alias** drop-down list. You can select a new certificate from the **Server Certificate** drop-down list.
Mutual	You can select a new certificate from the **Client Certificate** drop-down list.	You can select a new certificate from the **Client Certificate** drop-down list. You can select a new certificate from the **Server Certificate** drop-down list.

To learn more about adding authentication to a service profile, see "Adding Authentication to a Service Profile" on page 9-25. 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 9-44, 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 9-46, 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 9-25. 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 Detail**s 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 9-1 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 9-14 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 9-14 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 10-15 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 9-44, 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**.

   The **Configure Signature Transforms for XML DSIG** page is displayed.

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 9-44, 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**.

   The **Add PIP Failure** page is displayed.
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 9-44, 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.

Related Topics

- "Adding Protocol Bindings to a Trading Partner" on page 9-18
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

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 9-44, 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 9-20 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.

Related Topics

- "Adding a Custom Extension to a Trading Partner" on page 9-19
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

Viewing and Changing Services

The **View and Edit Service Details** page allows you to view and change service properties. For RosettaNet services, you can also add, edit, or delete the RosettaNet service defaults from this page.

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 **ebxml-service-name** set in the @jpd:ebxml annotation. For a RosettaNet process, this is the **pip-name** set in the @jpd:rosettanet annotation. 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)
Service Profiles			
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 "Adding Service Profiles to a Service" on page 9-23.	
	Status	Status of the service profile (enabled or disabled).	
	View	A **View** link that displays the **View Service Profile** page. To learn more, see "Viewing and Changing Service Profiles" on page 9-68.	
	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 9-46.
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.

To view and edit the defaults for RosettaNet service:

1. On the **View and Edit Service Details** page, click **View Service Defaults** to view the current settings.

2. Click **Edit Service Defaults** to update the settings. See "Adding Defaults to a RosettaNet Service" on page 9-22 for a description of the available settings.

3. Click **Submit** to save your changes.

To delete the defaults for a RosettaNet service:

1. On the **View and Edit Service Details** page, click **View Service Defaults** to view the current settings.

2. Click **Delete** to delete the current defaults.

   You are prompted to confirm.

3. Click **OK** to confirm and delete the RosettaNet service defaults.

   The defaults are deleted and you are returned to the **View and Edit Service Details** page.

Related Topics

- "Adding Defaults to a RosettaNet Service" on page 9-22
- "Viewing and Changing Service Profiles" on page 9-68
- "Adding Service Profiles to a Service" on page 9-23
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

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 9-46.
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 Profil**e 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 9-10.
- **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 9-70.

   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.

Related Topics

- "Viewing and Changing Services" on page 9-65
- "Enabling and Disabling Trading Partner and Service Profiles" on page 9-70

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 9-44.
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 9-44.
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 9-44.
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 9-44.
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 9-46.
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 Using the Trading Partner Bulk Loader in *Managing WebLogic Integration Solutions*.

Note: You cannot import certificate private key information for a local trading partner. Certificates with public keys can only be loaded for remote trading partners.

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 Using the Trading Partner Bulk Loader in *Managing WebLogic Integration Solutions*. 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.

   The **Import Trading Partner Management Data** page is displayed.

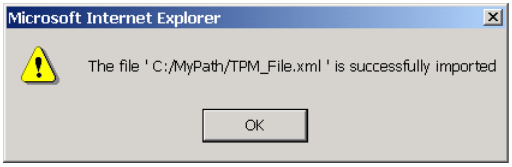
2. Do one of the following:

   – 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**
6. If the TPM file contains data for existing trading partners, you are prompted to disable any service profiles in use for the trading partners. If prompted, click **Disable** to disable the service profiles and continue.

   When the import process is complete, the following message is displayed.



7. Click **OK** to dismiss the message box.

Related Topics

- "Exporting Management Data" on page 9-75
- "Listing and Locating Trading Partners" on page 9-44

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**.

   The **Export Trading Partner Management Data** page is displayed.
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.

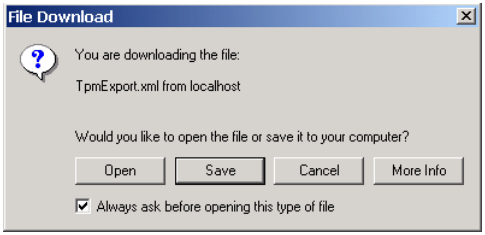
     Note: If you are exporting for import to WebLogic Integration - Business Connect, you can only export one trading partner profile at a time. Before continuing, verify that a single trading partner is selected.

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 it's 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. Do one of the following:
   - Uncheck the **Export Certificate Key Information** check box to suppress the export of certificate key information.
   - Check the **Export Certificate Key Information** check box to export certification key information.
8. 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.

   For example, Internet Explorer displays the following dialog box.



9. Select **Save** if prompted.
10. Specify the location and name of the file, then click **Save**.

    The file is saved to the specified location.

Related Topics

- "Importing Management Data" on page 9-73

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**.

   The **Delete Trading Partner Management Data** page is displayed.
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 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. 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 it's 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**.

   When the process is complete, the **Trading Partner Management** home page is displayed.

Related Topics

- "Deleting Trading Partner Profiles" on page 9-78
- "Deleting Certificates, Bindings, or Custom Extensions" on page 9-79
- "Deleting Services" on page 9-81
- "Deleting Service Profiles from a Service" on page 9-82

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 9-44.
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 9-44.
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.

Related Topics

- "Deleting Service Profiles from a Service" on page 9-82
- "Deleting Trading Partner Profiles and Services Using Bulk Delete" on page 9-77
- "Deleting Certificates, Bindings, or Custom Extensions" on page 9-79

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 9-44, 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 9-44, 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 9-44, 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 9-46.
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.

Related Topics

- "Deleting Service Profiles from a Service" on page 9-82
- "Deleting Trading Partner Profiles and Services Using Bulk Delete" on page 9-77

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 9-46.
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.

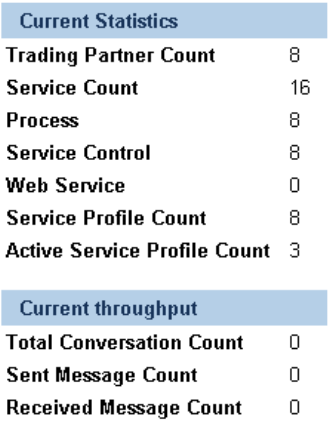
Viewing Statistics

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:

1. Locate the service as described in "Listing and Locating Services" on page 9-46.
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 **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 9-23.
- The purge schedule for the system. To learn more, see "Reporting and Purging Policies for Tracking Data" on page 10-4.

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 9-85.
   - 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 9-86.

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:

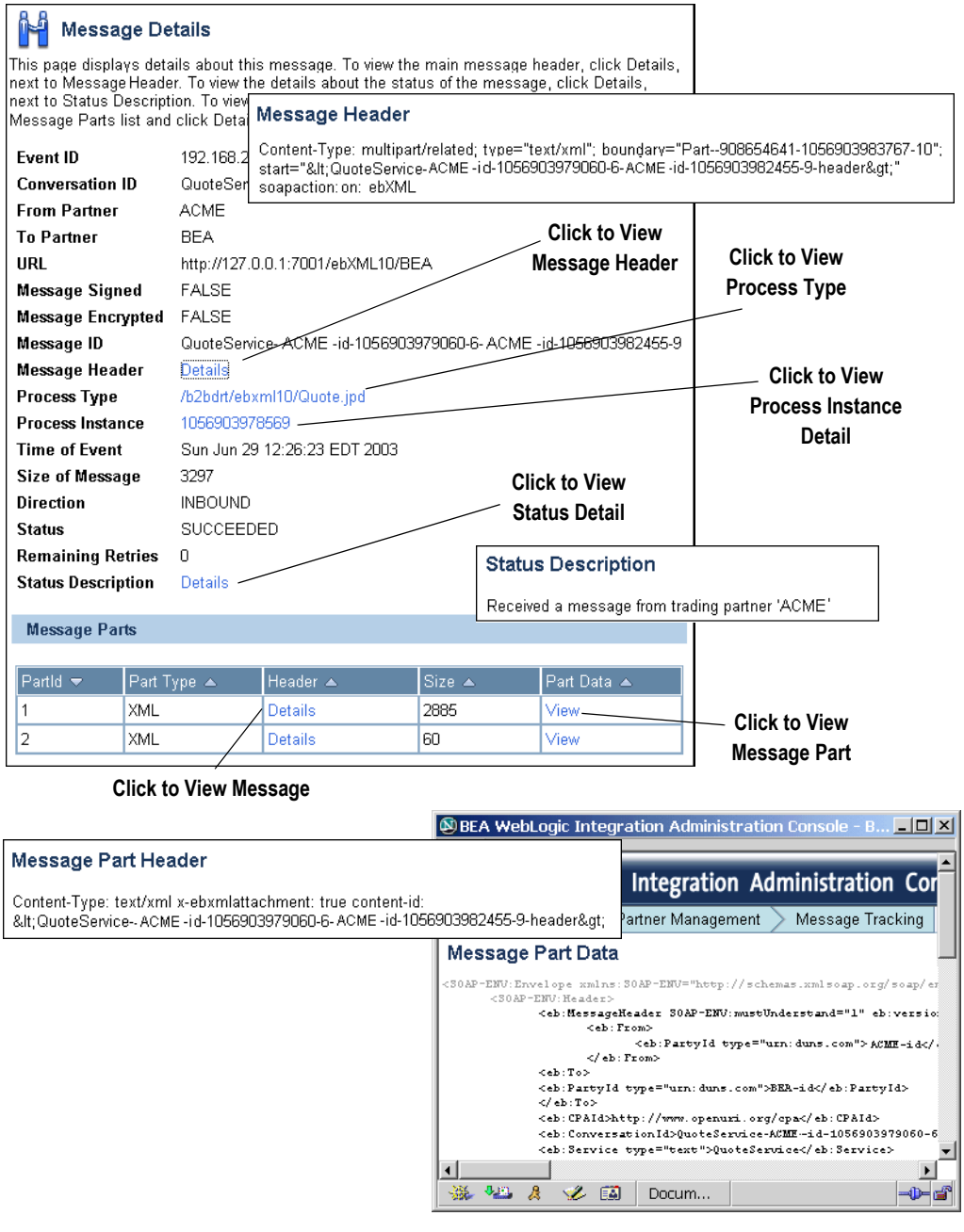
1. From the **Trading Partner Management** home page, select the **Message Tracking** module.

