



Forum Sentry™ Version 9

WSDL Policies Guide



Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Sentry™ Web Services Security Gateway, Presidio™ OpenPGP Security Gateway, Forum FIA Gateway™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 WSDL Policies Guide, published July 2024.

D-ASF-SE-783019

Table of Contents

FORUM SYSTEMS SENTRY™ VERSION 9	I
WSDL POLICIES GUIDE	I
INTRODUCTION TO THE WSDL POLICIES GUIDE	1
Audience for the WSDL Policies Guide	1
WSDL LIBRARIES	3
WSDL Library Features	3
WSDL POLICIES	4
WSDL Features	5
Services Tab Screen Terms for WSDL Policies	6
Virtual Directory Detail Terms for WSDL Policies	6
Single WSDL Policy Examples	10
Add a WSDL from File, URI or WSDL Library	10
Create New Network Policies for the WSDL Policy	11
View Components of a WSDL Policy	12
Upgrade a WSDL by File, URL or UDDI Search	16
Enable or Disable Operations on a WSDL Policy	18
WSDL Same-name Operations Support	19
WSDL Policy Access Control	20
Apply Intrusion Detection and Prevention to a WSDL Policy	20
Enable WS-ReliableMessaging for a WSDL policy	20
Virtualized WSDL Policies Examples	21
Create a WSDL Library	21
Create a Virtualized WSDL Policy	22
Upgrade a WSDL File from the WSDL Library	26
Update Remote Policy on a WSDL Policy	27
SERVICES FOR WSDL POLICIES	28
Virtual Directories	28
Services Tab Terms	28
How Inbound and Outbound Messages Map to a Virtual Directory	29
Relationship Between HTTP Network Policies and WSDL Policies	30
Default Filter Expression in a Virtual Directory	30
Replace Expression in a Virtual Directory	30
Task List Groups on WSDL Operations	31
WSDL Schema Tightening	31
Virtual Directories Examples	33
WSDL Virtual Directory Settings	33
Enable or Disable a Virtual Directory	35
WSDL Policy Dynamic WSDL Retrieval with Enable WSDL Access	35
View or Reconfigure a Virtual Directory	35
WSDL Operation Level Access Control	36
WSDL Fault Policy Settings	37
Override WSDL Endpoint Location on Export	37
Edit WSDL Schema Constraints	38
Override WSDL Validation Settings on WSDL Operations	39
Request Filters for WSDL Policies	40
TASK LISTS AND TASK LIST GROUPS FOR WSDL POLICIES	42
Relationship Between Task List Groups and Elements of a WSDL Policy	42
Global Task List Groups For All WSDL Operations	43
Task List Group to Pre-Process Requests	43
Task List Group to Post-Process Requests	44
Task List Group to Pre-Process Responses	44
Task List Group to Post-Process Responses	44
Task List Groups on WSDL Operations	45
SETTINGS FOR WSDL POLICIES	46

WSI Validation Features and Examples with WSDL Policies	48
Reconfigure Validation Tests	49
SOAP XSD Validation Enforcement Examples	51
Validate SOAP Documents	52
Access Control with WSDL Policies	53
IDP RULES FOR WSDL POLICIES	54
Edit WSDL IDP Group	55
Edit WSDL Operation IDP Group	55
LOGGING SETTINGS FOR WSDL POLICIES	56
Logging Tab Screen Terms for XML Policy	56
DOCUMENTS FOR WSDL POLICIES	57
WSDL PUBLISHING	57
Dynamic WSDL Retrieval	57
Business Keys	58
Publish WSDL Screen Terms	59
Publish a WSDL Policy to UDDI	60
WS-RM (RELIABLE MESSAGING) POLICIES	62
WS-RM License Feature	62
Reliable Messaging - WSRM Policies	62
TRANSFERRING EXPORTING AND IMPORTING WSDL POLICIES	63
APPENDIX	64
Appendix A - Constraints in WSDL Policies Guide	64
Appendix B - Specifications in WSDL Policies Guide	64
Appendix C - Virtual Directory Reference Chart in WSDL Policies Guide	64
INDEX	66

