BEA AquaLogic® Service Bus

WS Transport User Guide

Version: 3.0
Revised: February 2008

Contents

WS Transport

WS Transport

The Web Services Reliable Messaging (WSRM) specification describes a protocol that allows messages to be delivered reliably between distributed applications even if a software, system, or network failure occurs.

WS-ReliableMessaging is a specification co-developed by IBM, BEA, Microsoft and TIBCO Systems. This specification is not the same as the WS-Reliability (WSR), which is a competing specification developed by OASIS.

WSRM functionality is available in ALSB as the WS transport. ALSB supports the specification submitted in February 2005. For more information about the specification, see Web Services Reliable Messaging Protocol (WS-ReliableMessaging).

The WS transport implements both inbound and outbound requests for services derived from SOAP 1.1 and SOAP 1.2 based WSDLs with WSRM policy. However, the WSRM policy can be a part of the WSDL or can be attached to the service. In addition, security policies can also be declared in the WSDL or can be associated with a WSDL-based service. When you configure WSDL-based services with WSRM policies using the ALSB Console, you must choose the WS transport for the service. ALSB checks for the WSRM policy when you save the service configuration and throws a validation error if WSRM policies are not declared for the WSDL associated with the service.

The following are the key features of the WS Transport

- One-way and request/response message patterns. For more information, see Messaging Patterns.

- Exactly-once transfer between WS transport and other transports (JMS, SB, and Tuxedo transports) that support XA transactions.
- HTTPS with basic authentication, and with client-certificate authentication (two-way SSL) but without client authentication,. For more information, see Authentication and Authorization of Services.
- Retaining WSRM security configuration while importing resources. For more information, see Importing and Exporting Resources.
- Assignment of transport-level access control policy to a WS proxy service in ALSB Console. Only an administrator can assign this policy. For more information, see Assigning Transport Access Control to Proxy Services.
- WS-Addressing specification submitted in August 2004. For more information, see Web Services Addressing (WS-Addressing).
- WS-I Basic Profile compliance. For more information, see Web Services Interoperability.
- Quality of Service (QoS) in ALSB for WS proxy service is always set as Exactly Once. For more information, see Quality of Service in Modeling Message Flow in ALSB in *AquaLogic Service Bus User Guide*.

  You can set the QoS only in the RM policy file using the `<beapolicy:QOS>` element. This element has one attribute, `QOS`, which can take any of the following values:

  - `AtMostOnce`
  - `AtLeastOnce`
  - `ExactlyOnce`
  - `OnOrder`

  Note: QoS for WS transport is different from QoS for ALSB.
- You can associate only SOAP 1.1 and SOAP 1.2 based WSDLs with WSRM policy with a proxy or business service. For more information, see Configuring Proxy Services to Use the WS Transport and Configuring Business Services to Use the WS Transport.

Supported Functionality

This section provides detailed information about functionalities supported by the WS transport.

Messaging Patterns

WSRM supports both one-way and request/response messaging patterns. The WS transport does not support reliable response. While the request is always reliable, the response is not sent reliably.

For business services, sending a request to an external web service is asynchronous. Successful invocation implies that the message is given to the RM layer successfully and it will be delivered reliably. However, successful invocation does not mean that the message is sent to the endpoint and has successfully invoked the web service. For the request/response messaging pattern, the response is received from the external web service for a request. In this case, the request and response paths have two different transactions and run in two different threads. The response pipeline is executed evenly for one-way messaging message pattern. For the one-way pattern, response pipeline invocation means that the message reliably reached the target destination and the web service invocation is complete.

Policies

A proxy service or business service that uses the WS transport must have a WS-Policy with RM assertions. This also implies that services that use any other transport must not have any WS-Policy with RM assertions. WS-Policy with RM assertions and WSSP v1.2 transport-level security assertions are supported for the WS transport. However, WSSP v1.2 message-level security assertions and 9.X BEA proprietary security assertions are not supported. RM assertions should only be bound at the service level and not at the operation or operation request/response levels.

Note: You must use only one RM assertion for a WS-Policy.

WS-Policy Configurations

WS-Policies can be configured in any one of the following two ways:

- WS-Policy configuration is specified as part of the WSDL associated with the service. The policies specified in the WSDL may be included in the WSDL or referred in the WSDL.
- WS-Policy is assigned to the service from the ALSB Console.

