Oracle® WebLogic Integration

Using the WebLogic Integration Administration Console

10*g* Release 3 (10.3)

November 2008

ORACLE®

Oracle WebLogic Intergation Using the Oracle WebLogic Integration Administration Console , 10*g* Release 3 (10.3)

Contents

Process Instance Monitoring

Message Broker

Event Generators

Trading Partner Management

System Configuration

XML Cache

Introducing the Oracle WebLogic Integration Administration Console

The Oracle WebLogic Integration Administration Console allows you to manage and monitor the entities and resources required for your Oracle WebLogic Integration applications.

Starting the Oracle WebLogic Integration Administration Console

Access to the Oracle WebLogic Integration Administration Console is password protected. Before you start the server, you need to create a WLI domain using the Configuration Wizard. For more information, see "Creating a new WebLogic Domain" in *Creating WebLogic Domains Using the Configuration Wizard*.

To start the WLI Administration 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 Oracle WebLogic Server administrative server, and `port` is the server listening port. For example type the following to open the WLI Administration Console: `http://localhost:7001/wliconsole`.

2. Enter the username and password in the **WLI Administration Console** window.

    Note: The user must be a member of the Administrators, IntegrationAdministrators, IntegrationOperators, or IntegrationMonitors group. For more information, see "About WebLogic Integration Users, Groups, Roles, and Security Policies" in Using Worklist Console. If this is the sample integration domain, the default login is:

username: weblogic
password: weblogic

The Oracle WebLogic Integration Administration Console home page is displayed.

Figure 1-1 Oracle WebLogic Integration Administration Console - Home Page
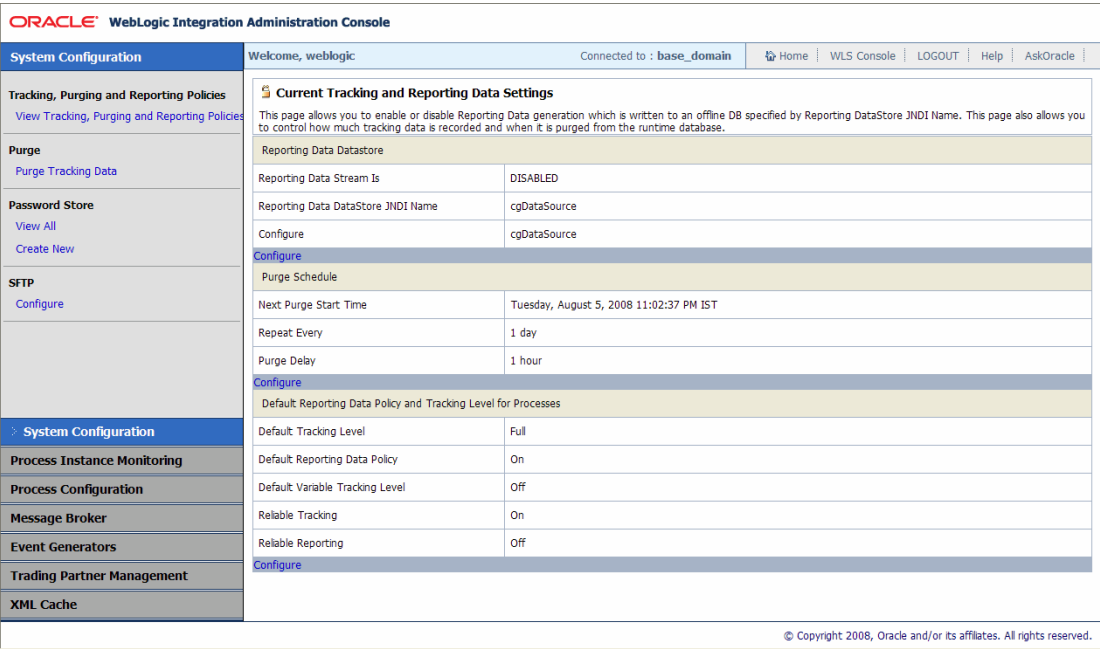
The tool bar on top of the home page contains the following links:

- Home: To return to the home page at any time during the session. If the console is idle for a period of time, you are automatically logged off.

- WLS Console: To invoke the Oracle WebLogic Server Console in a new window.

- LOGOUT: To log out of the WLI Administration Console.

- Help: To access the online help at any time.

- Ask Oracle: To directly contact the Oracle Support team for any clarifications or questions you may have regarding the WLI Administration Console.

This tool bar is available on every page regardless of the module you are accessing in the WLI Administration Console.

The panel to the left side of the screen (left navigation menu) provides access to the modules of the console. The left navigation menu contains the following links:

- System Configuration

- Process Instance Monitoring

- Process Configuration

- Message Broker

- Event Generators

- Trading Partner Management

- XML Cache

This panel is available on every page regardless of the module you are accessing in the WLI Administration Console. You can use this panel to navigate to any of the modules whenever required.

The following table lists the modules of the WLI Administration Console and summarizes the tasks associated with each module.

Table 1-1 Modules of Oracle WebLogic Integration Administration Console

Module	Associated Tasks
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 Data Policy and Tracking Level for Processes 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 SFTP
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, and Unfreezing Process Instances
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 and Changing Dynamic Client Callback Selectors Updating Security Policies Adding and Changing Dynamic Control Selectors Defining Process Control Properties for a Selector Defining Service Broker Control Properties for a Selector Defining ALSB Control Properties for a Selector Deleting Dynamic Control Selectors
Message Broker	Listing and Locating Channels Viewing Channel Details and Subscriptions Setting Channel Security Policies Viewing Global Message Counts Resetting Message Counts

Table 1-1 Modules of Oracle WebLogic Integration Administration Console

Module	Associated Tasks
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 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 Counters
	Deleting Channel Rules
	Deleting Event Generators

Table 1-1 Modules of Oracle WebLogic Integration Administration Console

Module	Associated Tasks
Trading Partner Management	Configuring Trading Partner Management
	Configuring 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
	Editing Trading Partner Profiles
	Listing and Locating Trading Partners
	Listing and Locating Services
	Viewing and Changing Trading Partner Profiles
	Viewing and Changing Certificates
	Enabling and Disabling Trading Partner and Service Profiles
	Viewing and Changing a Custom Extension
	Viewing and Changing Services
	Viewing and Changing Service Profiles
	Importing and Exporting Data
	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
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

Common Logging and WebLogic Diagnostic Framework

The Oracle WebLogic Administration Console uses the logging services of Oracle Weblogic Server. We can configure logging services using Oracle WebLogic Server. For more information, see Configuring WebLogic Logging Services in *Configuring Log Files and Filtering Log Messages*.

We can monitor the process instances with MBeans by configuring diagnostic services using Oracle Weblogic Server Administration Console. The Weblogic Logging and Diagnostic Framework (WLDF) is configured and monitored using configuration and runtime APIs. Both the configuration and runtime APIs are exposed as MBeans.

- The configuration MBeans and system module MBeans create and configure WLDF resources, and determine their runtime behavior.

- The runtime MBeans monitor the runtime state and the operations defined for the different components.

You can use WLDF to configure, activate, and deactivate data collection; to configure watches, notifications, alarms, and diagnostic image captures; and to access data. For more information on diagnostic services, see Configuring and Using the WebLogic Diagnostics Framework.

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. For more information, see "About WebLogic Integration Users, Groups, Roles, and Security Policies" in Using the Worklist Console.

The following topics are provided:

- About Process Configuration

- Overview of the Process Configuration Module

- Listing and Locating Process Types

- Listing and Locating Dynamic Controls

- Viewing and Changing Process Details

- Viewing an Interactive or Printable Process Type Graph

- Managing Process Versions

- Adding and Changing Dynamic Client Callback Selectors

- Updating Security Policies

- Adding and Changing Dynamic Control Selectors

- Defining Process Control Properties for a Selector

- Defining Service Broker Control Properties for a Selector

- Defining ALSB Control Properties for a Selector

- Deleting Dynamic Control Selectors

About Process Configuration

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

- Managing Process Tracking Data

- Process Security Policies

- Service Level Agreements

- Process Versions

- Dynamic Controls

Managing Process Tracking Data

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

- Capturing only the necessary data.

- 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.

Table 2-1 System Properties and Configuration tasks

Property	Configuration Task	Task Type and Reference
Default Tracking Level	Set the system default tracking level.	System Configuration. For more information, see "Configuring the Default Data Policy and Tracking Level for Processes" on page 7-13.
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. For more information, see "Viewing and Changing Process Details" on page 2-13.
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. For more information, see "Configuring the Reporting Data and Purge Processes" on page 7-10.

Table 2-1 System Properties and Configuration tasks (Continued)

Property	Configuration Task	Task Type and Reference
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. For more information, see "Configuring the Reporting Data and Purge Processes" on page 7-10.
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. For more information, see "Configuring the Reporting Data and Purge Processes" on page 7-10.
Default Reporting Data Policy	Set the system default reporting data policy to **On** or **Off**.	System Configuration. For more information, see "Configuring the Default Data Policy and Tracking Level for Processes" on page 7-13.
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 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. For more information, see "Viewing and Changing Process Details" on page 2-13

To learn more, see the following topics:

- "Process Tracking Data" on page 7-3.

- "Reporting and Purging Policies for Tracking Data" on page 7-4

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 .

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 OracleWebLogic Integration Administration Console allows you to set the following thresholds:

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

- SLA warning threshold, which is a percent of the total SLA.

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

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

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

This ability to set SLA thresholds allows you to easily identify processes that do not execute within the target time frame. You can then make the changes necessary to meet agreements between suppliers and customers, or to achieve your own performance goals. To learn how to set the SLA for a process, see "Viewing and Changing Process Details" on page 2-13.

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 *Guide to Building Business Processes*:

- 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 2-24.

Note: Processes that are not versioned can also be enabled and disabled. For more information, see "Viewing and Changing Process Details" on page 2-13. 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 Oracle WebLogic Integration Administration Console override both configuration changes made in the Oracle Workshop for WebLogic development environment and static annotations.

To learn more about the dynamic controls, see the following topics in *Using Integration Controls*:

- Process Control

- Service Broker Control
- ALSB Control

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 of the types are provided in Table 2-2.

Table 2-2 Elements of Process Configuration Module

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, architecture policy, and SLA.	"Listing and Locating Process Types" on page 2-11
	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, architecture policy, SLA), dynamic client callback properties, execution and authorization policies, variables, and active version are displayed.	"Viewing and Changing Process Details" on page 2-13
	Access an interactive and printable graph of the process.	"Viewing an Interactive or Printable Process Type Graph" on page 2-21
	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	

Table 2-2 Elements of Process Configuration Module (Continued)

Page	Associated Tasks	Help Topics
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 2-13
Edit Process Versioning	Enable, disable, or set the activation date and time for the selected version.	"Managing Process Versions" on page 2-24
Add New Client Callback Properties	Add a selector value and properties, which can be used to dynamically configure the callback to the client.	"Adding and Changing Dynamic Client Callback Selectors" on page 2-26
Edit Client Callback Properties	Edit the properties used to dynamically configure the callback to the client.	"Adding and Changing Dynamic Client Callback Selectors" on page 2-26
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 2-30 "Process Security Policies" on page 2-5
Edit Process Authorization Policy	Set the minimum authorized roles for the methods (client requests) in the process.	"Updating Security Policies" on page 2-30 "Process Security Policies" on page 2-5
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 2-30 "Process Security Policies" on page 2-5
Edit Call Back Authorization Policy	Set the authorized roles for the selected callback.	"Updating Security Policies" on page 2-30 "Process Security Policies" on page 2-5

Table 2-2 Elements of Process Configuration Module (Continued)

Page	Associated Tasks	Help Topics
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 2-12
	Delete a selector from the control.	"Deleting Dynamic Control Selectors" on page 2-39
	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 and Changing Dynamic Control Selectors" on page 2-32
Add New Process Control Selector	Define the properties for a new selector.	"Defining Process Control Properties for a Selector" on page 2-33
Edit Process Control Selector	Update the properties for an existing selector.	"Defining Process Control Properties for a Selector" on page 2-33
Add New Service Broker Control Selector	Define the properties for a new selector.	"Defining Service Broker Control Properties for a Selector" on page 2-35
Edit Service Broker Control Selector	Update the properties for an existing selector.	"Defining Service Broker Control Properties for a Selector" on page 2-35
Add New ALSB Control Selector	Define the properties for a new selector.	"Defining ALSB Control Properties for a Selector" on page 2-37
Edit ALSB Control Selector	Update the properties for an existing selector.	"Defining ALSB Control Properties for a Selector" on page 2-37

Listing and Locating Process Types

The **Process Property Summary** page displays the following information for each deployed process type. For a more detailed description of the properties, see "Viewing and Changing Process Details" on page 2-13.

Figure 2-1 Process Property Summary

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

Display Name	Public URI	State	Tracking Level	Arch.Policy	SLA
Process	/myb2bWeb/processes/Process.jpd	Stateless	Default	Default	NA
RoundtripBuyer	/myb2bWeb/ebxml/RoundtripBuyer.jpd	Stateful	Default	Default	NA
RoundtripSeller	/myb2bWeb/ebxml/RoundtripSeller.jpd	Stateless	Default	Default	NA

Table 2-3 Elements of Process Property Summary Page

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.
Architecture Policy	The architecture policy set for tracking data.
SLA	Service level agreement set for the process.

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 2-13

- "Updating Security Policies" on page 2-30

- "Adding and Changing Dynamic Control Selectors" on page 2-32

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 and Changing Dynamic Control Selectors" on page 2-32.

Figure 2-2 View Dynamic Control Properties

View Dynamic Control Properties					
This page displays all the dynamic controls and selectors defined for each control. To edit properties associated with each selector, click Edit. To add a new selector, click Add Selector. To delete a selector, click Delete.					
			Items 1-1 of 1	|◀ ◀ 1 ▶ ▶|
Context Path	**Control Name** ⌃	**Control Type**	**Selector Value**	**Edit**	**Delete**
/SBCTestW	processes.NewSBTestC Add Selector	ServiceBrokerControl	No Data		
			Items 1-1 of 1	|◀ ◀ 1 ▶ ▶|

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:

   – Re-sort 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 2-7
- "Adding and Changing Dynamic Control Selectors" on page 2-32

Viewing and Changing Process Details

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

Figure 2-3 Process Type Details Page

Process Type Details	
This page displays details about a process type such as configuration information, variable definitions, and security-related properties.	
Process Type Details	
Service URI	/myb2bWeb/processes/Process.jpd
Application Name	myb2bEar
Stateful/Stateless	Stateless
Description	
Version Group URI	This process is not part of a version group
Process Graph	Interactive View Printable View
Configurable Properties	
Display Name	Process
Tracking Level	Default
Reporting Data Policy	Default
SLA	NA
SLA Warning Threshold	NA
Save Process Variable Values on Completion	Default
Is Enabled	true
Activation Date	January 1, 1970 5:30:00 AM IST
Deactivation Date	NA
Configure	
Execution Policy	
Run As	caller's identity
Single Principal Required	No

Figure 2-4 Process Type Details Page (Continued)

Process Authorization Policy	
Authorized Roles	

Method Authorization Policy
No configurable method found

Control Callback Authorization Policy
No configurable control callback found

Variables

Items 0-0 of 0	|◁ ◁ ▷ ▷|
Variable Name	**Declared Type**
No matching data found.	
Items 0-0 of 0	|◁ ◁ ▷ ▷|

4. To update configurable properties, do the following:

a. In the **Configurable Properties** section, click **Configure** to display the **Edit Process Properties** page.