List of Figures

Figure 1: The System Distinguishes Between Same-name Operations on Various Screens	19
Figure 2: How Inbound and Outbound Messages Map to Virtual Directories	29
Figure 3: Relationship Between Task List Groups and Elements of a WSDL Policy.	42
Figure 4: Relationship of USER ACLs to WSDL and Listener Policies.	53
Figure 5: The Virtual Directory Screen and Associated Options.	65

INTRODUCTION TO THE WSDL POLICIES GUIDE

Audience for the WSDL Policies Guide

The *Forum Systems Sentry™ Version 9 WSDL Policies Guide* for System Administrators who will:

- Create, import or export WSDL Policies.
- Publish WSDL projects.
- Specify WSDL endpoint location upon export.
- Map WS-I Basic Profile 1.0 Test Assertions to WSDL policies and SOAP validation.
- Create merged WSDL policies.
- Apply schema tightening to WSDL policy message objects.
- Apply a Task List or Task List Group to an XML policy.
- Apply a Pattern Match policy to XML requests/responses via the Pattern Match task on a Task List or as part of a Task List Group.
- Associate IDP Groups to WSDL Policies.

* For more information on storing elements or documents to a database, refer to the Data Sources section of the *Forum Systems Sentry™ Version 9 Logging Guide*.

Conventions Used in the WSDL Policies Guide

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. (For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.)

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

For the focus of this document, the STATUS column is displayed on WSDL policies, the Virtual Directory and individual requests and responses.

WSDL POLICIES		
<input type="text"/>	<input type="text"/>	
Search Usage: type any text Filter Usage: type or select the label		
No Labels		
<input type="checkbox"/> NAME	PORT	STATUS
<input type="checkbox"/> Cust FS WSDL	<input checked="" type="checkbox"/> QAServicesSoap	
<input type="checkbox"/> WSDL Policy 1	<input checked="" type="checkbox"/> MainServiceHttpsSoap11Endpoint	
	<input checked="" type="checkbox"/> MainServiceHttpsSoap12Endpoint	

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: Cust FS WSDL

Upgrade

Export WSDL

Publish WSDL

WSI Validation

Services

Task Lists

Settings

IDP Rules

Logging

Documents

<input type="checkbox"/>	SERVICE	PORT	STATUS	VIRTUAL URI	PHYSICAL URI
<input type="checkbox"/>	QAServices	QAServicesSoap		http://127.0.0.1:80/qaservice/qaservice.asmx	
<div>EnableDisable</div>					

Service: QAServices — Port: QAServicesSoap

<input type="checkbox"/>	OPERATION	STATUS	ACL	INPUT MESSAGE	OUTPUT MESSAGE	IDP GROUP
<input type="checkbox"/>	BuildElementXML		[Allow All]	BuildElementXMLSoapIn	BuildElementXMLSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/>	BuildNestedXML		[Allow All]	BuildNestedXMLSoapIn	BuildNestedXMLSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/>	BuildSizeXML		[Allow All]	BuildSizeXMLSoapIn	BuildSizeXMLSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/>	BuildValidateFailXML		[Allow All]	BuildValidateFailXMLSoapIn	BuildValidateFailXMLSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/>	Echo		[Allow All]	EchoSoapIn	EchoSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/>	SeverallInputs		[Allow All]	SeverallInputsSoapIn	SeverallInputsSoapOut	<input checked="" type="checkbox"/> Default Operation Group (0)
<div>EnableDisable</div>						

Request Filters, however, have a status of Enabled or Disabled only.

<input type="checkbox"/> #	HTTP REQUEST FILTER	FORMAT	DESCRIPTION	STATUS
<input type="checkbox"/> 1	SOAP 1.1 Filter	Simple	WSDL 1.1 SOAP 1.1 HTTP Filter	
Restore Defaults Enable Disable				

Assumptions

This document assumes that the reader is familiar with the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

WSDL LIBRARIES

A WSDL library is a repository for storing one or more WSDL documents. Using a WSDL Library, a virtual WSDL policy can be created by selecting operations across one or more WSDL documents and merging them into a single WSDL document and policy. The advantage of a virtual WSDL is that the new WSDL maps to a single IP and port and combines and exposes only the selected operations from one or more web services into a common “virtual” WSDL document.