Note: You can use only one of these methods to associate a security policy with the service. So, if you configure a policy using the ALSB Console, any policies defined in the WSDL are ignored.

Streaming Content for Large Messages

The WS transport does not have streaming support for large messages because the underlying infrastructure (WLS JAX-RPC stack) uses a fully materialized payload. However, when you configure a proxy service for large message processing, the message is fully materialized into a Java object by the WS transport using the streaming optimization in ALSB. During the proxy service configuration, you can specify if you want to stream content for large message processing by buffering content either in memory or to disk. For more information, see "Streaming body Content" in Message Context in *AquaLogic Service Bus User Guide*.

Web Services Interoperability

The WS transport supports web services interoperability through WS-I Basic Profile. Currently, ALSB proxy services do not follow all the WS-I Basic Profile restrictions. However, any services configured to use this transport strictly follow the WS-I Basic Profile specification. WS proxy services do not have a WS-I Compliance check in the service configuration and always follow WS-I Basic Profile. This is valid for SOAP1.1 WSDL bindings as WS-I Basic Profile applies only to SOAP 1.1.

Authentication and Authorization of Services

This section provides information about how proxy and business services are authenticated and authorized.

Proxy Service Authentication

WS proxy services support both basic and client-certificate (two-way SSL) authentication. When basic authentication is specified in the WS-Policy, all HTTP requests, including RM protocol messages to the WS proxy service must have a valid username and password.

Proxy service authentication is supported as follows:

- Outbound client-certificate authentication using SSL key-pair assigned to the service key provider referenced by the proxy service.
- Username-password identity propagation through a WS proxy service (with basic authentication) to any other outbound transport, or outbound WSS username token.
- Credential mapping between WS proxy service (with basic or two-way SSL authentication) and any other transport.

- Sending asynchronous responses from WS proxy service to a RM client through HTTP or HTTPS. The default protocol used by proxy and business services is HTTP.
- Asynchronous responses from a WS proxy service to an RM client connect to the `AcksTo` or `ReplyTo` endpoint references specified by the RM client. The RM client can use either HTTP or HTTPS URL. If the RM client uses HTTPS, the RM client can request a client certificate during the SSL handshake. The WS transport uses the SSL key-pair of the service key provider upon request.

Proxy Service Authorization

Administrators can assign a transport-level access control policy to a WS proxy service in ALSB Console. As with all transports, this policy is enforced after the inbound transport provider passes the request message to the ALSB binding layer before invoking the request pipeline. For more information, see Assigning Transport Access Control to Proxy Services.

Business Service Authentication

WS business services support basic authentication and client-certificate authentication. Outbound basic authentication is supported by means of a service account. Username/password identity propagation and credential mapping are provided by the service account. However, a static account can also be used for authentication. The service account can be static, pass-through or mapped. Pass-through authentication allows passing a username/password from the client request to the backend RM service. Mapped service accounts allow credential mapping. Static service accounts are used when fixed credentials are required.

WS business services also support SSL client-certificate authentication (two-way SSL). The key-pair (private key and certificate) used for outbound two-way SSL is not configured on the WS business service, but on the service key provider referenced by the proxy service.

Routing a single message to a WS business service may involve multiple HTTP/S requests from the ALSB server and backend service. All such messages are subject to the authentication method configured in the WS business service. In other words, if the service is configured for basic authentication, all messages sent from ALSB include the HTTP Authorization header with the username/password and if the message is configured for client-certificate authentication, ALSB uses the key-pair to authenticate all messages.

Using the WS Transport

You can use the WS transport to reliably deliver messages in a distributed network.

The WSRM functionality is available as a transport only for SOAP 1.1 and SOAP 1.2 based WSDLs with WSRM policy. Ensure that the services are associated with a SOAP 1.l or 1.2 WSDLs with RM-policy or that a RM-policy is attached to the services. You can configure the WS-Policy in a WSDL or assign it to a service. For more information, see Configuring WS Policies.

Prior to configuring proxy and business services to use the WS transport, ensure that the required WSDLs or WS-Policy files are available in your ALSB domain. For more information, see Adding Resources to an ALSB Domain, Configuring Proxy Services to Use the WS Transport, and Configuring Business Services to Use the WS Transport.

You can optionally configure an error queue for services and ALSB delivers failed messages into the queue. The queue can be a distributed queue. Because this queue is not created automatically, you must create it prior to configuring the services. For more information, see Configuring an Error Queue.