   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 9-23.


Message Details
This page displays details about this message. To view the main message header, click Details, next to Message Header. To view the details about the status of the message, click Details, next to Status Description. To view Message Parts list and click Detail
Message Header
Content-Type: multipart/related; type="text/xml"; boundary="Part--908654641-1056903983767-10"; start="<QuoteService-ACME-id-1056903979060-6-ACME-id-1056903982455-9-header>" soapaction: on: ebXML
Event ID 192.168.2
Conversation ID QuoteSer
From Partner ACME
To Partner BEA
URL http://127.0.0.1:7001/ebXML10/BEA
Message Signed FALSE
Message Encrypted FALSE
Message ID QuoteService-ACME-id-1056903979060-6-ACME-id-1056903982455-9
Message Header Details
Process Type /b2bdrt/ebxml10/Quote.jpd
Process Instance 1056903978569
Time of Event Sun Jun 29 12:26:23 EDT 2003
Size of Message 3297
Direction INBOUND
Status SUCCEEDED
Remaining Retries 0
Status Description Details
Click to View Message Header
Click to View Process Type
Click to View Process Instance Detail
Click to View Status Detail
Status Description
Received a message from trading partner 'ACME'
Message Parts
PartId | Part Type | Header | Size | Part Data
1 | XML | Details | 2885 | View
2 | XML | Details | 60 | View
Click to View Message Part
Click to View Message
Message Part Header
Content-Type: text/xml x-ebxmlattachment: true content-id: <QuoteService-ACME-id-1056903979060-6-ACME-id-1056903982455-9-header>
BEA WebLogic Integration Administration Console - B...
Integration Administration Cor
Partner Management
Message Tracking
Message Part Data
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/er
<SOAP-ENV:Header>
<eb:MessageHeader SOAP-ENV:mustUnderstand="1" eb:versio
<eb:From>
<eb:PartyId type="urn:duns.com">ACME-id</
</eb:From>
<eb:To>
<eb:PartyId type="urn:duns.com">BEA-id</eb:PartyId>
</eb:To>
<eb:CPAId>http://www.openuri.org/cpa</eb:CPAId>
<eb:ConversationId>QuoteService-ACME-id-1056903979060-6
<eb:Service type="text">QuoteService</eb:Service>
Docum...

CHAPTER 10

System Configuration

The *System Configuration* module allows you to:

- View or set the purge schedule.
- Start or stop the purge process.
- Enable or disable the transmission of data to an offline datastore.
- View or set the JNDI name for the datastore used to store data offline.
- View or set the default tracking level and reporting data 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 11-3.

The following topics are provided:

- Viewing the Configuration for Tracking, Reporting, and Purging Data
- Configuring the Reporting Data and Purge Processes
- Configuring the Reporting Datastore
- Configuring the Default Tracking Level and Reporting Data Policy
- Manually Starting and Stopping the 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
- Configuring the Worklist Task Creation Role

About System Administration

The following sections provide background information related to system administration:

- Process Tracking Data
- Worklist Tracking Data
- Reporting and Purging Policies for 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).

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 Default Tracking Level and Reporting Data Policy" on page 10-12.
- Setting tracking level for a process type, see "Viewing and Changing Process Details" on page 3-12.

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 Default Tracking Level and Reporting Data Policy" on page 10-12.
- Contents of the worklist history tables, see "Task History Tables" in Worklist Tracking Data in *Using the Worklist*.

Reporting and Purging Policies for 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 9-10 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 purge process is configured to run at regular intervals set by the administrator.

Note: You cannot disable the purge process.

If the data is required for reporting and analysis, the administrator can enable the transfer of tracking data suitable for reporting to an offline database. If the reporting data stream is enabled, the specified database is populated by a near real-time data stream.

Note: Because the reporting database is populated by a near real-time stream, it is possible to see a snapshot of the data where some process instances contain partial data.

To provide a greater level of control, the administrator also configures the following:

- *Reporting data policy for each process type*
  The reporting data policy for a process can be set to one of the following:
  - **On**—Instance data for the process is transmitted to the reporting database if the reporting data stream is enabled.
  - **Off**—Instance data is not transmitted to the reporting database.
  - **Default**—The system default reporting data policy (described below) is used.
- *System default reporting data policy for processes*
  The system default reporting data policy can be set to **On** or **Off**. If the reporting data policy for a process is set to **Default**, the process inherits the system default setting. Instance data for the process is, or is not, transmitted to the reporting database, accordingly.
- *Purge Delay*
  The amount of time after the following events that must pass before the data is subject to purge by the purge process:
  - Completion or termination of a process instance.
  - Completion or cancellation of a worklist tasks.
  - Receipt or delivery of business message.

  For example, suppose the reporting data stream is enabled, the reporting data policy for a process is **On**, the purge delay is set to 5 days, and the purge process is configured to purge data every hour. In that case, the data for an instance completing on day 1 would be transmitted to the reporting database as it is generated, but would not be purged from the runtime database until 5 days elapsed.

The administrator can reset the purge schedule at any time and run the purge process on demand.

Only data for completed or terminated process instances, or completed or cancelled worklist tasks is subject to the 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 3-3.
- Configuring the reporting data stream, see "Configuring the Reporting Data and Purge Processes" on page 10-11.
- Setting the system default reporting data policy level, see "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12.
- Setting the reporting data policy for a process, see "Viewing and Changing Process Details" on page 3-12.
- The reporting data tables, see Querying WebLogic Integration Archive Data in *Managing WebLogic Integration Solutions*.

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 10-15.

Overview of the System Configuration Module

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

Page	Associated Tasks	Help Topics
Reporting and Tracking Policies		
Current Tracking and Reporting Data Settings	View the system-level settings for the reporting data generation and purge processes. The current status of the reporting data stream (enabled or disabled), purge schedule, purge delay, reporting datastore (if the reporting data stream is enabled), default reporting data policy, and default tracking level are displayed.	"Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9
Tracking Data Purge and Reporting Data Policy Settings	Enable or disable reporting data generation.	"Configuring the Reporting Data and Purge Processes" on page 10-11
	Edit the purge start time and repeat interval.	
	Edit the purge delay.	
Edit Data Store Configuration Settings	Change the JNDI name of the offline reporting database.	"Configuring the Reporting Data and Purge Processes" on page 10-11
Default Tracking Level and Reporting Data Policy for Processes	Change the default tracking level or default reporting data policy for processes.	"Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12
Edit Worklist Task Tracking Parameter	Change the default tracking level for worklist tasks.	"Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12

Page	Associated Tasks	Help Topics
Purge		
Purge Tracking Data	Request an immediate purge cycle.	"Manually Starting and Stopping the Purge Process" on page 10-14
	Interrupt a purge cycle.	
	View the number of records in the runtime database for completed or terminated process instances.	
	View the time the last purge cycle completed.	
Password Store		
View and Edit Password Aliases	View a list of password aliases.	"Listing and Locating Password Aliases" on page 10-16
	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.	"Deleting Passwords from the Password Store" on page 10-17
Add New Password Alias	Add a password by assigning a unique alias and defining the password.	"Adding Passwords to the Password Store" on page 10-15
Edit Password Alias	Change the password associated with a password alias.	"Changing the Password for a Password Alias" on page 10-16
Application Integration		
View Application Integration Configuration	View the application integration configuration. Debug status (enabled or disabled), JMS connection factory, and repository root directory are displayed.	"Configuring the Server for Application Integration" on page 10-17
Edit Application Integration Configuration	Edit the application integration debug status, JMS connection factory, or repository root directory.	"Configuring the Server for Application Integration" on page 10-17

Page	Associated Tasks	Help Topics
Worklist		
View Worklist Configuration	View current setting for the worklist task creation role.	"Configuring the Worklist Task Creation Role" on page 10-18
Edit Worklist Configuration	Edit the worklist task creation role.	"Configuring the Worklist Task Creation Role" on page 10-18

Viewing the Configuration for Tracking, Reporting, and Purging Data

The **Current Tracking and Reporting Data Settings** page allows you to view the:

- Reporting data configuration.
- Purge schedule and purge delay.
- Default tracking level for processes and tasks.
- Default reporting data policy for processes.