Figure 2-5 Edit Process Properties

b. Set the properties as required. The properties are described in Table 2-4.

c. Click **Submit** to update the properties and return to the **Process Type Details** page.

5. For information on how to enable, disable, or activate a version, see "Managing Process Versions" on page 2-24.

6. For information on how to configure dynamic client callback properties, see "Adding and Changing Dynamic Client Callback Selectors" on page 2-26.

7. For information on how to update the execution policy, process authorization policy, or method authorization policy, see "Updating Security Policies" on page 2-30.

Table 2-4 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.

Table 2-4 Elements of Process Type Details page

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 *Guide to Building Business Processes*.	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. For more information, see "Viewing an Interactive or Printable Process Type Graph" on page 2-21.	No
Configurable Properties		

Table 2-4 Elements of Process Type Details page

Property	Description	Administrator Can Set (Yes/No)
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
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). For more information, see "Configuring the Default Data Policy and Tracking Level for Processes" on page 7-13.	
	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. For more information, see "Reporting and Purging Policies for Tracking Data" on page 7-4.	

Table 2-4 Elements of Process Type Details page

Property	Description		Administrator Can Set (Yes/No)
Save Process Variable Values on Completion	**On**	Process variable values are saved when the process is complete.	Yes
	Off	Process variable values are not saved when the process is complete.	
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 2-6.		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			

Table 2-4 Elements of Process Type Details page

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

Table 2-4 Elements of Process Type Details page

Property	Description		Administrator Can Set (Yes/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. For more information, see "Managing Process Versions" on page 2-24.	
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

Table 2-4 Elements of Process Type Details page

Property	Description	Administrator Can Set (Yes/No)
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 3-22

- "Updating Security Policies" on page 2-30

- "Adding and Changing Dynamic Control Selectors" on page 2-32

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. For more information, see "Viewing an Interactive or Printable Process Instance Graph" on page 3-22.

Note: The interactive process graph requires Adobe SVG Viewer Version 3.0 or Java Batik 1.7 SVG. To learn more, see "Requirements for the Interactive Graph" on page 3-4. The printable graph requires a PDF viewer such as Adobe Acrobat. We recommend that you use Java Batik to view the interactive process graph, if your browser does not support Adobe SVG Viewer.

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

1. Locate the process to view. For more information, see "Listing and Locating Process Types" on page 2-11.

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.

1. Verify that your browser meets the requirements. For more information, see "Requirements for the Interactive Graph" on page 3-4.

2. Locate the process to view. For more information, see "Listing and Locating Process Types" on page 2-11.

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.
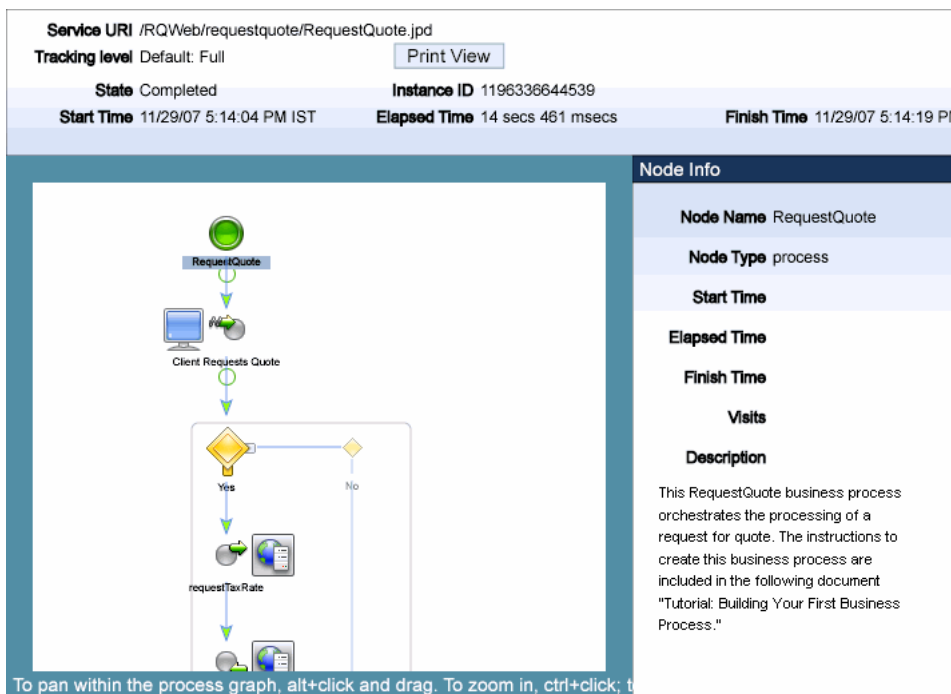
Java Batik SVG Viewer displays the interactive view as shown in the following figure.
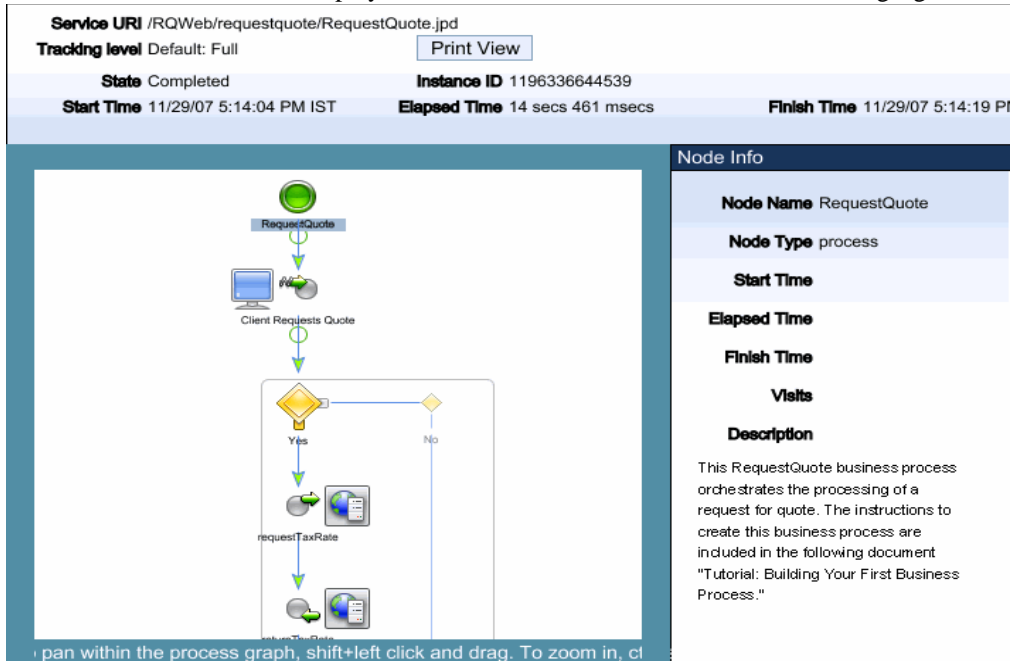
5. For Adobe SVG Viewer, do any of the following:

– 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.

6. If you do not have Adobe SVG Viewer on your system, the WLI Administration Console will display the Interactive view in an Java Batik SVG applet.

> **Note:** To view the java applet in the Java Batik 1.7 SVG viewer you require the Java Runtime Environment 1.6 to be installed in advance and the Sun Java console working with your browser. You can download the Java Runtime Environment 1.6 and the Java console at: http://java.sun.com/javase/downloads/index.jsp

For Java Batik SVG Viewer, do any of the following:

– To display the name, type and description for a node, click the node image.

– To pan within the process graph, **shift**+**left click and drag**.

– To zoom in, press and hold down the **Ctrl** key and select portion for zoom in.

– To zoom out, press and hold down the **Ctrl**+**Shift**+**right click**.

– To change to a printable view, click **Print View**. The process graph is displayed as PDF document.

Related Topics

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

- "Viewing an Interactive or Printable Process Instance Graph" on page 3-22

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.

Figure 2-6 Managing Process Versions

Version group	
Version Group URI	/RQWeb/requestquote/sbExample.jpd
Default Service URI	/RQWeb/requestquote/sbExample_v2.jpd
Current Active	/RQWeb/requestquote/sbExample_v2.jpd

Items 1-2 of 2 |◄   ◄   1   ▷   ▷|

Display Name ⌃	Service URI	Is Enabled	Activation Date	Deactivation Date	Configure
sbExample_v1	/RQWeb/requestquote/sbExample_v1.jpd	false	January 1, 1970 5:30:00 AM IST	January 1, 1970 5:29:59 AM IST	Configure
sbExample_v2	/RQWeb/requestquote/sbExample_v2.jpd	true	January 1, 1970 5:30:00 AM IST	January 1, 1970 5:29:59 AM IST	Configure

Items 1-2 of 2 |◄   ◄   1   ▷   ▷|

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 Oracle WebLogic Server:
```
production noiterativedev nodebug notestconsole
```

1. Locate the process to view. For more information, see "Listing and Locating Process Types" on page 2-11.

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.

Figure 2-7 Edit Process Versioning

🌿 **Edit Process Versioning**	
Version Group URI	/RQWeb/requestquote/sbExample.jpd
Component URI	/RQWeb/requestquote/sbExample_v1.jpd
Is Enabled	☐
Activation Date	January ▼ 1 ▼ 1970 05 ▼ 30 ▼
Deactivation Date	⦿ Never Deactivates January ▼ 1 ▼ 1970 at 05 ▼ 29 ▼

[Submit] [Reset] [Cancel]

4. Define the required settings:

    – To set the activation time, select the month, date, and time from the **Activation Date** drop-down lists.

    – To enable the version, select 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 2-6
- "Viewing and Changing Process Details" on page 2-13

Adding and 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 *Guide to Building Business Processes*.

1. Locate the process. For more information, see "Listing and Locating Process Types" on page 2-11.

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 **Add a new callback property**.

   The **Add New Client Callback Properties** page is displayed.

Figure 2-8 Add New Client CallBack Properties Page

– 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 Table 2-5 summarizes the settings available on the Add New Client Callback Properties and **Edit Client Callback Properties** pages.

Table 2-5 Elements of Edit Client Callback Properties page

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. For more information, see "Password Aliases and the Password Store" on page 7-6.	

Table 2-5 Elements of Edit Client Callback Properties page

Setting	Description	Required/ Optional
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. For more information, see "Password Aliases and the Password Store" on page 7-6.	
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. For more information, see "Password Aliases and the Password Store" on page 7-6.	
In the **Keystore Type** field, enter the keystore type.	The keystore type.	

1. Locate the process. For more information, see "Listing and Locating Process Types" on page 2-11.

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 2-13

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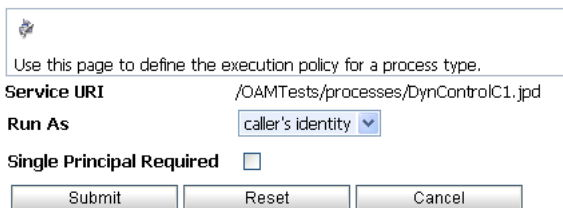
The **Process Type Details** page allows you to set the security policies for the process or its methods and callbacks.

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, For more information, see Security Provider Requirements for User Management in the *Worklist User Guide*.

1. Locate the process to view. For more information, see "Listing and Locating Process Types" on page 2-11.

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.

Figure 2-9 Edit Process Execution Policy

   b. From the **Run As** drop-down list, select **caller's identity** or **start user**.

   c. Check or uncheck the **Single Principal Required** check box.

   d. Click **Submit** to update the properties and return to the **Process Type Details** page.

4. To configure the method authorization policies, do one or more of the following:

– To configure the authorization policy for the process methods, in the **Method Authorization Policy** section, click **Configure**.

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

Figure 2-10 Edit Method Authorization Page

Note: If no roles are specified, everyone is authorized.

Note: All the methods in the process inherit the roles assigned in the authorization policy for the process method. 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.

Figure 2-11 Edit Callback Authorization Policy

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 2-5

- "Viewing and Changing Process Details" on page 2-13

Adding and Changing Dynamic Control Selectors

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

1. Locate the dynamic control to update. For more information, see "Listing and Locating Dynamic Controls" on page 2-12.

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.

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 Oracle 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*

- Process Control, see Process Control in *Using Integration Controls*.

- 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.

Figure 2-12 Add New Process Control Selector Page

The following table summarizes the available settings.

Table 2-6 Elements of Add New Process Control Selector Page

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. For more information, see "Password Aliases and the Password Store" on page 7-6.	Optional

Related Topics

- "Dynamic Controls" on page 2-7

● "Adding and Changing Dynamic Control Selectors" on page 2-32

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 Oracle 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*, and for more information on the Service Broker Control see, Service Broker Control in *Using Integration Controls*.

The **Add New Service Broker Control Selector** and **Edit Service Broker Selector** pages allow you to set the selector value and associated properties.

Figure 2-13 Add New Service Broker Control Selector Page

The following table summarizes the available settings.

Table 2-7 Elements of Add New Service Broker Control Selector page

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 Oracle 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
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

Table 2-7 Elements of Add New Service Broker Control Selector page (Continued)

Setting	Description	Required/ 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. For more information, see "Password Aliases and the Password Store" on page 7-6.	
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. For more information, see "Password Aliases and the Password Store" on page 7-6.	
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. For more information, see "Password Aliases and the Password Store" on page 7-6.	
In the **Keystore Type** field, enter the keystore type.	The keystore type.	

Related Topics

- "Dynamic Controls" on page 2-7

- "Adding and Changing Dynamic Control Selectors" on page 2-32

Defining ALSB Control Properties for a Selector

For more information, see ALSB Control in *Using Integration Controls*.

The **Add New ALSB Control Selector** page allows you to set the selector value, service URI, JNDI URL, user name, and password alias.