In addition, you can also import and export resources using the ALSB Console. For more information, see Importing and Exporting Resources and Importing and Publishing Services Using UDDI Registries.

Adding Resources to an ALSB Domain

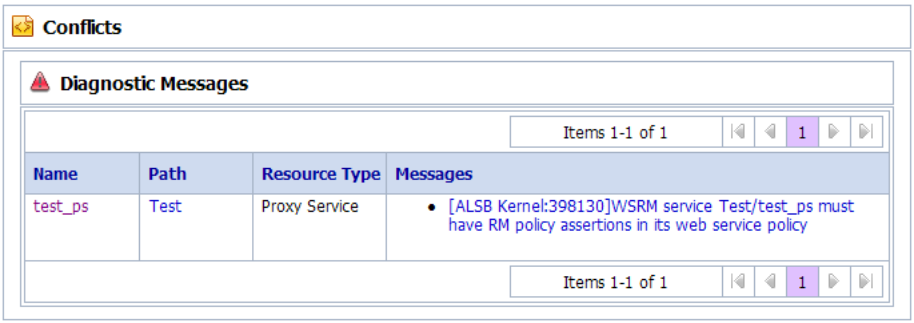
You can add WSDLs, and custom WS-Policy files to the domain using the ALSB Console. For more information, see Adding WSDLs in WSDLs and Adding Custom WS-Policies in *Using the AquaLogic Service Bus Console*.

Configuring WS Policies

The WS transport can be used only with SOAP WSDLs that have a WSRM policy. You can configure a WS-Policy in a WSDL or assign a WS-Policy to a Service from the ALSB Console. For more information, see Policies.

When no RM police assertions are specified for the WSDL associated with a service (you configure a service using a WSDL with no policy), a validation message appears when you activate the session.

Figure 1 Conflicts – When no RM police assertions are specified for the WSDL



To resolve this conflict, you need to update the WSDL or attach the policy to the service. For more information, see Attaching WS Policies to a Service and Using Web Services Policy to Specify Inbound Message-Level Security in the *AquaLogic Service Bus Security Guide*.

Attaching WS Policies to a Service

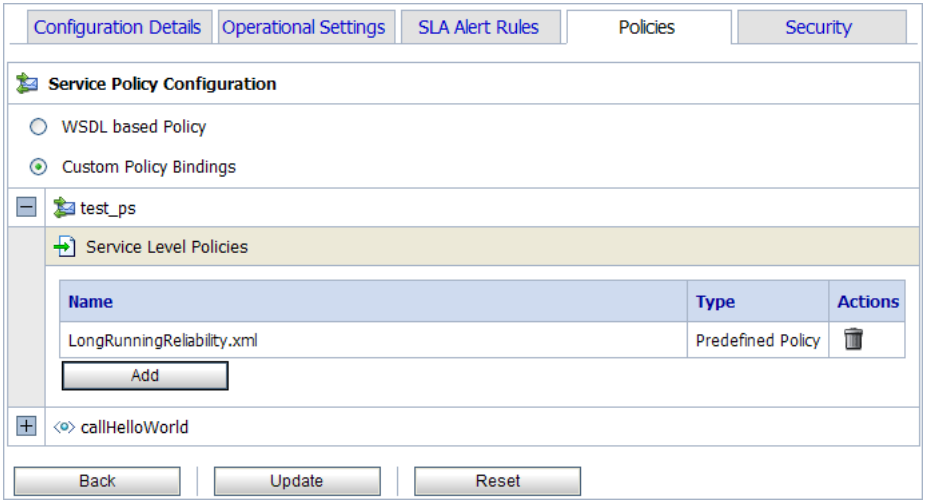
To attach a WS-Policy file to a service:

1. Locate the proxy or business service and click on the name of the service.

   The View a Proxy Service or Business Service page appears.