To view the configuration for tracking, reporting, and purging data:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Tracking, Purging, and Reporting Policies**.

The following table describes the properties displayed on the page:

Property	Description
Schedule	
The Reporting Data Stream Process Is	Status of reporting data generation (enabled or disabled): **Note:** Tracking data includes process instance, task instance, and trading partner message history. To learn more, see "Reporting and Purging Policies for Tracking Data" on page 10-4.

Property	Description	
Next Purge Start Time	The start date and time for the purge process.	
Repeat Every	Intervals from the start time that the purge process runs.	
Purge Delay	The amount of time after completion or termination before process instance, task tracking. or message history data is subject to purge.	
Reporting Data Datastore		
Reporting Data Datastore JNDI Name	JNDI name of the database to which reporting data is written when the reporting data stream is enabled.	
Default Reporting Data Policy and Tracking Level for Processes		
Default Tracking Level	The system default tracking level (full, node, minimum, or none). If the **Tracking Level** for a process is set to **Default**, the process inherits this setting. To learn how to set the reporting data policy for a process see "Viewing and Changing Process Details" on page 3-12.	
Default Reporting Data Policy	The system default reporting data policy (on or off). If the **Reporting Data Policy** for a process is set to **Default**, the process inherits this setting. Instance data for the process is, or is not, transmitted to the reporting database accordingly. To learn how to set the reporting data policy for a process see "Viewing and Changing Process Details" on page 3-12.	
Default Variable Tracking Level	The system default **Variable Tracking Level** (on or off). Process variable tracking is available only if the **Tracking Level** for a process is set to full, node, or minimum.	
Worklist Task Tracking Level		
Task Tracking Level	Tracking level for worklist tasks.	
	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.

Related Topics

- "Configuring the Reporting Data and Purge Processes" on page 10-11
- "Configuring the Reporting Datastore" on page 10-12
- "Configuring the Default Tracking Level and Reporting Data Policy" on page 10-12
- "Process Tracking Data" on page 10-2
- "Reporting and Purging Policies for Tracking Data" on page 10-4

Configuring the Reporting Data and Purge Processes

The **Tracking Data Purge and Reporting Data Policy Settings** page allows you to enable or disable the reporting data stream and update the purge schedule and purge delay.

To configure the reporting and purging policies:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Tracking, Purging, and Reporting Policies**.
3. In the **Purge Schedule** section, click the **Configure** link.
4. Do one or more of the following:
   - To enable or disable the reporting data stream, check or uncheck the **Enable Reporting Data Generation** check box.
   - To update the **Next Purge 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 Tracking and Reporting Data Settings** page.

Note: When you update the repeat interval without changing the **Next Purge Start Time**, the new interval will not be effective until after the next scheduled purge. The scheduled start

time for the next purge is displayed in the **Purge Schedule** section of the **Current Tracking and Reporting Data Settings** page.

Related Topics

- "Reporting and Purging Policies for Tracking Data" on page 10-4
- "Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9

Configuring the Reporting Datastore

The **Edit Datastore Configuration Settings** page allows you to specify the database used to store reporting data.

To configure the JNDI name for the datastore:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Tracking, Purging, and Reporting Policies**.
3. In the **Reporting Data Datastore** section, click the **Configure** link.
4. In the **Reporting Data Datastore JNDI Name** field, enter the JNDI name for the datastore.
5. Click **Submit** to save your changes and return to the **Current Tracking and Reporting Data Settings** page.

Note: When you set or update the **Reporting Data Datastore JNDI Name**, the change will not take effect until you restart the server.

Related Topics

- "Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9

Configuring the Default Tracking Level and Reporting Data Policy

In addition to allowing you to configure the reporting data stream and purge processes, the **Current Tracking and Reporting Data Settings** page allows you to configure:

- The default tracking level and reporting data policies for processes.
- The tracking level for worklist tasks.

See "Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9 for a description of all the properties displayed on the **Current Tracking and Reporting Data Settings** page.

To configure the default reporting data policy and tracking level for processes:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Tracking, Purging, and Reporting Policies**.
3. In the **Default Reporting Data Policy and Tracking Level for Processes** section, click the **Configure** link.

   The **Default Tracking Level and Reporting Data Policy for Processes** page is displayed.
4. Do one or all of the following:
   - From the **Default Tracking Level** drop-down list, select **Full**, **Node**, **Minimum**, or **None**.
   - From the **Default Reporting Data Policy** drop-down list, select **On** or **Off**.
   - From the **Default Variable Tracking Level** drop-down list, select **On** or **Off**.
5. Click **Submit** to save your changes and return to the **Current Tracking and Reporting Data 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 **Tracking, Purging, and Reporting Policies**.
3. In the **Worklist Task Tracking Level** section, click the **Configure** link.

   The **Edit Worklist Task Tracking Level Parameter** page is displayed.
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 Tracking and Reporting Data Settings** page.

Related Topics

- "Viewing the Configuration for Tracking, Reporting, and Purging Data" on page 10-9
- "Process Tracking Data" on page 10-2

- "Reporting and Purging Policies for Tracking Data" on page 10-4

Manually Starting and Stopping the Purge Process

The **Purge Tracking Data** page displays the:

- Number of records stored in the runtime database for completed or terminated process instances.
- Time the purge process last completed.

If the 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 purge process run immediately, or if a purge operation is underway, you can manually stop the process, as described in the following procedure.

To start or stop a purge of the tracking data:

1. From the home page, select the **System Configuration** module.
2. From the left panel, select **Purge** to display the **Purge Tracking Data** page.
3. Do one of the following:
   - To start a purge of the tracking data, click the **Purge Tracking Data** button.
   - To stop a purge operation that is currently underway, click the **Stop Current Purge Operation** button.

   A confirmation dialog box is displayed.
4. Click **OK** to confirm, or **Cancel** to dismiss the dialog and cancel the action.

Related Topics

- "Reporting and Purging Policies for Tracking Data" on page 10-4
- "Configuring the Reporting Data and Purge Processes" on page 10-11

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 the changes and return to the **View and Edit Password Aliases** page, click **Cancel**.

Related Topics

- "Password Aliases and the Password Store" on page 10-6
- "Listing and Locating Password Aliases" on page 10-16

Listing and Locating Password Aliases

The V**iew 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.

Related Topics

- "Adding Passwords to the Password Store" on page 10-15
- "Changing the Password for a Password Alias" on page 10-16
- "Deleting Passwords from the Password Store" on page 10-17

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 10-16.
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 the 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 10-16.
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 **Debug Enabled** check box.	When **Debug** 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 **JMS Connection Factory JNDI Name** 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 **Repository Root Directory** field, enter repository root.	Files related to application views are stored in a file repository (`wlai-repository`). 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.

CHAPTER 11

User Management

The *User Management* module allows you to add, delete, and modify the users, groups, and roles defined for 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 11-3.

The following topics are provided:

- 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 3-4.
- *Message Broker channels*
  Policies define the roles required to subscribe and publish to a given channel. See "Setting Channel Security Policies" on page 5-7.
- *Application Views*
  Policies define the roles required to execute services and subscribe for events on an application view. See "Managing Application Integration Security" on page 8-7.

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.

Note: The following sections provide information specific to WebLogic Integration. To learn more about protecting resources in a platform-based application, see *Introducing WebLogic Platform 8.1 Security*.

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 11-5.