Figure 2-14 Add New Process Control Selector Page

The following table summarizes the available settings.

Table 2-8 Elements of Add New ALSB Control Selector Page

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.	Required
In the **Service URI** field, enter the URI for the service.	The URI for the service that is associated with this look up key.	Optional
In the JNDI URL field, enter the JNDI URL for the service.	The JNDI URL for the service	Optional
In the **User Name** field, enter the user name.	The user name (if required) used to invoke the target service.	Optional
In the **Password Alias** field, enter the password alias.	The password alias used to look up the user password in the password store. For more information, see "Password Aliases and the Password Store" on page 7-6.	Optional

Related Topics

- "Dynamic Controls" on page 2-7
- "Adding and Changing Dynamic Control Selectors" on page 2-32

Deleting Dynamic Control Selectors

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

1. Locate the dynamic control to update. For more information, see "Listing and Locating Dynamic Controls" on page 2-12.

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

   The selector is deleted from the list.

Process Configuration

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 "About WebLogic Integration Users, Groups, Roles, and Security Policies" in User Management in *Using the Worklist Console*.

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 2-3.

The following topics are provided:

- Overview of the Process Instance Monitoring Module

- Requirements for the Interactive Graph

- Viewing Instance Statistics by Process Type

- Viewing System Health Statistics

- Listing and Locating Process Instances

- Constructing an Advanced Search

- Viewing Process Instance Details

- Viewing an Interactive or Printable Process Instance Graph

- Suspending, Resuming, Terminating, and 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.

Table 3-1 Elements of Process Instance Monitoring Module

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, above SLA, and above SLA warning) are displayed.	"Viewing Instance Statistics by Process Type" on page 3-8
	Filter the list by URI or display name. Use ? to match any single character or * to match zero or more characters.	

Table 3-1 Elements of Process Instance Monitoring Module

Page	Associated Tasks	Help Topics
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 3-11
	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, and Unfreezing Process Instances" on page 3-24
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 3-13
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 3-9
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 3-16
	Suspend, Resume, Terminate, or Unfreeze the process instance.	"Suspending, Resuming, Terminating, and Unfreezing Process Instances" on page 3-24
	Access an interactive or printable process graph.	"Viewing an Interactive or Printable Process Instance Graph" on page 3-22

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 or Java Batik 1.7. You can download the Adobe SVG viewer from the Adobe Web site (http://www.adobe.com/svg/viewer/install/main.html).

You can download the Java Batik SVG Viewer from the Sun Java Downloads page:

(http://java.sun.com/javase/downloads/index.jsp)

For more information on how to set up the environment, see Enabling Sun JRE for Java Batik SVG Viewer.

The Table 3-2 provides viewer availability by browser and operating system.

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. See http://support.microsoft.com/kb/q287247/ for more details.

Table 3-2 Browser-wise availability of Adobe SVG Viewer

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. For more information, 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.

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.

Enabling Sun JRE for Java Batik SVG Viewer

Java Runtime Environment (JRE) is not enabled by default in the web browser. If the JRE is already installed but applets do not work, you may need to enable the JRE through your web browser.

Please follow these instructions to enable the Sun JRE though your web browser:

Internet Explorer 4.x and Higher

1. Click **Tools > Internet Options**.

2. Select the Advanced Tab, and scroll down to **Java (Sun).**

3. Select the box next to the **Use Java 2** version.

4. Next, select the Security Tab, and select the **Custom Level** button

5. Scroll down to **Scripting of Java applets**

6. Make sure the **Enable** radio button is selected.

7. Click **OK** to save your preference.

Mozilla 1.x

1. From the menu bar, choose **Edit > Preferences.**

2. Select the **Advanced** category.

3. Select the box labeled **Enable Java.**

4. Click **OK** to save your preference.

Netscape 7.x

1. From the menu bar, choose **Edit > Preferences**.

2. Select the **Advanced** category.

3. Select the box labeled **Enable Java**.

4. Click **OK** to save your preference.

Netscape 4.x

1. From the menu bar, choose **Edit > Preferences**.

2. Select the **Advanced** category.

3. Select **Certificates**.

4. Select the box labeled **Enable Java**.

5. Select the box labeled **Enable Java Plug-in**.

6. Click **OK** to save your preference.

Firefox 0.8 and Higher

1. Start Mozilla Firefox browser or restart the browser if it is already running.

2. Select **Tools > Options**.

3. Click **Web Features > Select Enable Java.**

AOL 3.x and Higher

Please refer to the Help page on AOL Issues with Java software.

Opera 4.x and Higher

1. Opera for Windows does not use the Sun JRE, but an embedded version already inside the Opera Web browser.

2. Opera for other platforms may support Java software through the use of the Sun JRE. Please consult your Opera platform documentation.

3. For further information, please review the following Opera Support article:

 Support for Java software in Opera.

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.

1. From the home page, select the **Process Instance Monitoring** module.

Figure 3-1 Process Instance Statistics

Note: For stateless processes, N/A is displayed in the **Running** instance column. These


```
 Process Instance Statistics
This page displays a summary of process instances grouped by the process type. To view instances of a process type, click the process
name.
```

Display Name ⌃	Average.Elapsed ⌄	Running ⌄	Susp. ⌄	Aborted ⌄	Frozen ⌄	Term. ⌄	Comp. ⌄	Above SLA ⌄
RoundtripSeller	0.1 secs	N/A	0	1	0	0	0	N/A
Process	0 ms	N/A	0	0	0	0	0	N/A
RoundtripBuyer	0 ms	0	0	0	0	0	0	N/A
Process	0 ms	0	0	0	0	0	0	N/A
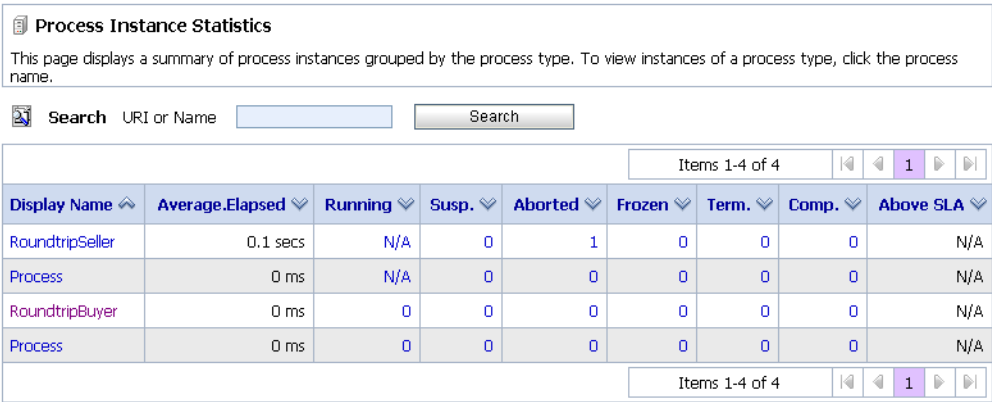
processes start and end in a single transaction.

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. For more information, see "Listing and Locating Process Instances" on page 3-11.

Related Topics

- "Reporting and Purging Policies for Tracking Data" on page 7-4

- "Viewing Process Instance Details" on page 3-16

- "Service Level Agreements" on page 2-6

Viewing System Health Statistics

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

1. From the home page, select the **Process Instance Monitoring** module.

2. From the left panel, select **System Health**.

Figure 3-2 System Health Page

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.

Listing and Locating Process Instances

The **Process Instance Summary** page displays the following information for each process instance. For a more detailed description of the properties, see "Viewing Process Instance Details" on page 3-16.

1. From the home page, select the **Process Instance Monitoring** module.

2. In the left panel, click **View All**.

Figure 3-3 Process Instance Summary Page

Note: The process instances are sorted by start time, the most recent listed first (by default).

Table 3-3 Elements of Process Instance Summary

Property	Description
ID	Process Instance ID. This is a link to the **Process Instance Detail** page. For more information, see "Viewing Process Instance Details" on page 3-16.
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 class in *Javadoc for WebLogic Integration Classes*.
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.

3. To locate a specific process, do one of the following:

– Select a default filter from the **Go** drop-down list. The following figure lists the available options:
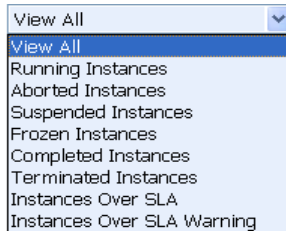
– Filter by instance ID. Enter the required instance ID, then click **Instance ID**. The instance identified is displayed.

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. For more information, see "Constructing an Advanced Search" on page 3-13.

Related Topics

- "Viewing Process Instance Details" on page 3-16

- "Suspending, Resuming, Terminating, and Unfreezing Process Instances" on page 3-24

- "Reporting and Purging Policies for Tracking Data" on page 7-4

Constructing an Advanced Search

The **Advanced Search** page allows you to construct a complex process instance search.

1. From the home page, select the **Process Instance Monitoring** module.

2. In the left panel, click **Advanced Search** to view the **Advanced Search** page.

Figure 3-4 Advanced Search Page

Table 3-4 summarizes the available search criteria available using the Advanced Search page.

Table 3-4 Advanced 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 following figure lists the available options: 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.

Table 3-4 Advanced Search Criteria

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 process instances that have labels containing the specified string. **Note:** Do not use wildcard characters to specify a search target.

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.

1. Locate the process. For more information, see "Listing and Locating Process Instances" on page 3-11.

2. Click the process ID to display the **Process Instance Details** page.

Figure 3-5 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. For more information, see "Requirements for the Interactive Graph" on page 3-4. To learn more about the interactive process view, see "Viewing an Interactive or Printable Process Instance Graph" on page 3-22.

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

Table 3-5 Elements of 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.		
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. For more information, see "Suspending, Resuming, Terminating, and Unfreezing Process Instances" on page 3-24.	
		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 *Guide to Building Business Processes*.	
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 Oracle Workshop for WebLogic help.		

Table 3-5 Elements of Process Instance Detail page (Continued)

Property	Description
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 2-6.
Start Time	Time this instance started.
Exception	Exception content displayed only for a aborted or frozen instance.
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 displayed only for a completed process.
Termination Time	Termination date and time for a process that has been terminated.
Pending Activities	This information is displayed only for 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" />`

Table 3-5 Elements of Process Instance Detail page (Continued)

Property	Description
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 3-20. **Note:** The parent or child instance is only displayed if the tracking level for the process is **Minimum**, **Node**, or **Full**.
Child Instance	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.
Tasks to which this instance is listening	Worklist tasks this process is listening to. The task name and ID are displayed.
B2B Events	Displays summary information for any business messages for B2B events. 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	Displays the Name, type, and value of each variable defined for running instances. You can view the value of an XML or string variable by clicking it.

Parent-Child Navigation

When a process instance calls another process via the Process control, the process invoked is considered a "child process." Information about related processes is available on 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.

Figure 3-6 Process Instance Details

Related Topics

- "Viewing an Interactive or Printable Process Instance Graph" on page 3-22

- "Suspending, Resuming, Terminating, and Unfreezing Process Instances" on page 3-24

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 Oracle Workshop for WebLogic Design View. Visual cues are provided to indicate node status as described in the following table:

Table 3-6 Node Status

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

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

The top panel displays selected process properties. To learn more about the properties displayed, see "Viewing Process Instance Details" on page 3-16. 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. For more information, see "Suspending, Resuming, Terminating, and Unfreezing Process Instances" on page 3-24.

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.

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

1. Locate the process instance to view. For more information, see "Listing and Locating Process Instances" on page 3-11.

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.

4. Verify that your browser meets the requirements. For more information, see "Requirements for the Interactive Graph" on page 3-4.

5. Locate the process instance to view. For more information, see "Listing and Locating Process Instances" on page 3-11.

6. Click the process name to display the **Process Instance Details** page.

7. Click **Graphical View**.

   The Adobe SVG Viewer displays the interactive view.
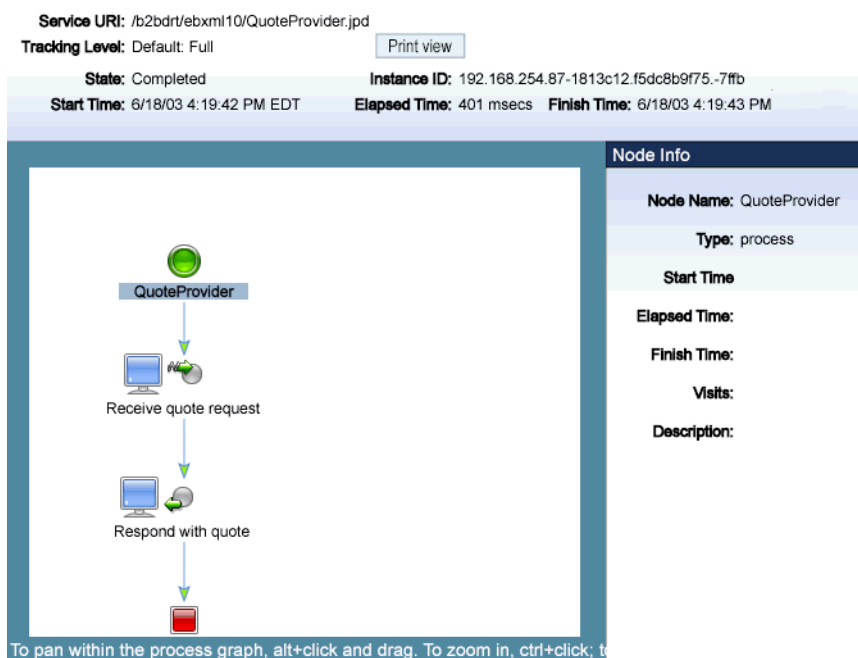
8. Do any of the following:

   – 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 3-4

Suspending, Resuming, Terminating, and 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:

Table 3-7 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 *Guide to Building Business Processes*. The ability to freeze a process 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**

1. Locate the process. For more information, see "Listing and Locating Process Instances" on page 3-11.

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.

5. Display the **Process Instance Summary** page as described in "Listing and Locating Process Instances" on page 3-11.

6. Click the check box to the left of each instance to be suspended, resumed, terminated, or unfrozen.

7. Click **Suspend**, **Resume**, **Terminate**, or **Unfreeze**.

   A confirmation dialog box is displayed.

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

9. Locate the process. For more information, see "Listing and Locating Process Instances" on page 3-11.

10. Click the process name to display the **Process Instance Details** page.

11. Click **Graphical View**.

12. In the top panel of the interactive graph, click **Suspend**, **Resume**, **Terminate,** or **Unfreeze**, as required.

A confirmation dialog box is displayed.