2. Click on the **Policies** tab. You can view the service policy configuration details.

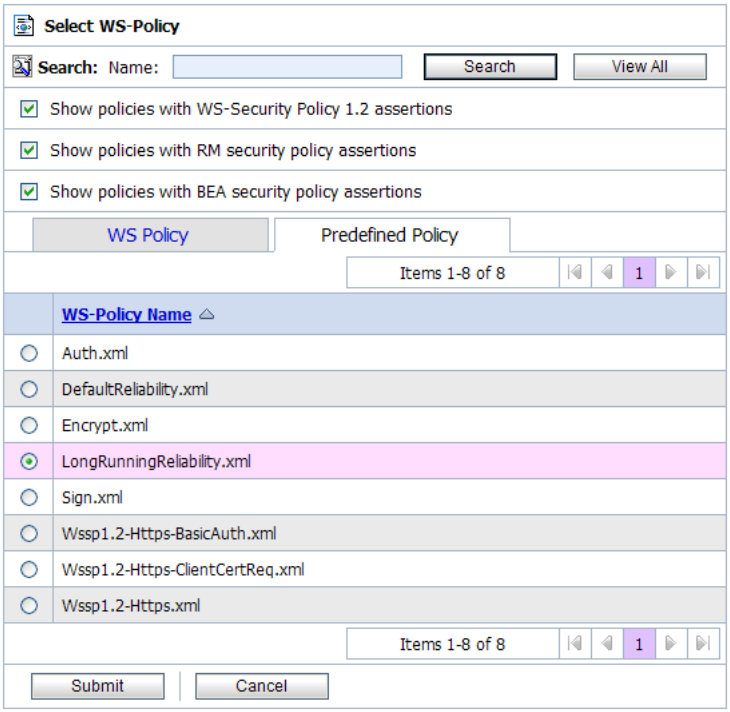
Figure 2 Configuration Details



3. Click on the **Custom Policy Bindings** radio button.
4. Expand the proxy service folder and click **Add**.

   The Select WS-Policy page appears.

Figure 3 Select WS-Policy



5. You can search for the required policy and select the policy from the list of predefined policies or custom policy resources and click **Submit**.
6. Click **Update**.

The selected policy is now attached to the proxy service or business service.

Note: When you attach a WS-Policy to a service, any policies defined in the WSDL associated with the service are ignored.

Configuring an Error Queue

By default, undelivered messages are discarded after the specified number of retries. However, you can optionally configure error queues for business services and ALSB delivers messages that fail in the message flow into these queues.

You must configure a JMS queue for errors. BEA recommends that you configure a error queue locally instead of a remote queue.

For business services, when response timeout occurs, the response pipeline is invoked with an error. If sequence expiration interval is reached, the message is placed in an error queue configured for the business service and the response pipeline is invoked with an error. However, if the response timeout has already occurred, the message is placed in the error queue, but the response pipeline is not invoked.

Note: For both one-way and request-response services, putting failed messages in the error queue is only a best effort.

Configuring Proxy Services to Use the WS Transport

Proxy services using the WS transport must be associated with WS-Policy with RM assertions. For more information, see Policies.

A proxy service receives the requests from clients and passes it to the message flow after the processing related to WSRM is done. The proxy service could also send the response back to the client after receiving it from the response pipeline. A proxy service using the WS transport can be invoked from any other proxy service and it follows the same behavior as it is invoked by an external client.

When an HTTP proxy server is configured (per WLS wsee stack), WS proxy services send asynchronous messages using the HTTP proxy server.

Proxy services based on WSDL with SOAP 1.2 binding support SOAP 1.2 messages only and throw a fault with version mismatch error for SOAP 1.1 messages. Similarly, proxy services based on WSDL with SOAP 1.1 binding support SOAP 1.1 messages only and throw a fault with version mismatch error for SOAP 1.2 messages.

When you create a proxy service from the ALSB Console, select the transport protocol as `ws` in the Transport Configuration page.

Note: For more information about configuring proxy services, see Proxy Services: Creating and Managing in *Using the AquaLogic Service Bus Console*.

Table 1 describes the fields you can specify to configure a proxy service to use the WS transport:

Table 1 Fields Required to Configure a Proxy Service to Use the WS Transport

Field	Description
Protocol	Select `ws` from the list of available protocols.
Endpoint URI	Endpoint configuration for a proxy service that uses the WS transport is similar to that of http/s proxy service configuration. Specify the URI in `/contextPath` format. **Note:** Make sure that the context path is unique for proxy services that use either HTTP or the WS transport.

Now, you must specify configuration details specific to the WS transport.

Table 2 describes the dispatch policy and advanced options like the retry count and retry delay values you can specify to configure the WS transport for a proxy service.