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/secwlres/secroles.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 "Default Security Policies" on page 11-5 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)
IntegrationDeployer	The WebLogic Integration deployer 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:(IntegrationDeployers)

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.
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 (**IM**), IntegrationOpertator (**IO**), and IntegrationAdmin (**IA**), and IntegrationUser (**IU**) roles can execute:

Resource	Action	IM	IO	IA	IU
Servers in a Cluster	Start Stop		✓	✓	

Resource	Action	IM	IO	IA	IU
Processes	Configure versions, tracking, and reporting data policies		✓	✓	
	Configure Security			✓	
	Terminate Suspend Resume Unfreeze		✓	✓	
	Invoke	Configured by the administrator. Until policies are defined, the default is everyone.			
	Monitor	✓	✓	✓	
Dynamic Control Selectors	Configure		✓	✓	
	View	✓	✓	✓	
Worklist Tasks	Modify Reassign Complete Cancel Claim Delete		✓	✓	✓
	Configure Security			✓	
	View	✓	✓	✓	✓

Resource	Action	IM	IO	IA	IU
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	✓	✓	✓	
Users, Groups, and Roles	Create Delete Modify			✓	
	View			✓	
Business Calendars	Create Delete Modify		✓	✓	
	Manage user and group mappings		✓	✓	
	View	✓	✓	✓	

Resource	Action	IM	IO	IA	IU
Application Integration	Configure connection parameters and environment variables		✓	✓	
	Configure security			✓	
	Monitor	✓	✓	✓	
Trading Partner and Service Profiles	Create Delete Modify		✓	✓	
	View	✓	✓	✓	
Trading Partner Management Server	Configure		✓	✓	
	View	✓	✓	✓	
System	Configure the reporting data and purge policies, or manually kick off the purge process			✓	
	Manage password aliases			✓	
	View repository size	✓	✓	✓	

Security Provider Requirements for User Management

The ability to define users and groups, and to configure security for WebLogic Integration resources, is dependent on the availability of an authenticator that implements the following MBeans:

- `UserEditor`
- `GroupEditor`
- `GroupMemberLister`
- `MemberGroupLister`

If there is no authenticator that implements all the above MBeans, all functionality in the WebLogic Integration Administration Console related to configuring users or groups, or to granting specific privileges to users or groups, is disabled.

As described in *Introducing WebLogic Platform 8.1 Security* (http://edocs.bea.com/platform/docs81/secintro/secure.html), it is possible to run more than one security provider at a time. If multiple authenticators are running, and more than one authenticator implements the MBeans required for WebLogic Integration administration (`UserEditor`, `GroupEditor`, `GroupMemberLister`, and `MemberGroupLister`), there is currently no mechanism for specifying the which provider is to be used by the WebLogic Integration Administration Console. Due to this limitation, we recommended that you run a single authenticator that meets the requirements.

To learn more about WebLogic Server security realms and security providers, see "Security Realms" in *Introduction to WebLogic Security*, at the following URL:

http://edocs.bea.com/wls/docs81/secintro/realm_chap.html

Overview of the User Management Module

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

Page	Associated Tasks	Help Topics
Users		
View and Edit Users	View a list of users. User name, email, group membership, and associated business calendar are displayed.	"Listing and Locating Users" on page 11-17
	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.	"Deleting Users, Groups, or Roles" on page 11-22
Add New User	Add a user by assigning a unique name and password. Optionally, assign a description, email address, group membership, and business calendar.	"Adding a User" on page 11-12
View User Details	View user properties.	"Viewing and Changing User Properties" on page 11-19
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.	"Viewing and Changing User Properties" on page 11-19
Groups		
View and Edit Groups	View a list of groups. Group name, description and group membership are displayed.	"Listing and Locating Groups" on page 11-18
	Filter the list by group name. Use `?` to match any single character or `*` to match zero or more characters.	
	Delete one or more groups.	"Deleting Users, Groups, or Roles" on page 11-22

Page	Associated Tasks	Help 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.	"Adding a Group" on page 11-13
View Group Details	View group properties.	"Viewing and Changing Group Properties" on page 11-21
Edit Group Details	Change group properties. Add a description, or update the group membership.	"Viewing and Changing Group Properties" on page 11-21
Roles		
View and Edit Roles	View a list of roles. Role name is displayed.	"Listing and Locating Roles" on page 11-18
	Filter the list by role name. Use `?` to match any single character or `*` to match zero or more characters.	
	Delete one or more roles.	"Deleting Users, Groups, or Roles" on page 11-22
Add New Role	Add a role by assigning a unique role name and defining the conditions that constitute the role statement.	"Adding a Role" on page 11-14
View Role Conditions	View or change role conditions. Add, delete, or reorder conditions.	"Viewing and Setting Role Conditions" on page 11-22
Add Role Conditions	Define a condition to be added.	"Constructing a Role Statement" on page 11-15
Sort Role Conditions	Change the order of the conditions in the list.	"Constructing a Role Statement" on page 11-15
Edit Role Conditions Command	Change the command that joins conditions.	"Constructing a Role Statement" on page 11-15

Adding a User

The **Add New User** page allows you to create a new user.

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.)

      Note: By default, the IntegrationUsers group appears on the Current Groups list. Remove this entry if the user should not be a member of IntegrationUsers.

   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 clear entries, click **Reset**.

– To disregard the changes and return to the **View and Edit Users** page, click **Cancel**.

Related Topics

- "Default Groups, Roles, and Security Policies" on page 11-3

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 11-21.

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 the changes and return to the **View and Edit Groups** page, click **Cancel**.

Related Topics

- "Default Groups, Roles, and Security Policies" on page 11-3

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 **Submit**.

   The role is created and the **View Role Conditions** page for the role is displayed.
6. To add conditions to the role, click **Add Role Condition**. 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.

Related Topics

- "Default Groups, Roles, and Security Policies" on page 11-3

Constructing a Role Statement

You construct a role statement by adding conditions. See "Adding Conditions to a Role Statement" on page 11-15. Each condition is joined to the previous condition by a conjunction (**and**) or disjunction (**or**) command as shown in the following figure:

Role Statement:

	Command	Role Conditions
☐		Groups:(Auditors)
☐	and	Hours of Access are Between :(09:00:00,17:00:00)
☐	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 11-16.

Adding Conditions to a Role Statement

If you are logged in with sufficient privileges, you can add conditions from the **View Role Conditions** page. The **View Role Conditions** page is displayed when you create a new role, or when you select a role from the View and Edit Roles list. See "Listing and Locating Roles" on page 11-18.

To add a Groups condition:

1. On the **View Role Conditions** page, click **Add Role Condition** to display the **Add Role Conditions** 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. On the **View Role Conditions** page, click **Add Role Condition** to display the **Add Role Conditions** 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. On the **View Role Conditions** page, click **Add Role Condition** to display the Add Role Conditions 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 Conditions** page.

To update the joining command:

1. On the **View Role Conditions** page, 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. On the **View Role Conditions** page, 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. On the **View Role Conditions** page, 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.

Related Topics

- "Viewing and Changing User Properties" on page 11-19

- "Deleting Users, Groups, or Roles" on page 11-22

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.

Related Topics

- "Viewing and Changing Group Properties" on page 11-21
- "Deleting Users, Groups, or Roles" on page 11-22

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, previous, first, or last page.

Related Topics

- "Viewing and Setting Role Conditions" on page 11-22
- "Deleting Users, Groups, or Roles" on page 11-22

Viewing and Changing User Properties

The **View User Details** page displays the 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 11-17.
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:
   a. In the **Current Password** field, enter the current password.
   b. In the **New Password** field, enter the new password.

      Note: The password must be at least 8 characters long.

   c. In the **Confirm Password** field, enter the new password again.

5. Add or remove group 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.

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 the 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 11-18.
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 the changes and return to the **View and Edit Groups** page, click **Cancel**.

Viewing and Setting Role Conditions

The **View Role Conditions** 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 11-18.
2. Click the role name to display the **View Role Conditions** page.

   The role name and role statement are displayed.
3. To edit the role statement, see "Constructing a Role Statement" on page 11-15.

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 11-17.
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 11-18.
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 11-18.
2. Click the check box to the left of the roles to be deleted to select them.
3. Click **Remove Selected Roles**.

CHAPTER 12

Business Calendar Configuration

The *Business Calendar Configuration* module allows you 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 11-3.

The following topics are provided:

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 that 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 the Introduction in *Using the Worklist*.

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 6-24.

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.

If the calculation lands on a time that is busy, the calendar is rolled in the direction of the operation in one minute intervals until the next free time is reached. For example, if the calculation adds time (`addBusinessTime` method) and the addition lands on a busy time, the result rolls forward in one minute intervals until next available free minute. Alternately, if the calculation subtracts time (`subtractBusinessTime` method) and the subtraction lands on a busy time, the result rolls backward in one minute intervals until next available free minute. For instance, if the free time is 9:00 AM. to 5:00 PM, the subtraction rolls back to 4:59 PM.