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

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. For more information, see About WebLogic Integration Users, Groups, Roles, and Security Policies in User Management in *Using the Worklist Console*.

The following topics are provided:

● About Message Broker Channels

● Overview of the Message Broker Module

● Listing and Locating Channels

● Viewing Channel Details and Subscriptions

● Setting Channel Security Policies

- Viewing Global Message Counts

- Resetting 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 Oracle WebLogic Integration processes, controls, and event generators. Within a Oracle 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.

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.

Table 4-1 Elements of Message Broker Module

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 4-3
	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 4-4
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 4-8
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 4-10
	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, messages, and dead letters for each channel.

1. From the home page, select the **Message Broker** module to display the **Channel Summary List**.

Figure 4-1 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 4-4

Viewing Channel Details and Subscriptions

You can view channel details and subscriptions on the View Channel Details page.

1. Locate the channel. For more information, see "Listing and Locating Channels" on page 4-3.

2. Click the channel name to display the **View Channel Details** page. The page displays the following properties.

Figure 4-2 View Channel Details

Table 4-2 Elements of View Channel Details page

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

```
<channels xmlns="http://www.bea.com/wli/broker/channelfile"
        xmlns:foo="http://www.foo.com/bar"
        xmlns:fooMeta="http://www.foo.com/barMeta"
        channelPrefix="/myproject">
    <channel name="mygroup" messageType="none">
        <channel name="mytype" messageType="none">
            <channel name="mychannel" messageType="xml">
            </channel>
        </channel>
    </channel>
</channels>
```

Property	Description	Administrator Can Set (Yes/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

Table 4-2 Elements of View Channel Details page

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.	Yes
		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.	
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.	No
		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.	
	Subscriber URI	The URI of the subscriber. For processes, this URI is a link to the **Process Instance Summar**y page.	No

Note: The suppressible attribute works only if the same process contains both static and dynamic subscriptions on the same channel. If two different processes subscribe to a channel, or the same process subcribes to two different channels, the suppressible attribute has no effect.

Setting suppressible to true specifies that the static subscription is suppressed in favor of a dynamic subscription. An instance of the process should already be running and dynamically subscribed. When an event arrives and suppressible is set to true: the message is delivered to the running instance.

No new instances are created if suppressible is set to false: the message is delivered to the running instance. Additionally one new instance of the process is created.

Related Topics

- "Setting Channel Security Policies" on page 4-8

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" in User Management in *Using Worklist Console*.

1. Locate the channel. For more information, see "Listing and Locating Channels" on page 4-3.

2. Click the channel name to display the **View Channel Details** page.

3. Click **Edit Security Details**.

Figure 4-3 Edit Channel Subscribe and Publish Policies

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 though from an anonymous user.

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 ![arrow icon] 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

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.

The **View Message Broker Statistics** page displays the following:

Figure 4-4 View Message Broker Statistics Page

⟳ **View Message Broker Statistics**

This page displays message traffic routed through message brokers, the number of subscribed channels, and message counts.

Number of Active Channels	4
Number of Subscribed Channels	0
Dead Letter Count	0
Message Count	0
Time of Last Reset	Thursday, February 28, 2008 6:10:13 PM IST

Table 4-3 Elements of Message Broker Statistics page

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.

Related Topics

-

Resetting Message Counts

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

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

   The **Channel Summary List** is displayed.

2. Select the check box to the left of every channel that needs to be reset.

   Note: You can filter the list as described in .

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

Message Broker

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. For more information, see "About WebLogic Integration Users, Groups, Roles, and Security Policies" in User Management in *Using Worklist Console*.

The following topics are provided:

- About Event Generators

- Overview of the Event Generator Module

- Creating and Deploying Event Generators

- Defining Channel Rules for a File Event Generator

- Defining Channel Rules for an Email Event Generator

- Defining Channel Rules for a JMS Event Generator

- Defining Channel Rules for a Timer Event Generator

About 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 Oracle 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.

- **TIBCORV event generator**
  Enables Oracle WebLogic Integration to generate events to Message Broker channels. The messages are received in most formats supported by Rendezvous, converted to binary, and published to the Oracle WebLogic Integration Message Broker.

- **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.

- **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 publishes the messages 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, the following rules are configured for a JMS event generator:

Table 5-1 JMS Event Generator - Rules

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.

Table 5-2 Rules - Order Reversed

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:

Table 5-3 Event Generators

Page	Associated Tasks	Help Topics
File		
View All File Event Generators	View a list of file event generators. The 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 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the files read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58
Create a 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 5-13

Table 5-3 Event Generators (Continued)

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 5-18
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-18
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 5-53
	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.The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the emails read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58
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 5-13

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
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 5-27
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-27
JMS		
View All JMS Event Generators	View a list of JMS event generators.	"Listing and Locating Event Generators" on page 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the messages read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58
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 5-13

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
JMS Event Generator Details	Update the default channel rule for the event generator.	"Viewing and Updating Event Generator Channel Rules" on page 5-55
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 5-30
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-30
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 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the messages read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
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 5-13
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 5-32
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-32
MQ		
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 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the messages read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
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 5-13
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 Event Generator" on page 5-38
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 Event Generator" on page 5-38
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 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the messages read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58

Table 5-3 Event Generators (Continued)

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 5-13
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 5-46
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-46
RDBMS		
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 5-53
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	"Suspending and Resuming Event Generators" on page 5-57
	Reset the messages read or error count.	"Resetting Counters" on page 5-57
	Delete one or more event generators.	"Deleting Event Generators" on page 5-58

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
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 5-13
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 5-47
	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 5-55
	Delete one or more channel rules.	"Deleting Channel Rules" on page 5-58
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 5-47
TibcoRV		

Table 5-3 Event Generators (Continued)

Page	Associated Tasks	Help Topics
Create New TibcoRV Event Generator	Create and deploy a TibcoRV event generator.	For more information about TibcoRV Event Generators and other WLI products, see www.e-docs.bea.com/wli/docs10gr3/index.html
View All TibcoRV Event Generators	View a list of TibcoRV event generators. Generator name, number of channels, messages read, last reset time, number of errors, error reset time, and error status are displayed.	
	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. The status of an event generator is preserved when the server is restarted. For example, if the event generator is in the suspended state when the server is restarted, the event generator remains suspended.	
	Reset the messages read or error count.	
	Delete one or more event generators.	

Creating and Deploying Event Generators

The Event Generator module allows you to create and deploy the event generators included as part of Oracle 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.

Creating and Deploying 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.

Figure 5-1 Create a New JMS EG

4. In the **Generator Name** field, enter a unique name for the event generator.

   Note: Names are not case sensitive. Leading or trailing spaces are removed.

5. From the **Destination Type** drop-down list, select **javax.jms.Queue**, **javax.jms.Topic**, or **foreign_jms_destination**.

6. Do one of the following:

   – If you selected **javax.jms.queue** or **javax.jms.topic**, perform the following:

   • Select the JNDI name for the topic or queue from the **Destination JNDI Name** drop-down list.

   • Select the name for the topic or queue from the **JMS Connection Factory 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.

Figure 5-2 Create New JMS (2)

7. In the **Message Selector** field, specify the JMS message selector. For more information, 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. For more information, see "Defining Channel Rules for a JMS Event Generator" on page 5-30.

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.

Creating and Deploying 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, TIBCORV, HTTP**, or **RDBMS**).

3. Select the type of Event Generator from the Console main menu, and click **Create New**.

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

Figure 5-3 Create a New File Event Generator

> **Create a New File Event Generator**
>
> Use this page to create a new File Event Generator. Although new event generators are deployed immediately, they do not have channel rules. You can add rules after you create the new event generator.
>
> **Generator Name**   The name of the event generator must be unique.
>
> **JMS Connection Factory JNDI Name**   weblogic.jws.jms.QueueConnectionFactory
>
> [Submit]   [Reset]   [Cancel]

Note: You must ensure the following before starting the server, after you install MQSeries.

- The MQ Series installation directory should be defined in the server side PATH variable. Ensure that the installation directory is in BEA_HOME\wlserver_10.3

- The MQ Series com.ibm.mq.jar file must be defined in CLASSPATH as follows: **set EXT_PRE_CLASSPATH=C:\Program Files\IBM\WebSphere MQ\Java\lib\com.ibm.mq.jar;%EXT_PRE_CLASSPATH%**

Note: Sometimes, the File Event Generator picks up a file before it is completely uploaded to the polling directory. As a result, the process is invoked with incomplete data. The Event Generator should pick up the file only when it is completely uploaded. To solve this problem, you can edit the setDomainEnv.cmd/sh file to include **com.bea.wli.fileeg.waitTimeMillis** as the system property. This is useful if the file is being uploaded, and the File Event Generator must wait for a defined number of milli seconds before processing the file.

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**, and select JNDI n name from the JMS Connection Factory JNDI Name drop-down list.

Figure 5-4 Create a New HTTP Event Generator

5. Click **Submit** to create and deploy the event generator.

   The **Event Generator Definition** page is displayed.

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

6. Select **Define a New Channel Rule**.

7. Set the properties as required. For a description of the available properties, see the topic applicable to the event generator you are creating:

   – "Defining Channel Rules for a File Event Generator" on page 5-18

   – "Defining Channel Rules for an Email Event Generator" on page 5-27

   – "Defining Channel Rules for a Timer Event Generator" on page 5-32

   – "Defining Channel Rules for an MQ Event Generator" on page 5-38

   – "Defining Channel Rules for an HTTP Event Generator" on page 5-46

   – "Defining Channel Rules for a RDBMS Event Generator" on page 5-47

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

-

-

-

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.

Figure 5-5 Channel Rule Definition - File Event Generator - Disk File Type

Figure 5-6 Channel Rule Definition - File Event Generator - SFTP File Type

The following table summarizes the available settings:

Table 5-4 Elements of File Generator Rule Definition Page

Setting	Description	Required/ Optional
From the **File Type** drop-down list, select **Disk File**, **FTP**, or **SFTP**.	Type of file event. There are different channel rule requirements for Disk File, FTP, and SFTP.	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. For more information, see http://www.iana.org/assignments/character-sets for valid values.	Optional
Enter the **SFTP Host Location**	The name or IP address of the SFTP host or server.	Required
Enter the **SFTP Port Number**	This is the port number on which the SFTP daemon is running. The default port number for SFTP is 22.	Required

Table 5-4 Elements of File Generator Rule Definition Page (Continued)

Setting	Description	Required/ Optional
Select the **SFTP Authentication Method** from the drop-down list	The SFTP authentication method to use for authenticating with the SFTP server. You can configure the following authentication methods: • Password based - You are prompted to enter your SFTP User Name and Password. • Host based - You are prompted to enter your SFTP User Name, Host Private Key Location, Private Key PassPhrase, and SFTP Custom Properties. • Public key based - You are prompted to enter your SFTP User Name, Host Private Key Location, Private Key PassPhrase, and SFTP Custom Properties. • Other - You are prompted to enter your SFTP User Name, Password, and a list of name/value pairs separated by semi-colon (;). The SFTP custom properties are required when you are adding third-party SFTP client implementations.	Required
Enter the **SFTP User Name**	The SFTP username used for authenticating with the SFTP server.	Required
Enter the **SFTP User Password**	The password used for authentication with the SFTP server. You can enter the password in the following ways: • Using the Use Value option. • Configuring a Password Alias using the Use Value option **Note:** When you select SFTP as the File Type in the File Generator Channel Rule Definition page, Password Based becomes the default SFTP authentication method.	Required
Enter the **Host Private Key Location**	The path to the private key file for the host that is trying to connect to the SFTP server. You must configure the SFTP server with this host and its public key.	Required for Host Based Authentication

Table 5-4 Elements of File Generator Rule Definition Page (Continued)

Setting	Description	Required/ Optional
Enter the **User Private Key Location**	The path to the private key file of the user who is trying to connect to the SFTP server. You must configure the SFTP server with this user and its public key.	Required for Public Key Based Authentication
Enter the **Private Key PassPhrase**	The pass-phrase for the host or user's private key file. You can enter the pass-phrase in the following ways: • Using the Use Value option. • Configuring a Password Alias using the Use Value option	Required for Host Based Authentication and Public Key Based Authentication
Enter the **SFTP Custom Properties**	Any additional properties required for host-based and public key based authentication can be specified as a list of name/value pairs separated by semi-colon (;). The custom properties are required when you are adding third-party SFTP client implementations. See Sample Host File for Host Based Authentication for details.	Required for Host Based Authentication and Public Key Based Authentication
Enter the **SFTP Local Directory**	The local directory where remote files are copied before being processed.	Required
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**

Table 5-4 Elements of File Generator Rule Definition Page (Continued)

Setting	Description	Required/ Optional
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. For more information, see "Password Aliases and the Password Store" on page 7-6. 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**
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

Table 5-4 Elements of File Generator Rule Definition Page (Continued)

Setting	Description	Required/ Optional
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 XML channel type. 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
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**

Table 5-4 Elements of File Generator Rule Definition Page (Continued)

Setting	Description	Required/ Optional
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

Note: The File Event Generator polls a specified directory for a specified file pattern, finds a file, generates a event, and publishes it to the specified channel. In case of any error, the file is moved into an error directory. These details can be specified while creating a File Event Generator from the WLI Administration Console.

When the server is shut down, the File Event Generator encounters an exception during message publishing, as the corresponding JPD is already undeployed. The file is moved to the error folder. When the server is restarted, there is no recovery of the message, as the message was not successfully published to the channel, or the file had been moved to error directory, as the error was encountered during shutdown. In case of a force shutdown or crash, check the error directory for unprocessed/in-flight messages. You must manually redeliver and publish these messages after the server re-starts.