Table 2 Fields Required to Configure WS Transport for a Proxy Service

Field	Description
Dispatch Policy	Select a dispatch policy for this endpoint. Dispatch policy refers to the instance of WLS Work Manager that you want to use for the service endpoint. For information about work managers, see Using Work Managers to Optimize Scheduled Work and Create Work Manager in the WebLogic Server Administration Console Online Help.
Retry Count	The number of times, the WSRM layer tries to deliver a message to the ALSB message flow. The default is 3. If an unhandled exception occurs in the request flow of a proxy, the incoming WS Transport message is redelivered to the message flow up to the number of times specified by this value. This is important for reliably processing the WS transport messages. **Note:** When the message delivery fails, the current transaction is rolled back, but the message is not removed from the queue. The server tries to send the message until the message is successfully delivered or the retry limit is reached. When the retry limit is reached, that message is removed from the queue or moved to an error queue. The error queue can be a distributed queue and can be created from WebLogic Server Administration Console. For more information, see Configuring an Error Queue.
Retry Delay	The duration that the server should wait before retrying to deliver the message. The default is 5 seconds.

For more information about configuring proxy services using the WS transport, see WS Transport Configuration Page in Proxy Services: Creating and Managing in *Using the AquaLogic Service Bus Console*.

Assigning Transport Access Control to Proxy Services

Administrators can assign a transport-level access control policy to a WS Proxy Service in the ALSB Console. As with all transports, this policy is enforced after the inbound transport provider passes the request message to the ALSB binding layer before invoking the request pipeline.

Transport-level access control policies are managed within ALSB sessions. When the session is activated, the access policy is stored in an Authorization Provider. At runtime, the binding layer calls the security framework authorization APIs, which in turn call the authorization provider.

To determine the access control of the proxy service resources at runtime, administrators can add one or more policy conditions. For example, a basic policy might simply name the Operator user. At runtime, the security framework interprets this policy as "only an Operator can access the proxy service resources." For more information, see Adding Policy Conditions.

WARNING: Proxy services configured in the ALSB Console to use the WS transport can also be viewed in the WebLogic Server Administration Console. Administrators can assign an access control policy from the WebLogic Server Administration Console and the ALSB Console. However, policies assigned from the WebLogic Server Administration Console will have no effect and are not evaluated at runtime. Only access control policies assigned in the ALSB Console are enforced.

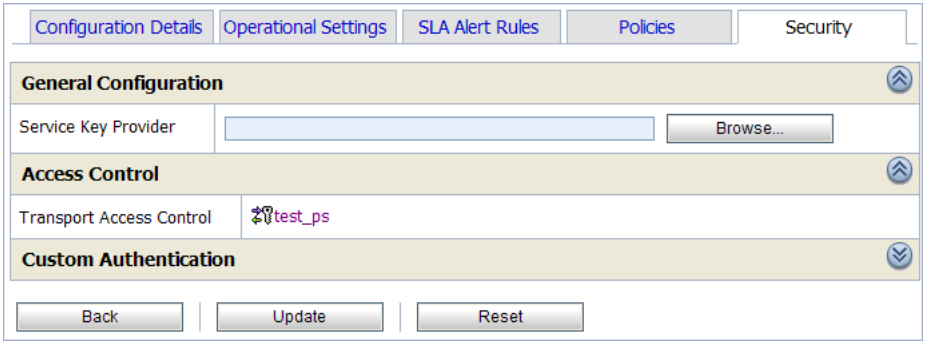
To assign transport access control to a proxy service:

1. Locate the proxy service and click the proxy service name.

   For more information, see Locating Proxy Services in Proxy Services: Creating and Managing in *Using the AquaLogic Service Bus Console*.