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 help topics associated with each are provided.

Page	Associated Tasks	Help 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.	"Listing and Locating Business Calendars" on page 12-6
	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.	"Exporting and Importing Business Calendars" on page 12-10
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.	"Viewing and Changing Business Calendars" on page 12-7
	Update time period rules by adding, changing, deleting or reordering rules	
Add Business Calendar Time Period Rule	Define a time period rule to be added.	"Defining a Time Period Rule" on page 12-9
Update Business Calendar Time Period Rule	Change an existing time period rule.	"Defining a Time Period Rule" on page 12-9
Sort Calendar Rules	Change the order of the rules in the list.	"Viewing and Changing Business Calendars" on page 12-7
Map Users to a Business Calendar	Select a business calendar and assign the calendar to selected users.	"Assigning Business Calendars to Users and Groups" on page 12-11
	Remove the business calendar assignment from selected users.	

Page	Associated Tasks	Help Topics
Map Groups to a Business Calendar	Select a business calendar and assign the calendar to selected groups.	"Assigning Business Calendars to Users and Groups" on page 12-11
	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 12-7.

Related Topics

- "About Business Calendars and Business Time Calculations" on page 12-2

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.

Related Topics

- "Viewing and Changing Business Calendars" on page 12-7
- "Exporting and Importing Business Calendars" on page 12-10
- "Deleting Business Calendars" on page 12-13

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 12-6.
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**.

   The **Edit Business Calendar** page is displayed.

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 Rule** page is displayed.
2. Define the time period as required. See "Defining a Time Period Rule" on page 12-9.
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 Rule** page is displayed.
2. Define the time period as required. See "Defining a Time Period Rule" on page 12-9.
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 Rule** and **Update Business Calendar Time Period Rule** 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**.

Related Topics

- "Viewing and Changing Business Calendars" on page 12-7

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 12-6.
2. Click the check box to the left of the calendar to select it.
3. Click **Export**.

   The **Export a Business 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 Calendar** from the left panel.

   The **Import a Business Calendar** page is displayed.
3. Specify the file in the **Business Calendar File** field. Click **Browse** to browse for the file.
4. 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 "Task Due Dates" in Creating and Managing Worklist Tasks in *Using the Worklist*.

Note: If an authenticator that implements the required MBeans is not configured, the calendar mapping options are disabled. To learn more about the authenticator requirements, see "Security Provider Requirements for User Management" on page 11-9.

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 12-11 to update the **In Use** status.

To delete calendars:

1. Locate the calendars to be deleted. See "Listing and Locating Business Calendars" on page 12-6.
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.

CHAPTER 13

XML Cache

The *XML Cache* module allows you to:

- Add new entries to the XML Cache.
- Modify existing XML Cache entries.
- Delete existing XML Cache entries.
- View the code for existing cache entries.

Note: You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to add, view, or modify XML Cache entries. See "Default Groups, Roles, and Security Policies" on page 11-3.

The following topics are provided:

About the XML Cache

The XML Cache stores XML metadata documents. When you are designing a business process, you use the XML MetaData Cache Control to retrieve the XML documents stored in the XML Cache. You use the XML Cache module to create and maintain the XML metadata documents stored in the XML Cache.

Different applications that reside on different server-nodes can share the XML Cache.

Overview of the XML Cache Module

The following table lists the pages you can access from the XML Cache module. The tasks and help topics associated with each are provided:

Page	Associated Tasks	Help Topics
Configure XML Cache	Add a new XML document to the cache.	"Adding XML Documents to the XML Cache" on page 13-3
	Update an existing XML document entry.	"Updating an XML Document in the XML Cache" on page 13-3
	View the code for an existing XML document entry.	"Viewing the Code for an XML Document" on page 13-4
	Delete an existing XML document entry.	"Deleting an XML Document from the XML Cache" on page 13-5
Note: If you make a mistake while entering information into any of the **Key** or **XmlFileName** fields on the **Configure XML Cache** page, you can clear your entry by clicking the **Reset** button below the field you made the incorrect entry in.		
View All	View all XML documents in the cache.	"Viewing All XML Documents in the XML Cache" on page 13-5

Adding XML Documents to the XML Cache

The XML Cache module allows you to add XML documents to the XML Cache.

To add an XML document to the XML Cache:

1. From the home page, select the **XML Cache** module.

   The **Configure XML Cache** page is displayed.

2. In the first **Key** field, enter a *key* for the XML document you want to add to the XML Cache. When you are entering the key, remember that entries in the **Key** field are case insensitive and cannot be more than 256 characters long.

   The *key* is a logical name that uniquely identifies the XML document in the XML Cache. Do not use MBCS characters in the key name.

   Note: Leading and trailing spaces are trimmed for entries in the **Key** field.

3. Enter a filename for the document in the **XmlFileName** field or click **Browse** and select an existing file.

4. Click **Add**.

   The XML document is added to the XML Cache.

Related Topics

- "About the XML Cache" on page 13-2
- "Viewing All XML Documents in the XML Cache" on page 13-5

Updating an XML Document in the XML Cache

You can update an existing XML document from the **Configure XML Cache** page.

To update an existing XML document:

1. From the home page, select the **XML Cache** module.

   The **Configure XML Cache** page is displayed.

2. In the second **Key** field, enter the *key* for the XML document you want update. When you are entering the key, remember that entries in the **Key** field are case insensitive and cannot be more than 256 characters long.

   The *key* is a logical name that uniquely identifies the XML document in the XML Cache.

3. Enter a new filename for the document in the **XmlFileName** field or click **Browse** and select an existing file.
4. Click **Update**.

   The XML document is updated in the XML Cache.

Related Topics

- "About the XML Cache" on page 13-2
- "Adding XML Documents to the XML Cache" on page 13-3
- "Viewing All XML Documents in the XML Cache" on page 13-5

Viewing the Code for an XML Document

You can view the code for any XML document stored in the XML Cache.

To view the code:

1. From the home page, select the **XML Cache** module.

   The **Configure XML Cache** page is displayed.
2. In the third **Key** field, enter the *key* for the XML document you want view. When you are entering the key, remember that entries in the **Key** field are case insensitive and cannot be more than 256 characters long.
3. Click **Get**.

   The code for the specified XML document is displayed in the **View XML Cache Content** page.
4. Click **Configure XML Cache** at the bottom of the page to return to the **Configure XML Cache** page.

Related Topics

- "About the XML Cache" on page 13-2
- "Adding XML Documents to the XML Cache" on page 13-3
- "Viewing All XML Documents in the XML Cache" on page 13-5

Deleting an XML Document from the XML Cache

You can delete any XML document from the XML Cache whenever you want.

To delete an XML document:

1. From the home page, select the **XML Cache** module.

   The **Configure XML Cache** page is displayed.

2. In the last **Key** field, enter the *key* for the XML document you want delete. When you are entering the key, remember that entries in the **Key** field are case insensitive and cannot be more than 256 characters long.

3. Click **Delete**.

   The XML document associated with the key you specified is deleted from the XML Cache.

Related Topics

- "About the XML Cache" on page 13-2
- "Adding XML Documents to the XML Cache" on page 13-3
- "Viewing All XML Documents in the XML Cache" on page 13-5

Viewing All XML Documents in the XML Cache

You can view all of the entries for the XML Cache from the XML Cache module.

To view all the entries in the XML Cache:

1. From the home page, select the **XML Cache** module.

   The **Configure XML Cache** page is displayed.

2. Click **View All** in the left panel.

   The **View XML MetaData Keys** page is displayed.

3. To view the individual details of a particular key, click the key name.

   The content for the selected key is displayed on the **View XML Cache Content** page.

APPENDIX A

Configuring a Production Database

When preparing a production environment for WebLogic Integration, the production database must be configured to include the tables required by WebLogic Integration. To allow your database administrator to manage the process, the tables required are not created automatically. This section provides information about the scripts available to create the tables.

The SQL scripts that create the database tables used by WebLogic Integration can be found in the following 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. The following table describes the scripts.

Table A-1 WebLogic Integration Database Scripts

Script filename	Description
wli_runtime.sql	SQL that creates tables involved in WebLogic Integration runtime activity.
wli_runtime_drop.sql	SQL that drops tables created by wli_runtime.sql. **Note:** All runtime data is destroyed.

Table A-1 WebLogic Integration Database Scripts

Script filename	Description
`wli_archive.sql`	SQL that creates tables used to store WebLogic Integration data for reporting and analysis.
`wli_archive_drop.sql`	SQL that drops tables created by `wli_archive.sql`. **Note:** All runtime data is destroyed.

Use your preferred SQL tool to run the scripts to create or drop the WebLogic Integration tables in your production database.