Sample Host File for Host Based Authentication

A sample host file for host-based authentication is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>

<HostAuthorizations>

<!-- Host Authorizations file, used by the abstract class
HostKeyVerification to verify the servers host key -->
```

```
    <!-- Allow the following hosts access if they provide the correct public
key -->

    <AllowHost HostName="testSFTPserver" Algorithm="ssh-dss"
Fingerprint="12H HRYYR %668 JJFJF"/>

    <AllowHost HostName="testSFTPserver1" Algorithm="ssh-dss"
Fingerprint="178H HRYHFHF %668 JJFJF"/>

    <!-- Deny the following hosts access -->

    <DenyHost HostName="testFTPServer111"/>

    <DenyHost HostName="testFTPServer134"/>

</HostAuthorizations>
```

The sample host file, `sftp_known_hosts.xml` is created in the
`\BEA_Home\wli_10.3\user_projects\domains\<Created Domain >\wli-config`
directory and named as `sftp_known_hosts.xml`.

Note: The properties for Allow Host is set in the `wli-config` file, then all the files from the
SFTP server are accepted. To deny access to a host, specify the host name using the Deny
Host option.

Related Topics

- "Creating and Deploying Event Generators" on page 5-13
- "Viewing and Updating Event Generator Channel Rules" on page 5-55

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.

Figure 5-7 Channel Rule Definition - Email Event Generator

The following table summarizes the available settings:

Table 5-5 Elements of Event Generator Channel Rule Definition

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. For more information, see "Password Aliases and the Password Store" on page 7-6. After the alias has been added to the password store, it is available for selection from the **Use Alias** drop-down list.	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

Table 5-5 Elements of Event Generator Channel Rule Definition

Setting	Description	Required/ Optional
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
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

-

- "Viewing and Updating Event Generator Channel Rules" on page 5-55

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.

Figure 5-8 JMS Event Generator - Channel Rule Definition

The following table summarizes the available settings:

Table 5-6 Elements of JMS Event Generator Channel Rule Definition Page

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.	Optional
	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.	

Table 5-6 Elements of JMS Event Generator Channel Rule Definition Page (Continued)

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 5-13

- "Viewing and Updating Event Generator Channel Rules" on page 5-55

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.

Figure 5-9 Timer Generator - Channel Rule Definition

The following table summarizes the available settings:

Table 5-7 Elements of Timer Generator Channel Rule Definition

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. If you want to create an event that fires at the same time, every day, for the calendar year, you must take into account the fact that a time change occurs when the time changes from standard time to daylight savings time. To account for this you must define two timer events, one that operates during standard time (e.g. from April 6 2004, 2:30PM to October 31 2004 2:30PM) and another that operates during daylight savings time (e.g. from November 1 2004 2:30PM to April 2 2005 2:30PM) with the interval set to 1 day. You also need to define more timers for future years as needed.	Required
From the **Daylight Saving (DST) Handling**, select Timer handles DST or Timer ignores DST.	If Daylight Saving is configured, the timer has an option to handle or ignore it.	Optional

Table 5-7 Elements of Timer Generator Channel Rule Definition

Setting	Description	Required/Optional
In Frequency, do one of the following: • Select the **Runs Once** option button. • Select the **Runs Every** option button, and specify the interval in days, hours, minutes, and seconds. • 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.	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. **Never Expires** and **Expires On** option, specifies the date and time the configured schedule expires. If the **Never Expires** option is selected, the configured schedule remains in effect until the option is changed.	Required
In the **Message** field, enter the 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. For example, if the message content is of string type, then select a String type channel. If it is an XML message, then select an XML type channel.	Optional

Table 5-7 Elements of Timer Generator Channel Rule Definition

Setting	Description	Required/ 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. For more information, see "About Business Calendars and Business Time Calculations" in the *Using WorkList Console*. 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 5-57.	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 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
Is Recoverable/Skippable	Select the **Recoverable** option to recover the timer events that are missed because of a server shutdown. If you do not want to recover those events, select the **Skippable** option, when you define the channel rules for a Timer event generator.	Optional
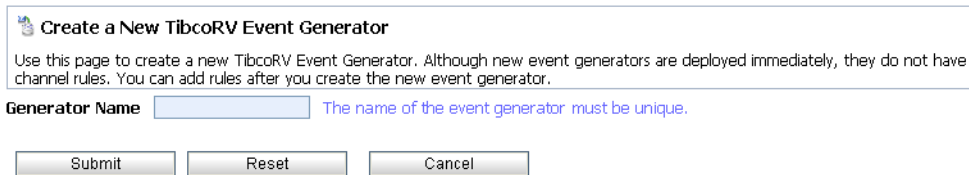
Related Topics

- "Creating and Deploying Event Generators" on page 5-13

- "Viewing and Updating Event Generator Channel Rules" on page 5-55

Overview of TibcoRV Event Generator

TIBCO Rendezvous (TIBCORV) Event Generator is one of the Oracle WebLogic Integration event generators that you can create from the Oracle WebLogic Integration Administration Console. The TIBCORV event generator listens for messages on a subject and raises events to the message broker on receiving the desired message. Figure 5-10 shows the Create New TibcoRV Event Generator page.

Figure 5-10 Create New TIBCORV Event Generator

Defining Channel Rules for TIBCORV Event Generator

Once you have created a new TIBCORV event generator, you can add the channel rule definition as shown in Figure 5-11.

Figure 5-11 TIBCORV Generator Channel Rule Definition

For more information about the TIBCORV event generator and creating the channel rule definition, see TIBCO Rendezvous Event Generator in the *TIBCO Rendezvous Control and Event Generator User Guide.*

Defining Channel Rules for an MQ Event Generator

The **MQSeries Generator Channel Rule Definition** page allows you to define the properties for the channel rule.

Figure 5-12 MQSeries Generator - Channel Rule Definition

Figure 5-13 MQSeries Generator - Channel Rule Definition - Continued

Messages Per Poll	-1	Number of Messages to be picked per poll of MQSeries Event Generator thread (-1 for picking all available messages)
MQSeries User Name		MQSeries User Name. Required only if MQSeries Authorization is to be enabled
MQSeries User Password		MQSeries User Password. Required only if MQSeries Authorization is to be enabled
SSL Required	☐	Sets the SSL option while getting the message data from the queue
Two Way SSL	☐	Enables Two Way SSL Authentication with MQSeries
MQ Cipher Suite		Enter the SSL Cipher Suite when Setting the SSL option; Required for SSL Connection
SSL Trust Store		Enter the SSL Trust Store when Setting the SSL option; Optional for SSL Connection
SSL Trust Store Type		Enter the SSL Trust Store Type when Setting the SSL option; Optional for SSL Connection
SSL Trust Store Password		Set the SSL Trust Store Password; Required when SSL Trust Store Location Set; Optional Otherwise
SSL Key Store Location		Provide SSL Key Store Location when enabling Two Way SSL
SSL Key Store Type		Provide SSL Key Store Type when enabling Two Way SSL Option
SSL Key Store Password		Provide SSL Key Store Password when enabling Two Way SSL
SSL Key Password		Provide SSL Key Password when enabling Two Way SSL
Publish As		Select a user to impersonate.

[Submit] [Reset] [Cancel]

The following table summarizes the available settings:

Table 5-8 Elements of MQSeries Generator Channel Rule Definition page

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
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**

Table 5-8 Elements of MQSeries Generator Channel Rule Definition page

Setting	Description	Required/ Optional
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
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, and the Event Generator will keep trying to send the same message, which eventually leads to an infinite loop.	Optional

Table 5-8 Elements of MQSeries Generator Channel Rule Definition page

Setting	Description	Required/ 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 5-44, this class is an extension of the com.bea.wli.mbconnector.mqseries.Abst ractContentFilter class.	Optional
Check or uncheck 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 **Number of Polling Threads** field, enter the number of polling threads.	Number of event generator polling threads.	Required
In the **Messages 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 or de-select the **SSL Required** check box.	Select the SSL Required check box to enable the SSL option, and get the message data from the queue	Optional

Table 5-8 Elements of MQSeries Generator Channel Rule Definition page

Setting	Description	Required/Optional
Select or de-select the **Two Way SSL** check box.	Selecting the **Two Way SSL** check box enables two-way SSL authentication with MQSeries.	Optional
Enter the required information in the **MQ Cipher Suite** field.	Enter the SSL Cipher Suite if you are setting the SSL option for SSL Connection.	Required for SSL Connection
Enter the Trust Store for the **SSL Trust Store** field.	Enter the SSL Trust Store when you are setting the SSL option.	Optional
Enter the SSL Trust Store Type for the **SSL Trust Store** field.	Enter the SSL Trust Store Type when you are setting the SSL option; Optional for SSL connection.	Optional
Enter the password for the **SSL Trust Store Password** field.	Set the SSL Trust Store Password.	Required when the SSL Trust Store Location is Set
Enter the location for the **SSL Key Store Location** field.	Provides the SSL Key Store Location and enables two-way SSL.	Optional
Enter the location for the **SSL Key Store Type** field.	Provides the SSL Key Store Type and enables two-way SSL.	Optional
Enter the password for the **SSL Key Store Password** field.	Provides the SSL Key Store Password and enables two-way SSL.	Optional
Enter the password for the **SSL Key Password** field.	Provides the SSL Key Password and enables two-way SSL.	
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 5-1 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.

1. Extract the mqegEjbUtil.jar from the *WLI_HOME*\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 5-1 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 Oracle 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.ContentFilter.

Related Topics

- "Creating and Deploying Event Generators" on page 5-13
- "Viewing and Updating Event Generator Channel Rules" on page 5-55

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.

Figure 5-14 HTTP Generator - Channel Rule Definition

The following table summarizes the available settings:

Table 5-9 Elements of HTTP Event Generator page

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 5-13

- "Viewing and Updating Event Generator Channel Rules" on page 5-55

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.

Figure 5-15 RDBMS Event Generator - Channel Rule Definition

Table 5-10 summarizes the available settings:

Table 5-10 Elements of RDBMS Event Generator Channel Rule Definition page

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.	Required
	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.	
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 Oracle WebLogic Server where the event generator is running.	Required
	For more information on configuring data sources, see the RDBMS Event Generator User Guide.	

Table 5-10 Elements of RDBMS Event Generator Channel Rule Definition page

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
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. If you set this property, messages are delivered to a secured Message Broker channel. If **Publish As** is not specified, messages are published as Anonymous.	Optional
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
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)

Table 5-10 Elements of RDBMS Event Generator Channel Rule Definition page

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. Check the radio button next to the table name you require and click **Submit** to select the table.	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 checking 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

Table 5-10 Elements of RDBMS Event Generator Channel Rule Definition page

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		

Table 5-10 Elements of RDBMS Event Generator Channel Rule Definition page

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.	Required
	For example, SELECT FIRST_NAME, LAST_NAME, EMPLOYEE_ID FROM RDBMS_USER.EMP_TBL WHERE STATUS = 'Intern'.	
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.	Optional
	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.	

Related Topics

- "Creating and Deploying Event Generators" on page 5-13

● "Viewing and Updating Event Generator Channel Rules" on page 5-55

Listing and Locating Event Generators

Listing Event Generators

The **View All File Event Generators** page displays the following information for each configured event generator:

Figure 5-16 View All File Event Generators Page

Table 5-11 Elements of View All File Event Generators page

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).

Table 5-11 Elements of View All File Event Generators page

Property	Description
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.

Note: The elements for Email, JMS, Timer, MQ Series, RDBMS, and HTTP event generators are the same as the File event generator and listed in the same sequence as on the **View all File Event Generators** page.

Locating Event Generators

To locate an event generator, do the following:

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.

Related Topics

- "Viewing and Updating Event Generator Channel Rules" on page 5-55

- "Suspending and Resuming Event Generators" on page 5-57

- "Deleting Event Generators" on page 5-58

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.

1. Locate the event generator. For more information, see "Listing and Locating Event Generators" on page 5-53.

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.

Figure 5-17 JMS Event Generator Details

4. Select a new channel from the **Default Rule Channel** drop-down list.

5. Click **Submit** to update.

6. Locate the event generator. For more information, see "Listing and Locating Event Generators" on page 5-53.

7. Click the event generator name to display the **Event Generator Definition** page.

8. 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.

9. Set the properties as required. For a description of the available properties, see the topic applicable to the event generator you are creating:

   "Defining Channel Rules for a File Event Generator" on page 5-18.

   "Defining Channel Rules for an Email Event Generator" on page 5-27.

   "Defining Channel Rules for a JMS Event Generator" on page 5-30.

   "Defining Channel Rules for a Timer Event Generator" on page 5-32.

   "Defining Channel Rules for an MQ Event Generator" on page 5-38.

   "Defining Channel Rules for an HTTP Event Generator" on page 5-46.

10. Click **Submit** to add or update the channel rule.

11. Click the check box to the left of the channel rules to be deleted.

12. Click **Delete**.

    A confirmation dialog box is displayed.

13. Click **OK** to confirm.

    The selected channel rules are deleted.

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 undeploys the Event Generator. On resuming the generator it is deployed.

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.

1. Locate the event generators to be suspended. For more information, see "Listing and Locating Event Generators" on page 5-53.

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".

4. Locate the event generators to be resumed. For more information, see "Listing and Locating Event Generators" on page 5-53.

5. Click the check box to the left of the event generators you want to select.

6. Click **Resume**.

   The selected generators are resumed.

Resetting Counters

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

1. Locate the event generators to be reset. For more information, see "Listing and Locating Event Generators" on page 5-53.

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**.

4. Locate the event generators to be reset. For more information, see "Listing and Locating Event Generators" on page 5-53.

5. Click the check box to the left of the event generators you want to select.

6. Click **Reset Error Count**.

Deleting Channel Rules

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

1. Locate the event generator. For more information, see "Listing and Locating Event Generators" on page 5-53.

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.

1. Locate the event generators to be deleted. For more information, see "Listing and Locating Event Generators" on page 5-53.

2. Click the check box to the left of the event generators you want to delete.

3. Click **Delete**.

   The selected generators are deleted.

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.

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. For more information, see About WebLogic Integration Users, Groups, Roles, and Security Policies in User Management in the *Worklist Console Online Help*.

The following topics are provided:

- About Trading Partner Management

- Overview of the Trading Partner Management Module

- Configuring Trading Partner Management

- Configuring 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

- Enabling and Disabling Trading Partner and Service Profiles

- Importing and Exporting Data

- Deleting Trading Partner Profiles
- Deleting Certificates, Bindings, or Custom Extensions
- Deleting Services
- Viewing Statistics
- Monitoring Messages

About Trading Partner Management

The basic building blocks of trading partner integration are trading partner profiles, services, and service profiles. In Oracle 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 Oracle WebLogic Integration Administration Console allows administrators to configure and manage the required profiles, certificates, and protocol bindings, and to monitor trading partner activity.

To start the Trading Partner Management, click the **Trading Partner Management module** link in the left panel of the Oracle WebLogic Integration Administration Console home page. The Trading Partner Management page appears.

Figure 6-1 Oracle WebLogic Integration Administration Console - Trading Partner Management - Home Page

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 in *Introducing Trading Partner Integration*.

- 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 *Using Integration Controls*.

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.

Table 6-1 Elements of Trading Partner Management Module

Page	Associated Tasks	Help Topics
Partner Profiles		
View and Edit Trading Partner Profiles	View a list of 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
	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
	Enable or disable the trading partner profile.	Enabling and Disabling Trading Partner and Service Profiles
Create New	Add a Trading Partner Profile.	Configuring Partner Profiles
Certificates		
Choose trading partner	Choose a trading partner, and then click Go. The View and Edit Trading Partner Certificates page appears.	Viewing and Changing Certificates
Create New	Choose a trading partner, and then click Go. The Add Certificates page appears.	Adding Certificates to a Trading Partner
Bindings		
Choose trading partner	Choose a trading partner, and then click Go. The Edit Binding page appears.	
Create New	Choose a trading partner, and then click Go. The Add Binding page appears.	Adding Protocol Bindings to a Trading Partner

Table 6-1 Elements of Trading Partner Management Module

Page	Associated Tasks	Help Topics
Custom Extension		
Choose trading partner	Choose a trading partner, and then click Go. The View and Edit Custom Extension page appears.	Viewing and Changing Certificates
Create New	Choose a trading partner, and then click Go. The Add Custom Extension page appears.	Adding a Custom Extension to a Trading Partner
Services		
View All	View a list of Service name, business service name, description, type, business protocol, and description.	Viewing and Changing Services
	Filter the list by service name. Use ? to match any single character or * to match zero or more characters.	
	Delete a service.	Deleting Services
Create New	Add a service definition for a newly deployed service. Assign the name, type, and business protocol. Optionally, assign a description.	Adding Services
Message Tracking		
View All	View the list of messages. Event ID, time of event, direction (inbound or outbound), and status are displayed.	Monitoring 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
Import/Export		
Import	Import Trading Partner Management Data—Select a trading partner management file for import, and set the import properties.	Importing Management Data
Export	Export Trading Partner Management Data—Select trading partners and services for export, and set the export properties.	Exporting Management Data

Table 6-1 Elements of Trading Partner Management Module

Page	Associated Tasks	Help Topics
Bulk Delete	Delete Trading Partner Management Data—Select trading partner profiles and services to delete and set the delete properties.	Deleting Trading Partner Profiles and Services Using Bulk Delete
Statistics		
View 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
Configuration		
General	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
Proxy Host	Proxy Configuration—Configure a proxy host.	Configuring a Proxy Host
Secure Audit Log	Audit Log Configuration—Enable or disable secure audit logging. If enabled, specify the secure audit logging class.	Configuring Secure Audit Logging