2. In the View a Proxy Service page, click the **Security** tab.

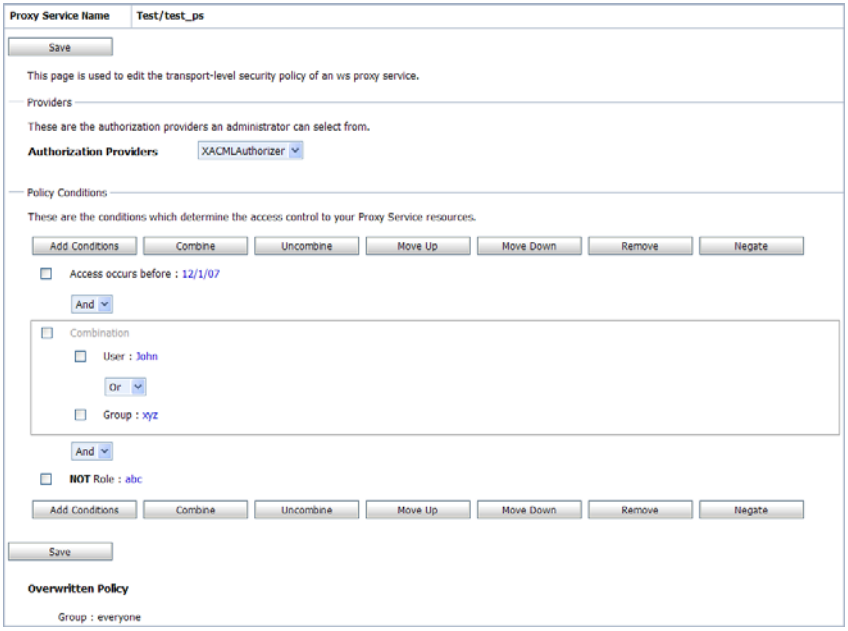
Figure 4 Security tab for a Proxy Service



3. Click the name of the proxy service.

   You can set the transport-level policy of the proxy service in this page.

Figure 5 Transport-Level Policy



4. Click **Add Conditions**. The Choose a Predicate page appears.
5. Select the required predicate and click **Next**. The Edit Arguments page appears.
6. Enter the parameters and values associated with the predicate to define the policy conditions.

   Administrators can:

   – Create complex conditions and combine them using the logical operators AND and OR (which is an inclusive OR). A combination of conditions can be uncombined later, if required.

   – Negate any condition, which would make sure that the inverse of the specified policy condition is applied.

   – Specify the order in which the policy conditions are executed.

   – Remove existing policy conditions.

   – Apply the AND and OR operators between multiple conditions.

   At runtime, the entire collection of conditions must be true for the proxy service.

For more information about the parameters to be specified for each predicate, see Adding Policy Conditions.

7. Click **Save**.
8. Click **Back** and click **Update**.

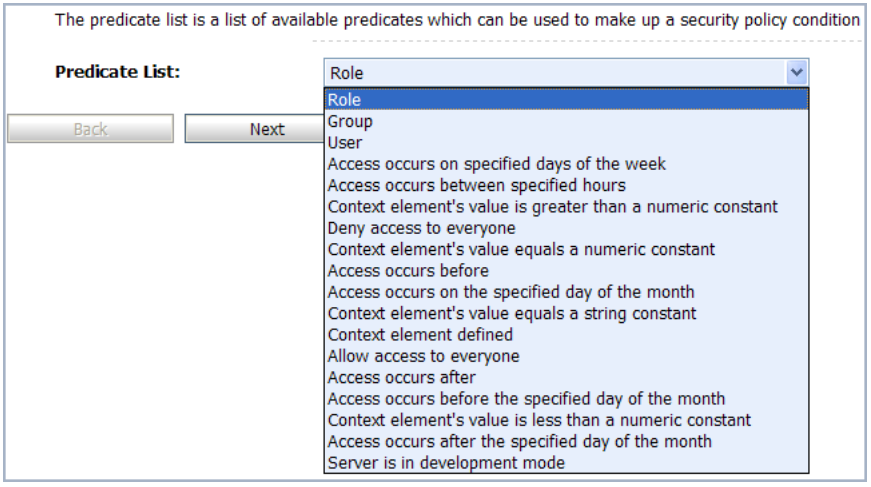
The specified access control policy conditions are now associated with the proxy service and applied at runtime.

Adding Policy Conditions

The policy conditions set by an administrator control access the access control to the proxy service resources. When you add a condition to a policy statement, you can use any of the existing predicates or policy conditions. Each predicate is a predefined statement that can be used to define the security policy statement. For each predicate, you need to edit the arguments that are associated with that predicate.

Click **Add Conditions** to view the list of predicates.

Figure 6 List of Predicates



These predicates include:

- Basic policy conditions that include adding specified users, groups, or roles, allowing or denying access to everyone, and so on.

- Date and time based policy conditions, which are used to grant access to the resources based on the date or time you specify.
- Context element policy conditions, which are used to create policies based on the value of HTTP Servlet Request attributes, HTTP Session attributes, and EJB method parameters.