In addition to the WebLogic Integration tables, you must also create the database tables that store conversational state information. To learn how to create the required tables, see How Do I: Deploy a WebLogic Workshop Application to a Production Server? in the WebLogic Workshop help, at the following URL:

http://edocs.bea.com/workshop/docs81/doc/en/workshop/guide/howdoi/howDeployWebLogicWorkshopWebServicestoaProductionServer.html

If you have trading partner management data, you can use the Bulk Loader to import the information. Refer to Appendix D, "Using the Trading Partner Bulk Loader."

APPENDIX B

Querying WebLogic Integration Reporting Data

As described in "About System Administration" on page 10-2, the reporting database tables contain information regarding events that occur during the execution of processes. These tables are created by the SQL commands in the file `wli_archive.sql` described in Appendix A, "Configuring a Production Database.".

To generate reports from reporting database, you will need to run SQL queries. This section describes useful tables and provides example queries:

The WLI_PROCESS_EVENT_ARCH Table

As a process executes, events are generated that track its execution. The events generated depend on the tracking level configured (see "Managing Process Tracking Data" on page 3-3). For example, if the tracking level for a process is set to **Full** or **Node**, two events, start node and end (or abort) node, are generated by each node.

If the process tracking data is transmitted to the reporting database, each event is stored as row in `WLI_PROCESS_EVENT_ARCH` table. The row contains the process name (a URI value), process instance ID, process event type (see com.bea.wli.management.archiving.TrackingEventType), and other values.

The `PROCESS_LABEL` column is set only for events generated by calls to:

`JpdContext.setProcessLabel(String)`

The WLI_DOCUMENT_DATA Table

Invoking the `JpdContext.trackData(payload)` method generates an event of type `EVENT_TYPE_PROCESS_LOG`. If the data is transmitted to the reporting database, each event is stored as a new row in the `WLI_DOCUMENT_DATA` table. The *`payload`* is stored in the `DATA` column of that table, and the `EVENT_DATA_ID` column provides a link to the event in the `WLI_PROCESS_EVENT_ARCH` table.

In addition to containing the results of `trackData()`, the `WLI_DOCUMENT_DATA` table contains unhandled exceptions generated by the process instance and business message payloads (if business messages are tracked).

The valid types for `WLI_DOCUMENT_DATA.TYPE` are defined in com.bea.wli.management.archiving.DocumentDataType.

For additional information about:

- The `trackData()` method, see JpdContext interface the WebLogic Workshop help.
- Configuring business message tracking, see "Configuring the Mode and Message Tracking" on page 9-10.

Example Queries

The following example queries are provided:

- Get the Average Elapsed Time for a Process
- Get the Average Elapsed Time for a Node
- Get Results of the trackData() API

Note: See com.bea.wli.management.archiving.TrackingEventType for the constant field value for each event type. For example, in the following examples, `3` corresponds to `EVENT_TYPE_PROCESS_ACTIVITY_END` and `20` corresponds to `EVENT_TYPE_PROCESS_LOG`.

Get the Average Elapsed Time for a Process

To get the average elapsed time for a given process on a given day, the SQL query is:

```
SELECT AVG(EVENT_ELAPSED_TIME) FROM WLI_PROCESS_EVENT_ARCH
WHERE PROCESS_TYPE = PROC_TYPE
AND ACTIVITY_ID = 0
AND EVENT_TYPE = 3
AND (EVENT_TIME >= START_TIME AND EVENT_TIME < END_TIME)
AND DEPLOYMENT_ID IN
       (SELECT MAX(DEPLOYMENT_ID)
       FROM WLI_PROCESS_EVENT_ARCH
       WHERE PROCESS_TYPE = PROC_TYPE)
```

In this query, *PROC_TYPE* should be replaced by a value from the `WLI_PROCESS_EVENT_ARCH` table, and *START_TIME* and *END_TIME* should be literal timestamps.

Get the Average Elapsed Time for a Node

To get the average elapsed time for a given node in a given process on a given day, the SQL query is:

```
SELECT AVG(WPEA.EVENT_ELAPSED_TIME)
FROM WLI_PROCESS_EVENT_ARCH WPEA, WLI_PROCESS_DEF_ARCH WPDA
WHERE WPEA.PROCESS_TYPE = PROC_TYPE
AND WPEA.EVENT_TYPE = 3
AND (WPEA.EVENT_TIME >= START_TIME and WPEA.EVENT_TIME < END_TIME)
AND WPEA.PROCESS_TYPE = WPDA.PROCESS_TYPE
AND WPEA.ACTIVITY_ID = WPDA.ACTIVITY_ID
AND WPEA.DEPLOYMENT_ID = WPDA.DEPLOYMENT_ID
AND WPDA.USER_NODE_NAME = NODE_NAME
AND WPDA.DEPLOYMENT_ID IN
       (SELECT MAX(DEPLOYMENT_ID) FROM WLI_PROCESS_DEF_ARCH
       WHERE PROCESS_TYPE = PROC_TYPE)
```

In this query, *PROC_TYPE* and *NODE_NAME* should be replaced by values from the `WLI_PROCESS_EVENT_ARCH` table, and *START_TIME* and *END_TIME* should be literal timestamps.

Get Results of the trackData() API

To get the result of all `trackData()` calls for a given process type, the SQL query is:

```
SELECT WDD.DATA, WDD.TYPE, WPEA.PROCESS_INSTANCE
FROM WLI_DOCUMENT_DATA WDD, WLI_PROCESS_EVENT_ARCH WPEA
WHERE WDD.EVENT_DATA_ID = WPEA.EVENT_DATA_ID
```

```
AND WPEA.PROCESS_TYPE = PROC_TYPE
AND WPEA.EVENT_TYPE = 20
```

In this query, *PROC_TYPE* should be replaced by a value from the WLI_PROCESS_EVENT_ARCH table.

APPENDIX C

Accessing Process Graphs from HTTP Clients

The interactive process graph, and the associated process type or process instance data, which can be viewed from within the WebLogic Integration Administration Console (see "Viewing an Interactive or Printable Process Type Graph" on page 3-20 or "Viewing an Interactive or Printable Process Instance Graph" on page 4-20), can also be accessed from other HTTP clients. This section describes the how to access the process graph. The following topics are provided:

Supported Clients

The following types of clients are supported:

- Web browsers with an SVG plug-in
- Java client applications using custom SVG tools, such as the Apache Batik toolkit.

The HTTP Request URL

The WebLogic Integration Administration Console Web application accepts HTTP requests (containing Service URI and Instance ID) from a client and returns an SVG document. The client fetches related JavaScript and image files via subsequent requests to the Web application. Both web browser clients (using an SVG plug-in) and Java client applications (using SVG tools) are supported.

The primary command has the following form:

```
http://localhost:7001/wliconsole/procgraph?com=procgraph&serviceuri=ServiceURI
&instanceid=InstanceID
```

For example:

```
http://localhost:7001/wliconsole/procgraph?com=procgraph&serviceuri=%2Fwlitest
%2Fmy_process.jpd&instanceid=1063226907001
```

If you omit `&instanceid=InstanceID`, the SVG document for the process type is returned.

The SVG document that is initially retrieved from the Web application references additional resources on the server such as images and JavaScript files. These additional resources are retrieved automatically by most browser plug-ins by processing the `xlink:href` attributes in the SVG document.

APPENDIX D

Using the Trading Partner Bulk Loader

The Bulk Loader is a command line tool that you can use to import, export, and delete trading partner management (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

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 E, "TPM Schema."

To learn about setting up keystore information and the transaction processing options in the `BulkLoaderConfig.xsd`, see "Transaction Processing Options" on page D-5 and "Importing or Exporting Certificate Elements" on page D-7.