Secure Timestamp	Secure Timestamp Configuration—Specify the Java class used for secure time-stamping.	Configuring Secure Audit Logging
Refresh Keystore	Refresh Keystore—Refresh the KeyStores (identity and trust) in memory from the disk.	Refreshing the Keystore
Certificate Verification Provider	Certificate Verification Provider—Specify the certificate verification provider.	Specifying the Certificate Verification Provider

Configuring Trading Partner Management

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

- Configuring the Mode and Message Tracking

- Configuring a Proxy Host

- Configuring Secure Audit Logging

- Refreshing the Keystore

- Specifying the Certificate Verification Provider

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.

1. From the **Trading Partner Management** page, select **Configuration > General**.

   The **General Configuration** page appears.

Figure 6-2 General Configuration Page

2. Set the message tracking properties, as required. See Figure 6-2 for settings.

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

Table 6-1 summarizes settings available on the **General Configuration** page.

Table 6-2 Elements of 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** (For more information, see Adding Service Profiles to a Service), 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
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.	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.

1. From the **Trading Partner Management** page, select **Configuration > Proxy Host**.

   The **Proxy Configuration** page appears.

Figure 6-3 Proxy Configuration Page

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

2. In the **Proxy Host** field, enter the host name or IP address.

3. In the **Port number of proxy server**, enter the port.

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

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.

1. From the **Trading Partner Management** page, select **Configuration > Secure Audit Log**.

   The **Audit Log Configuration** page appears.

Figure 6-4 Audit Log Configuration Page

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.

2. To configure the Secure Audit Logging, do one of the following:

   – Select the **Disable** option button to disable secure audit logging.

   – Select the **Enable** option button, and 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.

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

Configuring Secure Time-stamp

If your secure audit logging is enabled, the **Secure Timestamp Configuration** page allows you to specify the Java class that implements the secure time-stamp class.

1. From the **Trading Partner Management** page, select **Configuration > Secure Timestamp**.

   The **Secure Timestamp Configuration** page appears.

Figure 6-5 Secure Timestamp Configuration

2. In the **Secure Timestamp Class** field, enter the class.

> **Note:** If no class is entered, secure time-stamping is disabled.

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

Refreshing the Keystore

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

1. From the **Trading Partner Management** page, select **Configuration > Refresh Keystore**.

   The **Refresh Keystore** page appears.

Figure 6-6 Refresh KeyStore Page

2. Click the **Refresh Keystore** button to refresh the keystore.

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 to insert a Java class. The Java class implements an interface that calls out to a third-party service to verify trading partner certificates. Such an implementation, referred to as 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.

1. From the **Trading Partner Management** page, select **Configuration > Certificate Verification Provider**.

   The **Certificate Verification Provider** page appears.

Figure 6-7 Certification Verification Provider Page

2. In the **Certificate Verification Provider** field, enter the CVP Java class.

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

Configuring Partner Profiles

The Partner Profiles module allows you to view and edit trading partner profiles, or add trading partner profile. See the appropriate topic for instructions:

- Adding Trading Partner Profiles
- Editing Trading Partner Profiles
- Viewing and Changing Trading Partner Profiles
- Listing and Locating Services

Adding Trading Partner Profiles

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

1. From the **Trading Partner Management** page, select **Partner Profiles > Create New**.

   The **Add Trading Partner Profile** page appears.

Figure 6-8 Add Trading Partner Profile

2. Set the trading partner profile properties, as required. For more information, see Editing Trading Partner Profiles for a description of the available settings.

3. Click **Add profile**.

   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 displayed. A message indicating the problem is displayed above the input requiring correction.

4. Do one or more of the following:

   – To add certificates to the trading partner, see Adding Certificates to a Trading Partner.

   – To add bindings to the trading partner, see Adding Protocol Bindings to a Trading Partner.

   – To add a custom extension to the trading partner, see Adding a Custom Extension to a Trading Partner.

Editing Trading Partner Profiles

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

Table 6-3 Elements of Trading Partner Profile page

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
Select or un-select the **Default Trading Partner** check box.	When selected, the trading partner is designated as 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 as the default. The default is un-selected.	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

Table 6-3 Elements of Trading Partner Profile page (Continued)

Setting	Description	Required/ 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	Optional
	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.	
	The default is **ENABLED**.	
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
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. For more information, see Listing and Locating Users in *Using Worklist Console*. The value applies only if **Type** is set to **Remote**.	Optional

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.

Table 6-4 Elements of View and Edit Trading Partner Profile

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
Description	An optional description. This value is for administrative purposes only. It is not included in messages.	Yes
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
Default Trading Partner	Indicator of whether or not the trading partner is designated as 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
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

Table 6-4 Elements of View and Edit Trading Partner Profile (Continued)

Property	Description		Administrator Can Set (Yes/No)
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.	

Table 6-4 Elements of View and Edit Trading Partner Profile (Continued)

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.	

1. Locate the trading partner. For more information, see Listing and Locating Trading Partners.

2. Click the trading partner name.

   The **View and Edit Trading Partner Profile** page is displayed.

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

2. Update properties as required. For more information, see Editing Trading Partner Profiles.

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.

   – To add bindings to the trading partner, see Adding Protocol Bindings to a Trading Partner.

   – To add a custom extension to the trading partner, see Adding a Custom Extension to a Trading Partner.

   – To update a certificate, see Viewing and Changing Certificates.

   – To update a binding, see Enabling and Disabling Trading Partner and Service Profiles.

   – To update a custom extension, see Viewing and Changing a Custom Extension.

Listing and Locating Trading Partners

The View and Edit Trading Partner Profile page displays the following information for each trading partner.

Table 6-5 Elements of View and Edit Trading Partner Profile page

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).
Business ID	Identifier for the trading partner. The value is used to identify the partner in message exchanges.

Table 6-5 Elements of View and Edit Trading Partner Profile page (Continued)

Property	Description
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).

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

● Adding Certificates to a Trading Partner

● Adding Protocol Bindings to a Trading Partner

● Adding a Custom Extension to a Trading Partner

● Adding Service Profiles to a Service

- Importing Management Data

Adding Certificates to a Trading Partner

The Certificates module allows you to view and edit trading partner certificates, or add certificates. See the appropriate topic for instructions.

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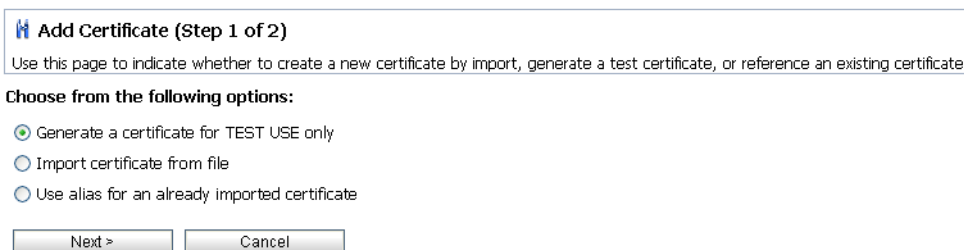
The **Add Certificate** page allows you to add certificates to a trading partner profile.

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.

1. Do one of the following:

    – Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

    – From the **Trading Partner Management** page, select **Certificates > Create New** from the left panel. On the **Choose Trading Partner** page, select the trading partner name from the **Name** drop-down list, then click **Go**.

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

Figure 6-9 Add Certificate Page

2. 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.

3. 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

    – Creating and Importing the Files for a Certificate

    – Creating a Reference to an Existing Certificate

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.

Figure 6-10 Add Certification - Step 2

This page allows you to create a client, signature, or encryption certificate definition. The certificate generated is appropriate for use only in 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. For more information, see "Password Aliases and the Password Store" on page 7-6.

   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. Select 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.

Figure 6-11 Add Certificate - Step 2

This page allows you to create a client, signature, or encryption certificate definition, and to 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. For more information, see Password Aliases and the Password Store.

   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.

Figure 6-12 Add Certification (2)

This page allows you to create a reference to an existing client, signature, encryption, or server 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. For more information, see Password Aliases and the Password Store.

   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.

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.

Figure 6-13 View and Edit Trading Partner Certificate Page

1. Do one of the following:

    – Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

    – From the **Trading Partner Management** page, select **Certificates > Choose Trading Partner** from the left panel. On the **Choose Trading Partner** page, select the trading partner name from the **Name** drop-down list, then click **Go**.

    The **View and Edit Trading Partner Certificates** page is displayed.

2. On the **View and Edit Trading Partner Certificate** page, select an existing certificate under the **Name** list.

3. Click **Edit Certificate**.

Figure 6-14 The **Edit Certificate** page is displayed. **Edit Certificate Page**

4. If required, update the password alias. From the **Password Alias** drop-down list, select a new password alias.

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

5. 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.

6. 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.

7. Click **Submit**.

8. 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 displayed. A message indicating the problem is displayed above the input requiring correction.

Adding Protocol Bindings to a Trading Partner

The Bindings module allows you to add bindings, define protocol bindings, or view and change bindings. See the appropriate topic for instructions.

Add Binding

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

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

   – From the **Trading Partner Management** page, select **Bindings > Create New** from the left panel. On the **Choose Trading Partner** page, select the trading partner name from the **Name** drop-down list, then click **Go**.

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

Figure 6-15 Add Binding (Step 1 of 2)

2. Select the **ebXML 1.0**, **ebXML 2.0**, **RosettaNet 1.1**, **RosettaNet 2.0**, or **Web Service** option button.

3. Click **Create Binding** to display the **Add Binding (Step 2 of 2)** page.

4. Set the binding properties as required. For more information, see Defining Protocol Bindings for a description of the available settings.

5. Click **Add Binding**.

The **Edit Binding** page is displayed. The binding is included in the binding summary table.

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

6. 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.

– 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.

Defining Protocol Bindings

The **Add Binding (Step 2 of 2)** pages allow you to define the properties for a protocol binding.

Figure 6-16 Defining Protocol Bindings

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 With 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.

Table 6-6 Settings Available For an ebXML 1.0 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-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 as 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

Table 6-6 Settings Available For an ebXML 1.0 or 2.0 Binding (Continued)

Setting	Description	Required/ 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, for more information, see Defining Endpoints for Projects Containing Multiple JPDs With the Same Name.	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**.	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

Table 6-6 Settings Available For an ebXML 1.0 or 2.0 Binding (Continued)

Setting	Description	Required/ Optional
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,
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.

Table 6-6 Settings Available For an ebXML 1.0 or 2.0 Binding (Continued)

Setting	Description	Required/ Optional
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 **ONCEANDON LYONCE** or **ATMOSTONC E** 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.	
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 6-22.	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. For more information, see Configuring Secure Audit Logging.	Optional

Table 6-6 Settings Available For an ebXML 1.0 or 2.0 Binding (Continued)

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.	Optional
	Archiving of signed messages in a secure audit log is controlled by the secure audit logging configuration. For more information, see Configuring Secure Audit Logging.	

Note: Within Oracle 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 Oracle 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. For more information, see Configuring Signature Transforms for ebXML Bindings.

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.

Table 6-7 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 as 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 With the Same Name.	Required

Table 6-7 Settings Available For a RosettaNet 1.1 or 2.0 binding (Continued)

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.

Table 6-7 Settings Available For a RosettaNet 1.1 or 2.0 binding (Continued)

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.	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

Table 6-7 Settings Available For a RosettaNet 1.1 or 2.0 binding (Continued)

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_P AYLOAD**
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 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. For more information, see Configuring Secure Audit Logging.	Required

Table 6-7 Settings Available For a RosettaNet 1.1 or 2.0 binding (Continued)

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. For more information, see Configuring Secure Audit Logging.	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 Oracle 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 Oracle 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. For more information, see Configuring PIP Notification of Failure Roles for RosettaNet Bindings.

Defining a Web Service Binding

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

Table 6-8 Elements of 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 With the Same Name.	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 With the Same Name

When you have multiple JPD files with the same name within the same Java package, that are in the same project, you must 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-cl
ass>
</filter>

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

After editing the `web.xml` file, define the endpoint URL of your trading partner.

Related Topics

- Enabling and Disabling Trading Partner and Service Profiles

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.

Figure 6-17 View Binding Details Page - RosettaNet

Figure 6-18 View Binding Details Page - ebXML

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

Table 6-9 Elements of 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
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 as 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

Table 6-9 Elements of View Binding Details Page (Continued)

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
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
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

Table 6-9 Elements of View Binding Details Page (Continued)

Property	Description	Property Applies To	Administrator Can Set (Yes/No)
Signature Receipt Required	Indicator of whether or not the message is acknowledged by a digitally signed receipt acknowledgement message using the signature certificate of the trading partner sending the acknowledgement (true or false).	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Signature Certificate	The name of the signature certificate used to digitally sign messages.	ebXML 1.0/2.0 RosettaNet 1.1/2.0	Yes
Non Repudiation Protocol	The predefined non-repudiation protocol (PKCS7).	RosettaNet 1.1/2.0	No
Hash Function	The 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
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). For more information, see Defining a RosettaNet 1.1 or 2.0 Binding 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

Table 6-9 Elements of View Binding Details Page (Continued)

Property	Description		Property Applies To	Administrator Can Set (Yes/No)
Authentication				
Authentication table	Entry for each authentication configured for the binding. For more information, see Adding Authentication to a Service Profile.		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.		
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.		

1. Do one of the following:

- Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

- From the **Trading Partner Management** home page, select **Bindings > Choose Trading Partner** from the left panel. In 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.

1. On the **View Binding Detail**s page, click **Edit Binding**.

   The **Edit Binding** page is displayed.

2. Update properties, as required. For more information, see Defining Protocol Bindings.

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 displayed. 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.

   - To Configure PIP failure notification to a RosettaNet binding, see Configuring PIP Notification of Failure Roles for RosettaNet Bindings.

Updating or Deleting Authentication

The authentication required for an exchange is configured as part of the service profile definition, but it 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 6-10 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. The following procedures describe how to update or delete an authentication from 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, 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, 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.

- 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 deleting authentication from the binding of a participant in a service profile, you can reconfigure it, as described in Adding Authentication to a Service Profile. In this case, options are only offered for configuring authentication for the participant whose authentication was deleted.

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 in the Authentication section of the View Binding Details page.

2. Click **Edit Authentication**.

3. Depending on the type of authentication, you can do one or more of the following. For more information, see Table 6-10 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 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 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 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*.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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 **Digital Signature Configuration for Non-Repudiation** section, click **Configure Signature Transforms**.

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

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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 displayed. A message indicating the problem is displayed above the input requiring correction.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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**.

5. The **Edit PIP Failure** page is displayed.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
- Enabling and Disabling Trading Partner and Service Profiles

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.