To Add or Remove a role to the policy condition:

1. Select **Role** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Specify the role and click **Add**.

   You can add one or more roles to this policy condition. If you add multiple roles, the condition evaluates as true if the user is a member of ANY of the roles associated with this policy condition.

   Note: To remove any role, select the role in the Remove list and click **Remove**.
4. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To add a group to the policy condition:

1. Select **Group** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Specify the group name and click **Add**.

   You can add one or more groups to this policy condition. If you add multiple groups, the condition evaluates as true if the user is a member of ANY of the groups associated with this policy condition.

   Note: To remove any group, select the group in the Remove list and click **Remove**.
4. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To add a user to the policy condition:

1. Select **User** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Specify the user name and click **Add**.

You can add one or more users to this role.

Note: To remove any user, select the user in the Remove list and click **Remove**.

4. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only on specified days of the week:

1. Select **Access occurs on specified days of the week** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the day of the week.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only between a specified time:

1. Select **Access occurs between specified hours** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the start time and the end time between which access to resources to enabled. Enter time in hh:mm AM|PM format.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only when the context element's value is greater than a numeric constant:

1. Select **Context element's value is greater than a numeric constant** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the name of the context element.

4. Enter a numeric value. Access to resources is enabled only when the specified context element's value is greater than this number.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To deny access to everyone:

1. Select **Deny Access to everyone** from the **Predicate List** drop-down list.
2. Click **Finish**.

All users and groups are denied access to the proxy service resources.

To enable access to proxy service resources only when the context element's value is equal to a numeric constant:

1. Select **Context element's value equals a numeric constant** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the name of the context element.
4. Enter a numeric value. Access to proxy service resources is enabled only when the specified context element's value is equal to this number.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only before a specified date:

1. Select **Access occurs before** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the date before which access to proxy service resources is enabled. Enter date in m/d/yy or m/d/yy hh:mm:ss AM|PM format.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only on the specified day of the month:

1. Select **Access occurs on the specified day of the month** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the day of the month on which access to proxy service resources is enabled.

   Access to proxy service resources is enabled only after an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to 31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only when the context element's value is equal to a string constant:

1. Select **Context element's value equals a string constant** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the name of the context element.
4. Enter a string value. Access to proxy service resources is enabled only when the specified context element's value is equal to this string value.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only when the defined context element is available:

1. Select **Context element defined** from the **Predicate List** drop-down list.
2. Click **Finish**.

Access to proxy service resources is enabled only when the specified context element exists.

To allow access to everyone:

1. Select **Allow Access to everyone** from the **Predicate List** drop-down list.
2. Click **Finish**.

Access to proxy service resources is enabled to all users and groups.

To enable access to proxy service resources only after a specified date:

1. Select **Allow access after** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the date after which access to proxy service resources is enabled. Enter date in m/d/yy or m/d/yy hh:mm:ss AM|PM format.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only before the specified day of the month:

1. Select **Access occurs before the specified day of the month** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the day of the month before which access to proxy service resources is enabled.

   Access to proxy service resources is enabled only before an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to 31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only when the context element's value is less than a numeric constant:

1. Select **Context element's value is less than a numeric constant** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the name of the context element.
4. Enter a numeric value. Access to proxy service resources is enabled only when the specified context element's value is less than this number.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only after the specified day of the month:

1. Select **Access occurs after the specified day of the month** from the **Predicate List** drop-down list.
2. Click **Next**. The Edit Arguments page appears.
3. Enter the day of the month after which access to proxy service resources is enabled.

   Access to proxy service resources is enabled only after an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to 31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.
4. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter GMT + hh:mm and if time zone in your location is behind GMT, enter GMT -hh:mm.
5. Click **Finish**.

The condition is added to the policy statement and displayed on the policy conditions page.

To enable access to proxy service resources only when Server is running in development mode:

1. Select **Server is in development mode** from the **Predicate List** drop-down list.
2. Click **Finish**.

Users and groups can access the proxy service resources only when the server is running in development mode.

Routing the WS Transport Through an HTTP Proxy Server

When an HTTP proxy server is configured, WS business services send outbound messages using the HTTP proxy server. For information about specifying the HTTP proxy server details in your client application, see "Using a Proxy Server When Invoking a Web Service" in Invoking Web Services in *WebLogic Web Services: Getting Started*.