Configuring the Bulk Loader Configuration File

The Bulk Loader uses a 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 D-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> [-nokeyinfo] [-select <selector.xml>]

-delete <selector.xml>
```

The following table summarizes the options for the Bulk Loader commands.

Table D-1 Bulk Loader Commands

Option	Description
`[-verbose]`	Optional. Use verbose mode to help you troubleshoot problems in your import, export, or delete process.
`[-config <blconfig.xml>]`	Optional. Use to designate an explicit configuration file. Default is `blconfig.xml`. If not using the default, specify the full path of the configuration file.
`[-wlibc]`	Optional. Use when you import and export an XML file for use by a trading partner using WebLogic Integration - Business Connect.
`-import <data.xml>`	Use to import data. Specify the full path of the TPM file you want to import. To learn more about importing, see "Importing and Exporting Trading Partner Management Data" on page D-5.

`-export <data.xml>`
`[-nokeyinfo]`
`[-select <selector.xml>]`
	Use to export data. Specify the full path of the TPM file you want to export.
	The `[-nokeyinfo]` option suppresses export of `KeyInfo` elements for trading partner certificates.
	The `-select` option specifies the selector file and `selector.xml` specifies the type of data to be exported. You can use the `selector.xml` 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 `TPM.xsd` schema.
	To learn more about exporting, see "Importing and Exporting Trading Partner Management Data" on page D-5.

`-delete <selector.xml>`	Use to delete data. Specify the full path of the TPM file used for selecting the elements to be deleted. Use `selector.xml` to specify the elements that you want to delete. This file must conforms to the `TPM.xsd` schema. To learn more about deleting, see "Deleting Management Data" on page D-10.

Importing and Exporting Trading Partner Management Data

You can import or export trading partner 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 D-7. 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 conforms 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> [-nokeyinfo] [-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; certificates for 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/xmldsig-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 D-2 blconfig.xml with Keystore Information

```
<?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>
    <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 D-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=#160d706565723140626561 2e636f6d,
    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=#160d706565723140626561 2e636f6d,
    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=#1610676172696d656c73406265612e636f6,
  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
hMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMSYwJAYDVQQKEx1
FQ0kgRGl2aXNpb24sIEJFQSBTeXN0ZW1zIEluYzERMA8GA1UECxMIV0xDIEx1a2UxFTATBgNVB
AMTDGx1a2UuYmVhLmNvbTEfMB0GCSqGSIb3DQEJARYQZ2FyaW1lbHNAYmVhLmNvbTAeFw0wMjA
xMDEwMDAwMDBaFw0wMzAxMDEwMDAwMDBaMIGOMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fsa
WZvcm5pYTEUMBIGA1UEChMLQkVBIFN5c3RlbXMxFTATBgNVBAsTDEVDSSBEaXZpc2lvbjEfMB0
GA1UEAxMWbG9jYWxob3N0LnBlZXIxLWVuLmNydDEcMBoGCSqGSIb3DQEJARYNcGVlcjFAYmVhL
mNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC3+QMrol7OTZ7fWTacxAxqA+5ewLnp1/XxhbQ
pGpBrz1Duj8fw7ybot04fkfQbJgRQEP6M3TyWBmoJAwMBkIbrAgMBAAGjGjAYMAkGA1UdEwQCM
AAwCwYDVR0PBAQDAgXgMA0GCSqGSIb3DQEBBAUAA0EAA8QAs20bOFvebMd6mU6ui7lAYZd+5+d
OhTU0R03VgY35ZQXzyaOH7GtMHNOomFqKaRdckwAi75FZTuAfKVYJfw==
</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 D-1.

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 Web 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.

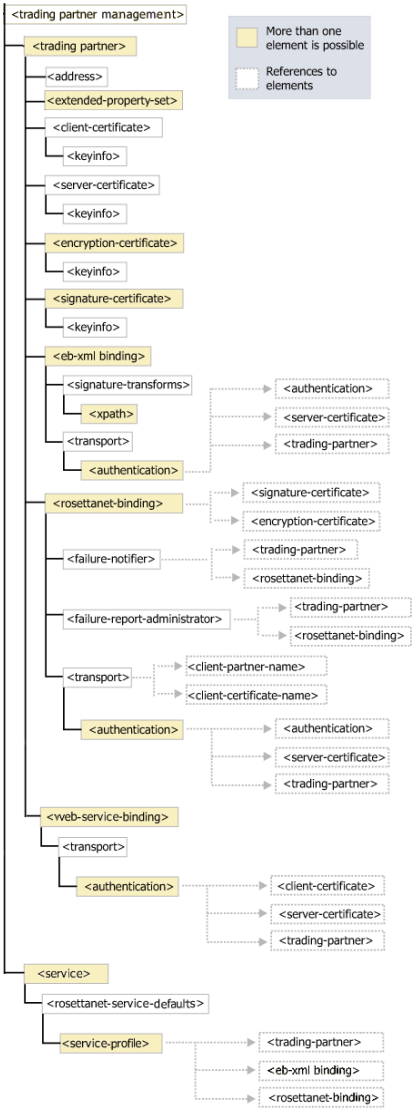
- `service`—a business process a trading partner offers

  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.


<trading partner management>
More than one element is possible
References to elements
<trading partner>
<address>
<extended-property-set>
<client-certificate>
<keyinfo>
<server-certificate>
<keyinfo>
<encryption-certificate>
<keyinfo>
<signature-certificate>
<keyinfo>
<eb-xml binding>
<signature-transforms>
<xpath>
<transport>
<authentication>
<authentication>
<server-certificate>
<trading-partner>
<rosettanet-binding>
<signature-certificate>
<encryption-certificate>
<failure-notifier>
<trading-partner>
<rosettanet-binding>
<failure-report-administrator>
<trading-partner>
<rosettanet-binding>
<transport>
<client-partner-name>
<client-certificate-name>
<authentication>
<authentication>
<server-certificate>
<trading-partner>
<web-service-binding>
<transport>
<authentication>
<client-certificate>
<server-certificate>
<trading-partner>
<service>
<rosettanet-service-defaults>
<service-profile>
<trading-partner>
<eb-xml binding>
<rosettanet-binding>

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 10-6.

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 E-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 E-54.

Related Topics

To learn more about using the WebLogic Integration Administration Console for TPM, see "Trading Partner Management" on page 9-1.

To learn more about Workshop trading partner integration controls, see TPM Control, RosettaNet Control, and ebXML Control in *Building Integration Applications* in the WebLogic Workshop help.

To learn more about using the Bulk Loader, see "Using the Trading Partner Bulk Loader" on page D-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		
client-authentication	**Description**	Specifies whether to use client authentication, and if so, what kind.
	Allowable Values	BASIC—username and password NONE—no authentication SSL_CERT_MUTUAL—mutual SSL certificates
	Use	optional
	Type	xs:NMTOKEN
	Default Value	none
client-certificate-name	**Description**	A reference to the name of the client certificate for mutual SSL authentication.
	Allowable Values	any
	Use	optional
	Type	reference
	Default Value	none
client-partner-name	**Description**	The name of the trading partner in the TPM repository to which the authentication applies.
	Allowable Values	any
	Use	required
	Type	reference
	Default Value	none

Attribute		
password-alias	**Description**	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 nis used.
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	none
server-authentication	**Description**	Specifies whether to use server authentication, and if so, what kind.
	Allowable Values	`NONE`—no authentication `SSL_CERT`—SSL certificate authentication
	Use	optional
	Type	`xs:NMTOKEN`
	Default Value	no default value
server-certificate-name	**Description**	A reference to the name of the server certificate for SSL authentication.
	Allowable Values	any
	Use	optional
	Type	`reference`
	Default Value	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

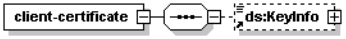
Used By

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

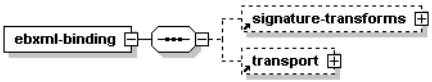
Used By

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 **Note:** Currently `1.0` and `2.0` are supported.
	Use	optional
	Type	`xs:string`
	Default Value	none

Attribute		
delivery-semantics	**Description**	This attribute specifies reliable messaging behavior.
	Allowable Values	BESTEFFORT—best effort attempt to deliver messages. No reliable messaging. ONCEANDONLYONCE—Once and only once reliable messaging. Select this option for messaging that requires acknowledgement. ATLEASTONCE—at least once reliable messaging. Select this option for messaging that requires acknowledgement, but not duplicate elimination. ATMOSTONCE—at most once reliable messaging. Select this option for messaging that requires duplicate elimination, but not acknowledgement. For ebXML 1.0, only BESTEFFORT or ONCEANDONLYONCE are valid. For ebXML 2.0, all values are valid.
	Use	optional
	Type	xs:NMTOKEN
	Default Value	false

Attribute		
is-default	**Description**	Identifies the default `ebxml-binding` for a trading partner in the event it has more than one.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	none
is-receipt-signature-required	**Description**	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. You can control the archival of signed receipts in a secure audit log by the global attribute `secure-audit-logging` in the root element `trading-partner-management`.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	none

Attribute		
is-signature-required	**Description**	This setting, if true, specifies that parties must digitally sign messages they send to the trading partner though this binding. You can control the archival of signed messages in a secure audit log by the global attribute `secure-audit-logging` in the root element `trading-partner-management`.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	none
persist-duration	**Description**	Specifies the duration for which messages have to be stored persistently for the purpose of duplicate elimination.
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	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 timeout period for message acknowledgement expires.
	Allowable Values	time duration string
	Use	optional
	Type	`xs:string`
	Default Value	none
signature-certificate -name	**Description**	References the name of the certificate for digitally signing messages.
	Allowable Values	any
	Use	optional This setting is required if the `is-signature-required` or `is-signature-receipt-required` attributes are true.
	Type	`reference`
	Default Value	none