```
...
<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>
...
```

This section includes:

- Add Custom Extension

- Viewing and Changing a Custom Extension

Add Custom Extension

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.

1. Do one of the following:

    – Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

    – From the **Trading Partner Management** page, select **Custom Extension > Create New** from the left panel. On the **Choose Trading Partner** page, select the trading partner name from the Name drop-down list, then click **Go**.

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

Figure 6-19 Add Custom Extension Page

2. In the **Name** field, enter a name for the custom extension.

3. In the **Description** field, enter an optional description.

4. 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 Adding a Custom Extension to a Trading Partner constitutes a valid entry.

5. Click **Create Custom Extension**.

    The **Add Custom Extension** 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.

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.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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.

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 Adding a Custom Extension to a Trading Partner 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

- Enabling and Disabling Trading Partner and Service Profiles

- Configuring Partner Profiles

● Importing Management Data

Adding Services

The Services module allows you to add services, or adding service profiles to services. See the appropriate topic for instructions.

Add Service

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

1. From the **Trading Partner Management** page, select the **Services > Create New**.

   The **Add Service** page appears.

Figure 6-20 Add Service Page

2. Do one of the following in the **Add Service** page:

   – 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.

3. From the **Type** drop-down list, select **Service Control, Process**, or **Web Service** to specify the type of service.

4. From the **Business Protocol** drop-down list, select **EBXML, ROSETTANET**, or **WEBSERVICE** to specify the service protocol.

5. In the **Description** field, enter an optional description of the service.

6. 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.

7. To add service profiles to the service, see Adding Service Profiles to a Service.

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

Adding Service Profiles to a RosettaNet Service

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

To add RosettaNet Service Defaults:

1. Locate the service as described in Listing and Locating Services.

2. Click the service name to select it.

   The **View and Edit Service Details** page appears.

3. Click **Add Service Profiles**.

4. Define the defaults as required. The following table describes the available settings.

Table 6-11 Elements of View and Edit Service Details page

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.

Table 6-11 Elements of View and Edit Service Details page

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

Adding Service Profiles to a Service

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

1. Locate the service as described in Listing and Locating Services.

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.

Figure 6-21 Add Service Profiles to a Service

4. The Collaborative Partner Agreement (CPA) Id for an ebXML control is listed in the **Service Profile Id** field. You can set the CPA Id manually in the ebXML control annotation using the Property Editor in the IDE. This value will override the existing Service Profile Id.

5. From the **Status** drop-down list, select **Enabled** or **Disabled**.

6. 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. For more information, see Configuring the Mode and Message Tracking.

   – **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.

7. 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.

8. 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.

9. Click **Submit**.

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

10. 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.

– Click **No**. You can configure authentication later as described in Adding Authentication to a Service Profile.

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.

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

Table 6-12 Authentication Properties

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.

Table 6-12 Authentication Properties

Transport Protocol	Authentication Mode	Local Trading Partner (LocalTP) Configuration	Remote Trading Partner (RemoteTP) Configuration
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 Trading Partner:** LocalTP
		Client Certificate: RemoteTP client certificate to be used for SSL mutual authentication.	**Client Certificate:** LocalTP client certificate to be used for SSL mutual authentication.
			Server Certificate: RemoteTP server certificate to be used for SSL authentication.

1. Locate the service as described in Listing and Locating Services.

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.

Table 6-13 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 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 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:.

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.

1. Locate the service as described in Listing and Locating Services.

2. Click the service name to select it.

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

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

    The **View Service Profile** page is displayed.

4. Click **Configure Authentication**.

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

Choose type of Authentication Mode	
LOCAL	**REMOTE**
⊙ Basic	⊙ Basic

5. Click the **Next** button.

6. Enter the **Username** required to access the remote endpoint.

7. Select the **Password Alias** from the drop-down list.

    Note: If the password alias has not been added, click the **Add Alias** link to the left of the drop-down list. See Adding Passwords to the Password Store 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:.

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    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  ----->
```

Listing and Locating Services

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

Table 6-14 Elements of View and Edit Services page

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).

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

2. To locate a specific service do one of the following:

    – Filter by service name. Enter the search target (use ? to match any single character or * to match zero or more characters.), then click **Search**. The services matching the search criteria are displayed.

    – Resort the list. Ascending ⌃ and descending ⌄ arrow buttons indicate sortable columns. Click the button to change the sort order.

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

Viewing and Changing 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.

Table 6-15 Elements of 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:ebxml 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

Table 6-15 Elements of View and Edit Service Details page

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.	
	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.	
	Statistics	A link to the **Trading Partner Management Statistics** page for the service profile.	

1. Locate the service as described in Listing and Locating Services.

2. Click the service name to select it.

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

3. On the **View and Edit Service Details** page, click **Edit Service**.

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

Figure 6-22 Edit Service Details Page

4. From the **Type** drop-down list, select **Service Control, Process**, or **Web Service** to specify the type of service.

5. From the **Business Protocol** drop-down list, select **EBXML, ROSETTANET**, or **WEBSERVICE** to specify the service protocol.

6. In the **Description** field, enter an optional description of the service.

7. Click **Submit.**

8. 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.

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

10. Click **Edit Service Defaults** to update the settings. See Adding Service Profiles to a RosettaNet Service for a description of the available settings.

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

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

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

   You are prompted to confirm.

14. 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 Service Profiles to a RosettaNet Service

- Viewing and Changing Service Profiles

- Enabling and Disabling Trading Partner and Service Profiles

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.

Figure 6-23 View Service Profile Page

1. Locate the service as described in Listing and Locating Services.

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. On the **View Service Profile** page, click **Edit Service**.

   The **Edit Service Profil**e page is displayed.

5. To change the status, select **Enabled** or **Disabled** from the **Status** drop-down list,

6. 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. For more information, see Configuring the Mode and Message Tracking.

   – **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.

7. 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.

8. 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.

9. Click **Submit**.

10. 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.

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

- Enabling and Disabling Trading Partner and Service Profiles

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.

1. Locate the trading partner(s) to be disabled. For more information, see Listing and Locating Trading Partners.

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. The service profiles are related to the disabled trading partners.

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.

5. Locate the trading partner(s) to be enabled. For more information, see Listing and Locating Trading Partners.

6. Click the check box to the left of each trading partner to select.

7. Click **Enable**.

   Note: The **Enable Trading Partner Service Profiles** page lists the service profiles that can be enabled. The service profiles are related to the enabled trading partners.You can selectively enable profiles by deselecting the profiles that you do not want to enable.

8. 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.

9. Locate the trading partner. For more information, see Listing and Locating Trading Partners.

10. Click the trading partner name.

    The **View and Edit Trading Partner Profile** page is displayed.

11. Click **Edit profile**.

12. From the **Status** drop-down list, select **DISABLED**.

13. Click **Submit**.

14. 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.

Note: The associated service profiles are not automatically enabled.

15. Locate the trading partner. For more information, see Listing and Locating Trading Partners.

16. Click the trading partner name.

    The **View and Edit Trading Partner Profile** page is displayed.

17. Click **Edit profile**.

18. From the **Status** drop-down list, select **ENABLED**.

19. 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.

20. Locate the service as described in Listing and Locating Services.

21. Click the service name to select it.

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

22. 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.

23. Click **Edit Service Profile**.

    The **Edit Service Profile** page is displayed.

24. From the **Status** drop-down list, select **Disabled** or **Enabled**.

25. 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 and Exporting Data

The Import/Export module allows you to import and export management data. See the appropriate topic for instructions:

- Importing Management Data

- Exporting Management Data

- Deleting Trading Partner Profiles and Services Using Bulk Delete

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 conform to the `tpm.xsd` schema.
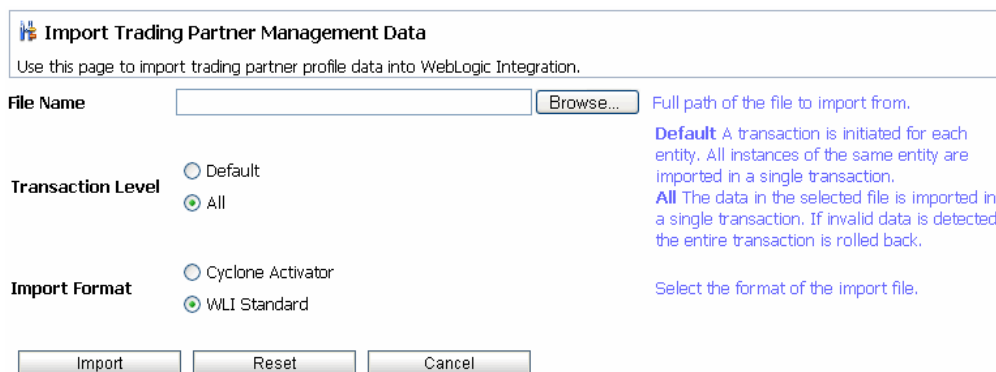
When you export TPM data using the console or the Bulk Loader utility, a file suitable for import is created. To learn more about the required structure, and how the file is used in import, export, and bulk delete operations, see Using the Trading Partner Bulk Loader in *Managing WebLogic Integration 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.

1. From the **Trading Partner Management** home page, select **Import/Export > Import**.

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

Figure 6-24 Import Trading Partner Management Data

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:

   – **WLI Standard**
   Imports the data that conforms to the TPM.xsd schema.

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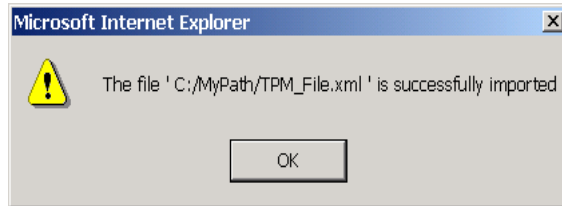
7. Click **OK** to dismiss the message box.

Related Topics

● Listing and Locating Trading Partners

Exporting Management Data

Before trading partners can participate in transactions hosted by Oracle 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.

1. From the **Trading Partner Management** page, select the **Import/Export > Export**.

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

2. Do one the following:

   – To export all trading partner management entities, select the **All** check box.

   – To export selected trading partner profiles, select 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**.

Figure 6-25 Choose Trading Partner Profiles

– To export selected services, select 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**.

Figure 6-26 Choose Service Page

Note: The above options are mutually exclusive.

3. Specify the **Export Format** by selecting :

   – **WLI Standard**

      Export data that conforms to the TPM.xsd schema.

4. In the **Encoding** field, specify the encoding, if other than the default. For more information, see http://www.iana.org/assignments/character-sets for valid values.

5. 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.

    – Uncheck the **Export All Referenced Entities** check box to export only the selected trading partners or services.

6. 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.

7. Click **Export**.

A download of the file is initiated. The dialog box that is displayed is browser-dependent, but typically, you are prompted to open or save the file.

For example, Internet Explorer displays the following dialog box.
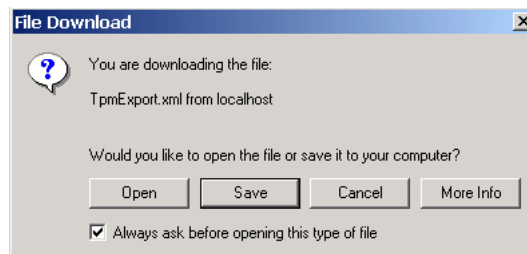
8. Select **Save** if prompted.

9. Specify the location and name of the file, then click **Save**.

The file is saved to the specified location.

Related Topics

- Importing Management Data

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.

1. From the **Trading Partner Management** page, select **Import/Export > Bulk Delete**.

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

Figure 6-27 Deleting Trading Partner Management Data

2. 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.

3. 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.

4. 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.)

– Uncheck the **Delete All Referenced Entities** check box to delete only the selected trading partners or services.

5. Click **Delete**.

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

Related Topics

- Deleting Trading Partner Profiles

- Deleting Certificates, Bindings, or Custom Extensions

- Deleting Services

- Deleting Service Profiles from a Service

Deleting Trading Partner Profiles

You can delete trading partner profiles from the **View and Edit Trading Partner Profiles** page. When you delete a trading partner, you must also delete all associated service profiles.

1. Locate the trading partners to be deleted. For more information, see Listing and Locating Trading Partners.

2. Click the check box to the left of each trading partner to select.

3. Click **Delete**.

   Note: If the selected trading partners are referenced in any service profiles, you are prompted to delete 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.

   A confirmation message is displayed.

4. Click **OK** to confirm.

   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
- Deleting Trading Partner Profiles and Services Using Bulk Delete
- Deleting Certificates, Bindings, or Custom Extensions

Deleting Certificates, Bindings, or Custom Extensions

You can delete certificates, bindings, or custom extension from the **Trading Partner Management Profile** page.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, then click the trading partner name.