Configuring Business Services to Use the WS Transport

Business services using the WS transport must be associated with WS-Policy with RM assertions. For more information, see Policies. A business service acts as a client for invoking an external reliable web service. It sends a request to the service and the response is received by an application deployed by ALSB, which invokes the response path.

When you create a business service from the ALSB Console based on the WSDL resource, select the transport protocol as `ws` in the Transport Configuration page.

Note: For more information about configuring business services, see Business Services: Creating and Managing in *Using the AquaLogic Service Bus Console*.

Table 1 describes the fields you must specify to configure a business service to use the WS transport, specify the following fields:

Table 1 Configuring a Business Service to use WS Transport

Field	Description
Protocol	Select ws from the list of available protocols.
Load Balancing Algorithm	Specify the load balancing algorithm as any one of the following values: • Round-robin • Random • Random-weighted • None
Endpoint URI	Point to the location of the web service. Endpoint configuration for a business service that uses the WS transport is similar to that of http/https configuration. Specify the URI in `http://host:port number/name` or `https://host:port number/name` format. Business services can have multiple endpoint URIs pointing to different reliable web services.

Table 1 Configuring a Business Service to use WS Transport

Field	Description
Retry Count	In case of delivery failure when sending outbound requests, specify the number of times to retry individual URL endpoints. The number in this field indicates the total number of times URIs are retried (not the number of URIs in the list).
Retry Iteration Interval	Specify the number of seconds the system should pause between retries of all the endpoint URIs in the list.
Retry Application Errors	Select Yes or No. In case of delivery failure when sending outbound requests, specify whether or not to retry endpoint URIs based on application errors (for example, a SOAP fault). For more information, see Error Handling.

To configure the WS transport for a business service, specify the values as described in Table 2:

Table 2 Configuring WS Transport for Business Service

Field	Description
Response Timeout	If the response does not come in the defined interval after sending a request, response pipeline is invoked with an error saying that service is timed out. A value of `0` implies that there would be no response timeout.
Service Account	Specify a service account. **Note:** This is only applicable if the WS business service has a ws-policy that requires basic authentication For more information, see Service Accounts in *Using the AquaLogic Service Bus Console*.
Queue Error Messages	Select this option if you want to send failed requests to an error queue. The following fields are available only if you select this option.

Table 2 Configuring WS Transport for Business Service

Field	Description
Error Queue URI	Error queue used for failed requests in the business service. Specify the URI in `jms://host:port/conn-factory-jndi-name/queue-jndi-name` format. **Note:** This queue can be a distributed queue. It is not created automatically so, make sure that a valid queue is available. For more information, see Configuring an Error Queue.
JMS Error Queue Service Account	The service account to be used for connecting to the JMS error queue.
Use SSL for Error Queue	Select this option to use SSL for connecting to a JMS error queue.

For more information about configuring business services using the WS transport, see "WS Transport Configuration Page" in Business Services: Creating and Managing in *Using the AquaLogic Service Bus Console*.

Error Handling

You can configure the WS transport-based business services to handle application errors by specifying whether or not to retry business service endpoint URIs when application errors occur. See "Retry Application Errors" in Creating and Configuring Business Services - Transport Configuration page in *Using the AquaLogic Service Bus Console*.

An application error occurs when a WS transport-based business service receives a SOAP fault as a response and the BEA-380001 error code is generated.

Note: When a response timeout or sequence timeout occurs for a request to a business service, the ALSB server tries to send the message to the next URI based on the load balancing algorithm. This behavior does not depend on the `Retry Application Errors` option.

Importing and Exporting Resources

When a resource exists in an ALSB domain, you can preserve the security and policy configuration details while importing that resource to ALSB by selecting the `Preserve Security and Policy Configuration` option. When you select this option, the values in the

existing resource are preserved when you import them, even if the security and policy configurations have been updated in the resource.

For information about importing resources from the ALSB Console, see Importing Resources in *Using the AquaLogic Service Bus Console*.

Importing and Publishing Services Using UDDI Registries

When a proxy service is published to an UDDI registry, the service is converted into WS business service with the WSDL. If present, the authentication configuration is also exported to UDDI.

When a WSDL-based business service with WSRM policy is imported from an UDDI registry to ALSB, the service is imported as a WS business service that is automatically configured to use the WS transport. For more information, see Policies.

For more information, see UDDI in *Using the AquaLogic Service Bus Console.*