WSDL Library Features

Features available in a WSDL library include adding, editing and deleting WSDL libraries; adding, viewing, and deleting WSDL documents in Libraries; and upgrading existing WSDL library documents and all dependent WSDL policies.

(For more information, refer to the Virtualized WSDL Policies Examples section of this document.)

WSDL LIBRARIES > WSDL LIBRARY

WSDL LIBRARY

Library Name:

QA_WSDL_Library

Library Description:

Save

<input type="checkbox"/>	WSDL NAME	WSDL DESCRIPTION	
<input type="checkbox"/>	gaservice		Upgrade WSDL
<input type="checkbox"/>	TrainingWsdL		Upgrade WSDL

RemoveAdd

WSDL POLICIES

A WSDL policy is a set of rules that provide a policy for processing of Web Service SOAP messages flowing through the system, and can be imported from a file, URL or UDDI search.

WSDL policies include the following accessible properties and actions; each manage a portion of the WSDL policy and is detailed later:

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: qa

Upgrade Export WSDL Publish WSDL WSI Validation

Services Task Lists Settings IDP Rules Logging Documents

<input type="checkbox"/> SERVICE	PORT	STATUS	VIRTUAL URI	PHYSICAL URI
<input type="checkbox"/> QAServices	QAServicesSoap		http://192.168.1.79/qaservice/qaservice.asmx	http://169.254.84.66/qaservice/qaservice.asmx

Enable Disable

Service: QAServices — Port: QAServicesSoap

<input type="checkbox"/> OPERATION	STATUS	ACL	INPUT MESSAGE	OUTPUT MESSAGE	IDP GROUP
<input type="checkbox"/> BuildElementXML		[Allow All]	BuildElementXMLSoapIn	BuildElementXMLSoapOut	<input type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/> BuildNestedXML		[Allow All]	BuildNestedXMLSoapIn	BuildNestedXMLSoapOut	<input type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/> BuildSizeXML		[Allow All]	BuildSizeXMLSoapIn	BuildSizeXMLSoapOut	<input type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/> BuildValidateFailXML		[Allow All]	BuildValidateFailXMLSoapIn	BuildValidateFailXMLSoapOut	<input type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/> Echo		[Allow All]	EchoSoapIn	EchoSoapOut	<input type="checkbox"/> Default Operation Group (0)
<input type="checkbox"/> SeverallInputs		[Allow All]	SeverallInputsSoapIn	SeverallInputsSoapOut	<input type="checkbox"/> Default Operation Group (0)

Enable Disable

- **Services:** To manage the Virtual Directory of the WSDL policy, Tasks and Schema Tightening, which are found under any Input and Output Messages. Also, Request Filters, Operation settings and Input and Output Message settings.
- **Task Lists:** To manage Task List Groups. (For more information on the Task Lists or performing Tasks, refer to the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.)
- **Settings:** To manage validation settings including SOAP Document validation and WS-I Basic Profile Tests validation. Also manages general WSDL policy settings and Task List Group processing settings.
- **IDP Rules:** To manage IDP Groups which represent a collection of Intrusion Detection and Prevention Rules. (For information on IDP Rules, refer to the *Forum Systems Sentry™ Version 9 IDP Rules Guide*.)
- **Logging:** To manage the policy level logging settings for the WSDL policy.
- **Documents:** To view the WSDL file and WSDL schemas.

From an open WSDL Policy, users may select:

- **Upgrade:** To upgrade the WSDL policy from a File, URL or WSDL Library.
- **Export:** To export all or specific operations on a WSDL policy based on access control.
- **Publish:** To publish a WSDL to a UDDI server.
- **WSI Validation:** To review the WS-I Basic Profile 1.0 Test Assertion Report for design-time validation of the WSDL.
- **Enable / Disable:** To enable or disable the Virtual Directory or specific Operations.