Reference

To

signature-certificate Element

From

service-profile Element

Hierarchy

Used By

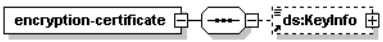
trading-partner Element

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		
name	**Description**	The name of the encryption 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
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

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		
`binding-name`	**Description**	References the name of the service 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

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

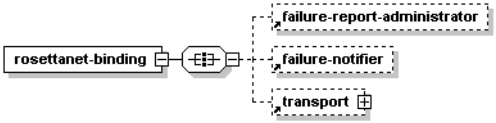
rosettanet-binding Element

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|RC2]"
       encryption-level="[NONE|PAYLOAD|ENTIRE_PAYLOAD]"
       is-signature-required="[true|false]"
       is-receipt-signature-required="[true|false]"
       signature-digest-algorithm="[SHA-1|MD5|None]"
       signature-certificate-name="signatureCertificateName"
       retries="noOfRetries"
       retry-interval="retryIntervalNo"
       process-timeout="processTimeoutNo">
       <failure-report-administrator/>
       <failure-notifier
       .
       .
       .
       />
       <transport
       .
       .
```

```
.
/>
</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		
business-protocol-version	**Description**	Identifies the version of the `business-protocol` name.
	Allowable Values	`1.1` `2.0`
	Use	optional
	Type	`xs:string`
	Default Value	none
is-default	**Description**	Identifies the default `rosettanet-binding` for a trading partner in the event it has more than one.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false
encryption-certificate-name	**Description**	The name of the encryption certificate for the encryption and decryption of messages.
	Allowable Values	any
	Use	optional
	Type	`reference`
	Default Value	none

Attribute		
cipher-algorithm	**Description**	The cipher algorithm for encrypting messages.
	Allowable Values	NONE RC5 DES TRIPLE_DES RC2
	Use	optional
	Type	xs:NMTOKEN
	Default Value	none
encryption-level	**Description**	This attribute determines how much of a message to encrypt.
	Allowable Values	NONE PAYLOAD ENTIRE_PAYLOAD
	Use	optional
	Type	xs:NMTOKEN
	Default Value	none

Attribute		
is-signature-required	**Description**	This setting, if true, specifies that parties must digitally sign messages they send to the trading partner though this binding. You can control the archival of signed messages in a secure audit log by the global attribute `secure-audit-logging` in the root element `trading-partner-management`.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false

Attribute		
is-receipt-signature -required	**Description**	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. You can control the archival of signed receipts in a secure audit log by the global attribute `secure-audit-logging` in the root element `trading-partner-management`.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false

Attribute		
signature-digest-algorithm	**Description**	This setting specifies the message digest algorith used for the digital signature.

	Allowable Values	`SHA-1`
		`MD5`
		`None`
		If the vaule is `SHA-1`, `None`, or null, the Secure Hash Algorithm 1 (SHA-1), which produces a 160-bit hash, is used.
		If the value is `MD5`, the Message Digest 5 (MD5) message hash algorithm, which produces a 128-bit hash, is used.

	Use	optional
	Type	`xs:NMTOKEN`
	Default Value	NONE
signature-certificate-name	**Description**	References the name of the certificate for digitally signing messages.
	Allowable Values	any
	Use	optional This setting is required if the `is-signature-required` or `is-signature-receipt-required` attributes are true.
	Type	`reference`
	Default Value	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	The XML schema for content validation. The service uses this schema only if `use-dtd-validation` is false and `validate-service-content` is true.
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	none
use-dtd-validation	Description	Specifies the kind of XML validation to perform. If true, the validation is from a DTD; if false, from XML schema.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false
validate-service-content	Description	Determines whether to validate the service content of all messages.
	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

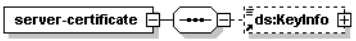
Used By

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

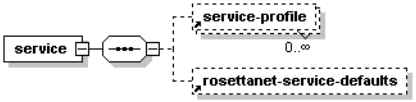
Used By

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		
`service-type`	**Description**	The kind of service the element represents
	Allowable Values	WEBSERVICE—a JWS file PROCESSS—a JPD file SERVICECONTROL—a service control (JCX file)
	Use	optional
	Type	`xs:NMTOKEN`
	Default Value	none
`business-protocol`	**Description**	The business protocol for the service, which determines the child service profile bindings.

	Allowable Values	`WEBSERVICE`
		`EBXML`
		`ROSETTANET`

	Use	optional
	Type	`xs:NMTOKEN`
	Default Value	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**	This attributes references either: • the name of a local trading partner that hosts a JWS or JPD • the name of a local trading partner that uses a control to send messages to an external partner If you do not provide a value in the repository for this attribute, at runtime the value for this property comes from the `is-default` attribute.
	Allowable Values	any
	Use	optional
	Type	`reference`
	Default Value	none
`local-binding`	**Description**	References the name of the binding for the corresponding local trading partner. If you do not provide a value for this attribute, at runtime the value property comes from the binding with the `is-default` value of true.
	Allowable Values	any
	Use	optional
	Type	`reference`
	Default Value	none

Attribute		
external-trading-partner	**Description**	References the name of the trading partner with which the local trading partner interacts. This attribute can describe: • Remote trading partners • Collocated local trading partners
	Allowable Values	none
	Use	required
	Type	`reference`
	Default Value	none
external-binding	**Description**	References the binding name for the corresponding `external-external-trading` partner.
	Allowable Values	any
	Use	optional
	Type	`reference`
	Default Value	none
status	**Description**	The deployed state of the service profile.
	Allowable Values	`ENABLED` `DISABLED`
	Use	optional
	Type	`xs:NMTOKEN`
	Default Value	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
       .
       .
       .
       />
```

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		
`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

ebxml-binding Element

rosettanet-binding Element

Hierarchy

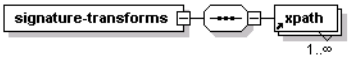
Used By

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

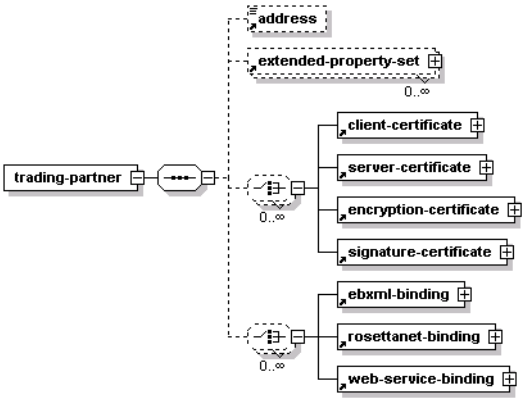
Used By

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		
name	**Description**	Name for the trading partner in the repository.
	Allowable Values	any
	Use	required
	Type	`xs:string`
	Default Value	none
description	**Description**	A short text description of the trading partner 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 of the trading partner.
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	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		
is-default	**Description**	This setting indicates whether or not the trading partner is the default trading partner for sending and receiving messages for the local host system. This attribute can be set to true for trading partners with a `type` attribute of `LOCAL` only. Only one `LOCAL type` trading partner can have this value set to `true`.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false
business-id-type	**Description**	Identifies the type for naming convention for the associated `business-id` attribute. For example, a trading partner that is registered with Dun and Bradstreet might use a value of "`DUNS`".
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	none
business-id	**Description**	Uniquely identifies the trading partner in message exchanges according to the `business-id-type`.
	Allowable Values	any
	Use	optional
	Type	`xs:string`
	Default Value	none

Attribute		
email	Description	An email address for the trading partner.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
phone	Description	A telephone number for the trading partner.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
fax	Description	A fax telephone number for a trading partner.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	none
username	Description	The username in the WebLogic Integration security configuration that represents the trading partner.
	Allowable Values	any
	Use	optional
	Type	xs:string
	Default Value	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

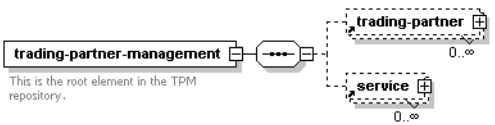
signature-certificate Element

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		
message-trace	**Description**	Toggles message tracing on and off.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	false
message-trace-directory	**Description**	The directory location where messages logs reside.
	Allowable Values	`false` `true`
	Use	optional
	Type	`xs:boolean`
	Default Value	none
secure-audit-logging	**Description**	Specifies whether signed messages reside in a secured audit log.
	Allowable Values	true, false
	Use	optional
	Type	`xs:boolean`
	Default Value	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

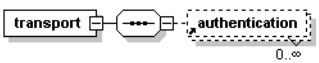
none

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 recieving 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

Hierarchy

Used By

ebxml-binding Element

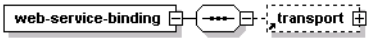
rosettanet-binding Element

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 `web-service-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

References

To

none

From

service-profile Element

Hierarchy

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

Hierarchy

Used By

signature-transforms Element

Children

none