   – From the **Trading Partner Management** page, select the **Certificates > Choose Trading Partner** from the left panel. In the **Choose Trading Partner** page, select the trading partner name from the **Name** drop-down list, then click **Go**.

2. In the **View and Edit Trading Partner Certificates** page, select the certificate you want to delete.

3. In the certificate table, click the **Delete** link for the entry to be deleted.

   A confirmation dialog box is displayed.

4. Click **yes** to confirm.

   A dialog box is displayed with the following question: "Do you want to remove the certificate from the keystore also?"

5. Click **OK** to remove the certificate from the keystore, or **Cancel** to leave the certificate in the keystore.

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 certificate summary table is displayed. The deleted certificate has been removed.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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.

1. Do one of the following:

   – Locate the trading partner as described in Listing and Locating Trading Partners, 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.

1. Locate the service as described in Listing and Locating Services.

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 Trading Partner Profiles and Services Using Bulk Delete

Deleting Service Profiles from a Service

You can delete service profiles from the **View And Edit Service Details** page.

1. Locate the service as described in Listing and Locating Services.

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.

● From the **Trading Partner Management** page, select **Statistics > View Statistics**.

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

1. Locate the service, as described in Listing and Locating Services.

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.

- The purge schedule for the system. To learn more, see Reporting and Purging Policies for Tracking Data.

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.

1. From the **Trading Partner Management** page, select the **Message Tracking** > **View All**.

The **View Messages** page is displayed.

Figure 6-28 View Messages Page

2. Do one or more of the following:

    – Filter the messages on the list as described in Filtering the Messages Displayed.

    – 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.

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.

1. From the **View Messages** page, select **Configure** from the drop-down.

2. Click **Go** to display the **Filter the Displayed Messages** page.

Figure 6-29 Filter Displayed Messages Page

3. 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.

4. 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.

1. From the **View Messages** page, 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.

System Configuration

The **System Configuration** module allows you to:

- View and set the purge schedule for tracking data.

- Start and stop the purge process.

- Enable and disable the transmission of data to an offline datastore.

- View and set the JNDI name for the datastore used to store data offline.

- View and set the default tracking level, reporting data, and purging policy for processes.

- Create, view, and change password store and aliases.

- Configure SFTP settings.

Note: You must be logged in as a member of the Administrators or IntegrationAdministrators group to make any changes to the system configuration. For more information, see About WebLogic Integration Users, Groups, Roles, and Security Policies in User Management in the *Worklist Console Online Help*.

Figure 7-1 System Configuration

The following topics are provided:

- About System Administration

- Overview of the System Configuration Module

- Viewing the Configuration for Tracking, Reporting, and Purging Data

- Configuring the Reporting Data and Purge Processes

- Configuring the Reporting Datastore

- Configuring the Default Data Policy and Tracking Level for Processes

- 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 SFTP

About System Administration

The following sections provide background information related to system administration:

- Process 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 Data Policy and Tracking Level for Processes.

- Setting tracking level for a process type, see Viewing and Changing Process Details.

Reporting and Purging Policies for Tracking Data

Tracking data includes:

- Process instance history (see Process Tracking Data above for tracking levels).

- Trading partner message history (see Configuring the Mode and Message Tracking 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.

- 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.

● 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.

● Configuring the reporting data stream, see Configuring the Reporting Data and Purge Processes.

● Setting the system default reporting data policy level, see Configuring the Default Data Policy and Tracking Level for Processes.

● Setting the reporting data policy for a process, see Viewing and Changing Process Details.

● 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 Oracle 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.

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:

Table 7-1 System Configuration Module

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
Tracking Data Purge and Reporting Data Policy Settings	Enable or disable reporting data generation.	Configuring the Reporting Data and Purge Processes
	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 Datastore

Table 7-1 System Configuration Module (Continued)

Page	Associated Tasks	Help Topics
Default Tracking Level and Reporting Data Policy for Processes	Change the default tracking level or default reporting data policy for processes.	Configuring the Default Data Policy and Tracking Level for Processes
Purge		
Purge Tracking Data	Request an immediate purge cycle.	Manually Starting and Stopping the Purge Process
	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
	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
Add New Password Alias	Add a password by assigning a unique alias and defining the password.	Adding Passwords to the Password Store
Edit Password Alias	Change the password associated with a password alias.	Changing the Password for a Password Alias
SFTP		
View the SFTP Configuration	View the SFTP configuration. SFTP Client Factory name and if the public keys sent from the server (Server Keys) are to be accepted or not.	Configuring SFTP
Edit SFTP Configuration	Edit the SFTP configuration.	Configuring SFTP

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.

- Default tracking level for processes and tasks.

- Default reporting data policy for processes.

Figure 7-2 Current Tracking and Reporting Data Settings

1. From the home page, select the **System Configuration** module. The **Current Tracking and Reporting Data Settings** is displayed by default.

Note: You can also click **Tracking, Purging, and Reporting Policies** on the left menu to access the **Current Tracking and Reporting Data Settings** page.

Table 8-1 describes the properties displayed on the page:

Table 7-2 Elements of Current Tracking and Reporting Data Settings page

Property	Description
Reporting Data Datastore	
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.
Reporting Data Datastore JNDI Name	JNDI name of the database to which reporting data is written when the reporting data stream is enabled.
Purge Schedule	
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.
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
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.
Default Variable Tracking Level	The default variable tracking level setting is Off.

Table 7-2 Elements of Current Tracking and Reporting Data Settings page (Continued)

Property	Description
Reliable Tracking	If this property is On, then the process tracking data is written in the same transaction of the process. If a problem is encountered during this operation, then the complete transaction including the process transaction is rolled back.
	If this property is Off, then tracking data is written in a different transaction of the process. If a problem is encountered during this operation, then there will be no impact on the process transaction.
Reliable Reporting	If this property is On, then process reporting data is written in the same transaction of the process. If a problem is encountered during this operation, then the complete transaction including the process transaction is rolled back.
	If this property is Off, then reporting data is written in a different transaction of the process. If a problem is encountered during this operation, then there will be no impact on the process transaction.

Related Topics

- Configuring the Reporting Data and Purge Processes

- Configuring the Reporting Datastore

- Configuring the Default Data Policy and Tracking Level for Processes

- Process Tracking Data

- Reporting and Purging Policies for Tracking Data

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.

Figure 7-3 Tracking Data Purge and Reporting Data Policy Settings

1. From the home page, select the **System Configuration** module. The **Current Tracking and Reporting Data Settings** is displayed by default.

Note: You can also click **Tracking, Purging, and Reporting Policies** on the left menu to access the **Current Tracking and Reporting Data Settings** page.

2. In the **Purge Schedule** section, click the **Configure**.

3. Do one or more of the following:

   – 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.

4. 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

- Viewing the Configuration for Tracking, Reporting, and Purging Data

Configuring the Reporting Datastore

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

Figure 7-4 Edit Reporting Data Configuration Settings Page

1. From the home page, select the **System Configuration** module. The **Current Tracking and Reporting Data Settings** is displayed by default.

Note: You can also click **Tracking, Purging, and Reporting Policies** on the left menu to access the **Current Tracking and Reporting Data Settings** page

2. In the **Reporting Data Datastore** section, click the **Configure** link.

3. To enable or disable the reporting data stream, check or uncheck the **Enable Reporting Data Generation** check box.

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

Configuring the Default Data Policy and Tracking Level for Processes

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

1. From the home page, select the **System Configuration** module. The **Current Tracking and Reporting Data Settings** is displayed by default.

Note: You can also click **Tracking, Purging, and Reporting Policies** on the left menu to access the **Current Tracking and Reporting Data Settings** page.

2. 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.

Figure 7-5 Default Tracking Level and Reporting Data Policy for Processes

3. Do one or both 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**.

– From the **Reliable Tracking** drop-down list, select **On** or **Off**.

– From the **Reliable Reporting** drop-down list, select **On** or **Off**.

4. 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

- Process Tracking Data

- Reporting and Purging Policies for Tracking Data

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.

Figure 7-6 Purge Tracking Data

If the purge process is scheduled to run regularly, tracking data, which includes process history,
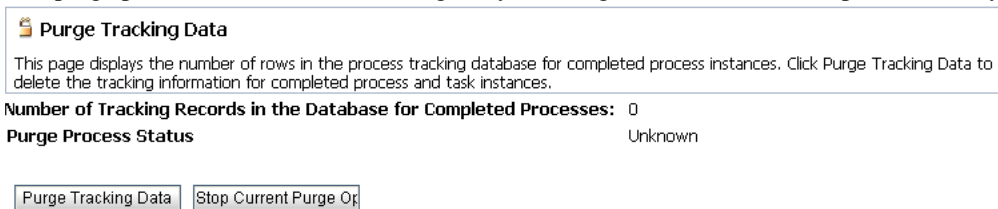
task history, and trading partner integration message history, is purged from the runtime datastore according to the schedule currently set. If required, you can request that the purge process run immediately, or if a purge operation is underway, you can manually stop the process, as described in the following procedure.

1. From the home page, select the **System Configuration** module.

2. From the left menu, 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

- Configuring the Reporting Data and Purge Processes

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.

Figure 7-7 Add New Password Alias

1. From the home page, select the **System Configuration** module.

2. From the left menu, select **Password Store**.

3. From the left menu, select **Create New** to display the **Add 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 New Password Alias** page is displayed again. 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

- Listing and Locating Password Aliases

Listing and Locating Password Aliases

The V**iew and Edit Password Aliases** page lists the password aliases defined in the password store.

Figure 7-8 View and Edit 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.

   – Sort the list again. 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.
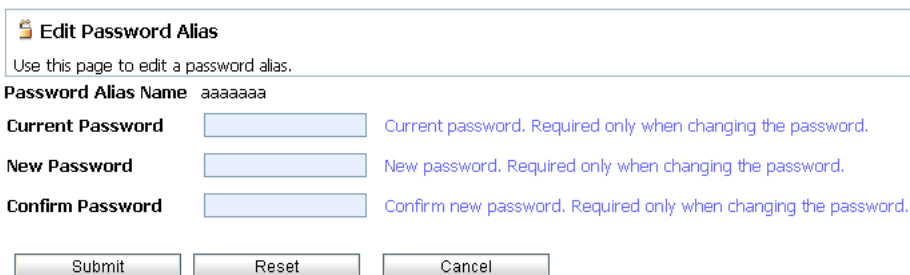
Related Topics

- Adding Passwords to the Password Store

- Changing the Password for a Password Alias

- Deleting Passwords from the Password Store

Changing the Password for a Password Alias

The **Edit Password Alias** page allows you to change the password associated with the password alias.

Figure 7-9 Edit Password

1. Locate the password alias. See Listing and Locating Password Aliases.

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.

1. Locate the password alias or aliases to be deleted. See Listing and Locating Password Aliases.

2. Click the check box to the left of the password aliases to be deleted to select them.

3. Click **Delete Selected Aliases**.

Configuring SFTP

The **Current SFTP Settings** page shows you the existing SFTP configuration.

Figure 7-10 Current SFTP Settings

1. From the home page, select the **System Configuration** module.

2. From the left panel, select **Configure**.

3. Click on the Configure link to edit the current settings. You can now edit the settings on the **Current SFTP Settings** page.

4. Enter the class name of the SFTP Client factory.

5. Specify whether the public key from the SFTP server must be accepted by default or not. The default setting is **Yes**. Click **Submit** to save changes, **Reset** to restore the original settings, and **Cancel** to return to the View mode of the **Current SFTP Settings** page.

System Configuration

CHAPTER **8**

XML Cache

The module allows you to:

- Add new entries to the XML cache.

- Update existing XML cache entries.

- Delete existing XML cache entries.

- View the code of existing XML 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 About WebLogic Integration Users, Groups, Roles, and Security Policies in User Management in the *Worklist Console Online Help*.

The following topics are provided:

- About the XML Cache

- Overview of the XML Cache Module

- 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

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:

Figure 8-1 XML Cache Module

Page	Associated Tasks	Help Topics
Configure XML Cache	Add a new XML document to the cache.	Adding XML Documents to the XML Cache
	Update an existing XML document.	Updating an XML Document in the XML Cache
	View the code for an existing XML document.	Viewing the Code for an XML Document
	Delete an existing XML document.	Deleting an XML Document from the XML Cache

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

Adding XML Documents to the XML Cache

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

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

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

Figure 8-2 Configure XML Cache

2. In the first **Key** field, enter a key for the XML document you want to add to the XML cache.

   Note: Entries in the **Key** field are case insensitive and should not exceed 256 characters.

   The key is a logical name that uniquely identifies the XML document in the XML cache. Do not use Multibyte Character Set 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

- Viewing All XML Documents in the XML Cache

Updating an XML Document in the XML Cache

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

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.

    Note: Entries in the **Key** field are case insensitive and should not exceed 256 characters.

    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

- Adding XML Documents to the XML Cache

- Viewing All XML Documents in the XML Cache

Viewing the Code for an XML Document

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

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 to view.

    Note: Entries in the **Key** field are case insensitive and should not exceed 256 characters.

3. Click **Get**.

   The code for the specified XML document is displayed in the **View XML Cache Content** page.

Figure 8-3 View XML Cache Content

View XML Cache Content

```
<!DOCTYPE weblogic-web-app PUBLIC "-//BEA Systems, Inc.//DTD Web Application
8.1//EN" "http://www.bea.com/servers/wls810/dtd/weblogic810-web-jar.dtd">
<weblogic-web-app>
 <jsp-descriptor>
  <!-- Comment the jspServlet param out to go back to weblogic's jspc -->
  <jsp-param>
   <param-name>jspServlet</param-name>
   <param-value>weblogic.servlet.WlwJSPServlet</param-value>
  </jsp-param>
  <jsp-param>
   <param-name>debug</param-name>
   <param-value>true</param-value>
  </jsp-param>
 </jsp-descriptor>
 <url-match-map>weblogic.servlet.utils.SimpleApacheURLMatchMap</url-match-map>
</weblogic-web-app>
```

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

- Adding XML Documents to the XML Cache

- Viewing All XML Documents in the XML Cache

Deleting an XML Document from the XML Cache

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

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 to delete.

   Note: Entries in the **Key** field are case insensitive and should not exceed 256 characters.

3. Click **Delete**.

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

Related Topics

- About the XML Cache

- Adding XML Documents to the XML Cache

- Viewing All XML Documents in the XML Cache

Viewing All XML Documents in the XML Cache

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

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.

Figure 8-4 View XML MetaData Keys

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.