WSDL Features

An overview of the features available in a WSDL policy includes:

- Review the WS-I Basic Profile Assertion Report for the WSDL document.
- Import and validate WSDL documents via the wizard.
- Add or upgrade a WSDL Policy from a file, URL or searching a UDDI.
- Create new or associate existing listener and/or remote network policy.
- View WSDL services, operations, ports and virtual directories.
- Enable dynamic WSDL retrieval.
- Enable / disable operations on a WSDL.
- Export a WSDL document.
- Publish WSDL document to UDDI.
- Specify alternate WSDL endpoint location upon export.
- Selectively configure WSI BP 1.0 Assertions to use during design-time or run-time validation of SOAP messages.
- Apply access control.
- SOAP document content validation.
- Associate an IDP Group.
- Transfer, import or export WSDL policies. (For more information, refer to the *Forum Systems Sentry™ Version 9 System Management Guide*).
- Apply Task List or Task List Group to all operations for Request or Response messages.
- Apply Task List or Task List Group to individual operations Request or Response messages.
- Use Error Template from Listener Policy with WSDL policy or select another.
- Enable WS-ReliableMessaging.

WSDL Import Sources

WSDL POLICIES > NEW WSDL POLICY

NEW WSDL POLICY

Name*:

WSDL Source: ☒ File Choose File No file chosen

☐ URL Browse UDDI

☐ WSDL Library

HTTP Basic Authentication:
Username Password

DEFAULT Edit

☐ Automatically load imported files.

Next

When adding a WSDL to the system, the following options are presented:

- Add the WSDL by File.
- Add a WSDL by URL (http) or a secure URL (https) with optional Basic Authentication or SSL X.509 credentials. The WSDL by URL method requires the **?WSDL** syntax be used at the end of the URL.
- Add a WSDL from a WSDL Library.
- Automatically load all referenced import files found in the selected WSDL file. With the Automatically load imported files checkbox checked, all imported WSDL and schemas are attempted to be loaded based on the import reference location. If unsuccessful, you are

prompted to import each file individually. With this checkbox unchecked, Administrators have the option to choose the source of the import reference manually.

Services Tab Screen Terms for WSDL Policies

The following table describes each term and definition on the Services tab in WSDL policies.

TERM	DEFINITION
Service	The top level service that is provided by the actual web service.
Port	Where the virtual directory mappings are performed for the WSDL services.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Yellow status light = a required functional element of this policy is disabled; i.e. The listener is disabled or the remote network policy is disabled.• Red status light = disabled policy.
Virtual URI	The Unique Resource Indicator (URI) path to the location of the local web service policy and used by clients to access this policy.
Physical URI	The Unique Resource Indicator (URI) path used by the system to send requests after processing. This is the actual URI and server location of the physical web service server.
Operation	The methods or operations provided by the web service.
Status	The status of each operation on the WSDL.
ACL	The User Access Control List associated with the provided operation.
Input Message	The SOAP request of the provided operation.
Output Message	The SOAP response of the provided operation.
IDP Group	The IDP Group associated with each operation of the WSDL.

Virtual Directory Detail Terms for WSDL Policies

The following table describes each term and definition found on the Virtual Directory of WSDL policies.

TERM	DEFINITION
Listener Policy	The Listener Policy on the system to associate with this Virtual Directory.
User Virtual Host as a Regular Expression	Using regular expressions within the virtual host definitions allow the HOST header to be matched based on the defined regular expression pattern. Enable this checkbox if the value entered in the virtual host field is to be interpreted as a regular expression rather than a string match for comparing to the inbound HOST header.

Virtual Host	<p>The Virtual Host option allows the IP:Port combination to have a 3rd parameter which uses the HOST header of the inbound request to determine which virtual directory policy matches. With no virtual host defined, the virtual directory is matched simply based on IP, Port and URI. With virtual host defined, the virtual directory is matched based on IP, Port, HOST Header, and URI.</p> <p>i.e.</p> <p>http://10.5.1.1:80/test/policy HOST: prod.company.com</p> <p>http://10.5.1.1:80/test/policy HOST: dev.company.com</p>
Virtual Path	The path used to receive requests.
Virtual URI	The Unique Resource Indicator (URI) path to the location of the local web service policy and used by clients to access this policy.
Filter Expression	<p>This value is a regular expression, which is used to evaluate the trailing portion of the incoming URL filtered and allowable on a virtual URI request before processing to determine if the URI pattern is allowed.</p> <p>Once the trailing portion is matched, this trailing portion may be applied to the physical URI based on the value of the Replace Expression field.</p> <p>Retaining the default value of <i>/?</i> in this field means that the trailing portion of the virtual URI must end with a <i>/</i> and then can have any other character.</p> <p>Changing the value to <i>***</i> means that any URI pattern is allowed.</p> <p>For more information, review the Default Filter Expression in a Virtual Directory section and the Replace Expression in a Virtual Directory section of this document. For information on Regular Expressions, refer to Appendix E - Regular Expressions Guide in the <i>Forum Systems Sentry™ Version 9 IDP Rules Guide</i>.</p>
Replace Expression	This value defines the portion of the Filter Expression value that is to be used as the trailing portion of the physical URI. The default value \$0 will use the entire portion of the URI matched by the Filter Expression field.
Send to Remote Server	When Checked, the request will be processed and sent to the selected remote policy. When unchecked, Sentry will process the request and send the processed request directly back to the client without ever sending to a remote policy.
Show all remote policies	When checked, the Remote Policies drop down list displays all existing Remote Policies on the system. By default, remote policies that do not match the remote endpoints in the WSDL are not shown.
Remote Policy	The Remote Policy associated with this Virtual Directory.

Physical URI	The Unique Resource Indicator (URI) path used by the system to send requests after processing. This is the actual URI and server location of the physical web service server.
Process Response	Indicates the Process Response status of the selected remote policy.
IP ACL	The IP Access Control List that will be enforced on this Virtual Directory. With Unrestricted selected, there is no access control by IP enforced.
ACL	The User Access Control List that will be enforced on this Virtual Directory. With the Allow All ACL selected, there is no access control enforced. The selected User ACL grants access of this WSDL policy to any member of the User ACL.
Password Authentication	<p>When set to From Listener Policy, the password authentication credentials captured at the Listener Policy level will be used for enforcement.</p> <p>When set to Specify, the administrator can choose to enforce any of the following Password Authentication options:</p> <ul style="list-style-type: none"> • Use basic authentication • Use digest authentication • Use cookie authentication • Use form post authentication • Username and Password Parameters are used with the form post authentication • Require password authentication (any): to enforce a successful authentication not just capture the credentials. <p>For more information on Password Authentication please refer to the Forum Sentry v9 Access Control Guide.</p>
Enable WSDL access	When checked, a GET request to the virtual URI ?WSDL will return the WSDL file for this policy.
Redirect Policy	The Redirect Policy that is associated to this Virtual Directory. Redirect Policies allow redirection to a different URL based on four events: Authentication Success, Authentication Failure, No Credentials and On Error. A valid Redirect Policy will need to be configured on the Resources>>Redirect Policies page in order to associate a Redirect Policy to the Virtual Directory.
Error Template	The Error Template used by this WSDL policy to format errors to the client.
Reliable Messaging Policy	The WS-RM policy that is associated with this Virtual Directory.
Publish a different location in exported WSDL	When checked, WSDL is exported with endpoints overridden by values entered in Published protocol, Published host and Published port fields.
Published protocol	Protocol to use while publishing this WSDL.
Published host	IP on which to publish this WSDL.

Published port	Port on which to publish this WSDL.
-------------------	-------------------------------------

For information on HTTP Request Filters, refer to the Request Filters for WSDL Policies section of this document.

Single WSDL Policy Examples

Examples for a single WSDL policy include:

- Add a WSDL Policy from a WSDL File, URL or WSDL Library.
- Create New Network Policies for a WSDL Policy.
- Use Existing Network Policy for a WSDL Policy.
- Add a WSDL Policy and Import Referenced Schemas.
- Export WSDL Policy Document.
- View Components of a WSDL Policy.
- Export WSDL Policy Documents.
- Upgrade a WSDL by File, URL or UDDI Search.
- Enable / Disable Operations on a WSDL Policy.
- Publish a WSDL Policy to UDDI.
- WSDL Policy Access Control.
- Apply Intrusion Detection Prevention to a WSDL Policy.
- Enable WS-ReliableMessaging for a WSDL Policy.

Add a WSDL from File, URI or WSDL Library

Adding a WSDL Policy from a File

- Navigate to the WSDL Policies screen and select **New**.
- In the Name field, enter the **Name** for this WSDL policy.
- In the Description field, enter a **Description** for this WSDL policy.
- From the WSDL File Location, select the **File** radio button. Click **Browse**.
- Navigate your file system to locate and select a **WSDL file**. Click **Open**.
- Click **Next**.

Adding a WSDL Policy from a URL

Adding a WSDL policy from a URL supports HTTP and HTTPS protocols. When using HTTPS, the system uses the SSL Initiation Policy set on the System screen as a default.

- Navigate to the WSDL Policies screen and select **New**.
- In the Name field, enter the **Name** for this WSDL policy.
- In the Description field, enter a **Description** for this WSDL policy.
- From the WSDL File Location, select the **URL** radio button.
- In the URL text field, enter the **URL** for a WSDL file.
- In the Username field, enter a **username** for HTTP Basic Auth authentication (if required).
- In the Password field, enter a **password** for HTTP Basic Auth authentication (if required).
- Click **Next**.

Adding a WSDL Policy from a WSDL Library

- Navigate to the **WSDL Libraries** screen.
- Click **New**.
- In the Library Name field, enter a **name** for this WSDL library.
- In the Library Description field, enter a **description** for this WSDL library.
- Click **Create**.
- Click **Add**.
- In the WSDL Name field, enter the **name** of a WSDL file to add to this library.
- In the WSDL Description field, enter a **description** for this WSDL file.
- From the WSDL Source area, click the **File** or **URL** radio button.

- Enter a **URL** in the URL field or click **UDDI**.
- In the Username and Password field, enter a **username** and **password** (if required).
- Click **Next**.
- Navigate to the WSDL Policies screen and select **New**.
- In the Name field, enter the **Name** for this WSDL policy.
- In the Description field, enter a **Description** for this WSDL policy.
- From the WSDL File Location, select the **WSDL Library** radio button.
- From the WSDL Library drop down list, select the name of a **WSDL Library**.
- Click **Next**.
- Click **Save**.

Create New Network Policies for the WSDL Policy

You may create a new Network Listener Policy when creating a WSDL Policy.

WSDL POLICIES > NEW WSDL POLICY

SET LISTENER POLICY

Please specify a listener policy for service: QAServices, port: QAServicesSoap

☐ Select from existing listener policies
NewXMLPolicy-Listener (0.0.0.0:88) [Edit](#)

☒ Create a new HTTP listener policy
Listener Policy Name*:
Use Device IP: ☐
Listener IP*:
Listener Port*:

SET VIRTUAL DIRECTORY PATH

Virtual Directory Path:

SET REMOTE POLICIES

☒ Send to remote server

Please specify a remote network policy for the URL: http://192.168.28.37/qaservice/qaservice.asmx

☐ Select from existing remote policies
qaservice-remote (192.168.28.37:80) [Edit](#)

☒ Create a new HTTP remote policy for this remote server
Remote Policy Name*:
Remote Policy Host*:
Remote Policy Port*:

Next

- From the SET LISTENER POLICY section, select the **Create a new HTTP listener policy** radio button.
- Enter the **Listener IP address** in the Listener IP field or check the **Device IP** checkbox to use the assigned device IP of the system.
- Enter the **Listener Port** in the Listener Port field.
- Enter the **virtual directory URI path** for accessing this policy (here users can “cloak” the back-end URI by entering a value different from the actual physical URI of the back-end web service).

- Select the **Create a new HTTP remote policy for this remote server** radio button.
- Enter the **Remote IP** in the Remote Policy Host field.
- Enter the **Remote Port** in the Remote Policy Port field and then click **Next**.

Use Existing Network Policy for the WSDL Policy

You may use an existing Network Listener policy when creating a WSDL policy as long as at least one listener policy has been created on the system. You may use an existing Remote policy as long as at least one Remote policy has been created on the system.

Add a WSDL Policy and Import Referenced Schemas

With the **Automatically load imported files** checkbox checked, all imported WSDL and schemas are attempted to be loaded based on the import reference location. If unsuccessful, you are prompted to import each file individually. With this checkbox unchecked, Administrators have the option to choose the source of the import reference manually.

Administrators must also associate a network policy to the WSDL policy to enable the Virtual Directory.

View Components of a WSDL Policy

To view the components of a WSDL policy (services, ports and operations); select the policy name from the **WSDL Policies** screen.

Viewing WSDL Services

Navigate to the WSDL Policies screen and click a WSDL policy name link. The WSDL POLICY screen appears with the Services tab visible. This tab lists the Service name, Port, Virtual Directory, Physical URI, and a listing of all Operations and Input and Output Messages.

WSDL POLICIES

Search Usage: type any text

Filter Usage: type or select the label

Always Show Expanded

NAME	PORT	STATUS	VIRTUAL URI	IDP GROUP	DATE MODIFIED
qa	QAServicesSoap		http://192.168.1.79/qaservice/qaservice.asmx	Default WSDL Policy Group (8)	2017/11/01 14:58
qaservice	QAServicesSoap			Default WSDL Policy Group (8)	2017/11/01 15:01

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: Cust FS WSDL

Services

Task Lists

Settings

IDP Rules

Logging

Documents

SERVICE	PORT	STATUS	VIRTUAL URI	PHYSICAL URI
QAServices	QAServicesSoap		http://127.0.0.1:80/qaservice/qaservice.asmx	

Service: QA Services — Port: QA ServicesSoap

OPERATION	STATUS	ACL	INPUT MESSAGE	OUTPUT MESSAGE	IDP GROUP
BuildElementXML		[Allow All]	BuildElementXMLSoapIn	BuildElementXMLSoapOut	Default Operation Group (0)
BuildNestedXML		[Allow All]	BuildNestedXMLSoapIn	BuildNestedXMLSoapOut	Default Operation Group (0)
BuildSizeXML		[Allow All]	BuildSizeXMLSoapIn	BuildSizeXMLSoapOut	Default Operation Group (0)
BuildValidateFailXML		[Allow All]	BuildValidateFailXMLSoapIn	BuildValidateFailXMLSoapOut	Default Operation Group (0)
Echo		[Allow All]	EchoSoapIn	EchoSoapOut	Default Operation Group (0)
SeverallInputs		[Allow All]	SeverallInputsSoapIn	SeverallInputsSoapOut	Default Operation Group (0)

Viewing WSDL Operations

View WSDL operations by clicking on any link under the OPERATION section. Click the operation link, and the Operation details screen appears. In this screen, users may apply an ACL for access control, view the remote Network policy associated with this WSDL, view the Physical URI of the remote Network policy and select an IDP Group to apply to this WSDL.

Services Task Lists Settings IDP Rules Logging Documents

Service: QAServices > Port: QAServicesSoap > Operation: Echo

OPERATION SETTINGS

ACL:

[Allow All] ▾

Remote Policy:

qa-remote

Physical URI:

http://169.254.84.66/qaservice/qaservice.asmx

IDP Group:

Default Operation Group ▾ [Edit](#)

Save

MESSAGES

[EchoSoapIn](#)

[EchoSoapOut](#)

FAULTS

No items to display

Viewing WSDL Port, Associated Network Policies and Settings

View WSDL ports, Virtual Directory and settings by clicking the link under PORT. The VIRTUAL DIRECTORY URI setting screen appears. From this screen, users can assign network policies and edit the URI settings, enable access control to the Port, enable dynamic access to this WSDL via “?WSDL”, and override the endpoint data that will be exposed on the WSDL file when exported.

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: Cust FS WSDL

[Upgrade](#) [Export WSDL](#) [Publish WSDL](#) [WSI Validation](#)

[Services](#) [Task Lists](#) [Settings](#) [IDP Rules](#) [Logging](#) [Documents](#)

Service: QAServices > Port: QA Services Soap

VIRTUAL DIRECTORY

Virtual URI: http://127.0.0.1:80/qaservice/qaservice.asmx(/.*)?

Physical URI:

WSDL SETTINGS

Enable WSDL access: ☐

☐ Publish a different location in exported WSDL

Published Protocol: http

Published Host:

Published Port:

VIRTUAL URI SETTINGS

Listener Policy: HttpListenerPolicy-1 [Edit](#)

Request Filter Policy: Request_Filter_Policy [Edit](#)

Virtual Host:

☐ Use virtual host as a regular expression

Virtual Path: /qaservice/qaservice.asmx

☐ Enable Virtual Path Case Insensitivity

Filter Expression: (/.)?

Replace Expression: \$0

Error Template: SOAP 1.1 Fault Template [Edit](#)

ACCESS CONTROL

IP ACL Policy: Unrestricted [Edit](#)

ACL Policy: [Allow All]

XACML Policy: [None]

Password Authentication: [From Listener Policy]

Redirect Policy: [None]

REMOTE SETTINGS

☐ Send to remote server

☐ Show all remote policies

Remote Policy: [None]

Remote Path:

Physical URI:

Process Response:

[Apply](#) [Save](#)

Export WSDL Policy Document

A WSDL document will be generated on export based on your WSDL policy settings. The WSDL can be exported directly from the policy from either the WebAdmin, or if enabled, for dynamic retrieval, the WSDL can be obtained using the Virtual URI of the policy with “?WSDL” appended to the HTTP(S) request. The resulting exported WSDL will show as the Virtual URI endpoint.

Export All Operations into a WSDL Policy

From the WebAdmin, you may export a WSDL document once the policy is created.

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: Cust FS WSDL

Upgrade Export WSDL Publish WSDL WSI Validation

Services Task Lists Settings IDP Rules Logging Documents

SERVICE	PORT	STATUS	VIRTUAL URI	PHYSICAL URI
QAServices	QAServicesSoap	ON	http://127.0.0.1:80/qaservice/qaservice.asmx	

Enable Disable

Service: QA Services — Port: QA ServicesSoap

OPERATION	STATUS	ACL	INPUT MESSAGE	OUTPUT MESSAGE	IDP GROUP
BuildElementXML	ON	[Allow All]	BuildElementXMLSoapIn	BuildElementXMLSoapOut	Default Operati
BuildNestedXML	ON	[Allow All]	BuildNestedXMLSoapIn	BuildNestedXMLSoapOut	Default Operati
BuildSizeXML	ON	[Allow All]	BuildSizeXMLSoapIn	BuildSizeXMLSoapOut	Default Operati
BuildValidateFailXML	ON	[Allow All]	BuildValidateFailXMLSoapIn	BuildValidateFailXMLSoapOut	Default Operati
Echo	ON	[Allow All]	EchoSoapIn	EchoSoapOut	Default Operati
SeveralInputs	ON	[Allow All]	SeveralInputsSoapIn	SeveralInputsSoapOut	Default Operati

Enable Disable

WSDL POLICY > EXPORT WSDL

EXPORT OPTIONS

☒ Export all operations

☐ Export operations based on ACL(s):

local_users

Export

- Navigate to the WSDL Policies screen and select a **WSDL policy name** link.
- From the top right section of the screen, click **Export**.
- Select the **Export all operations** radio button, and then click **Export**.
- The File Download screen appears.
- Click **Save**, and the Save as screen appears.
- Navigate your file system to the directory in which to save this file. Click **Save**.

Export Specific WSDL Operations Based on a User ACL

User Access Control Lists (ACLs) can be used to restart the operations which are exported either from the WebAdmin policy screen, or via dynamic “?WSDL” retrieval.

Follow these steps to export specific WSDL operations based on a User ACL:



- Navigate to the WSDL Policies screen and select a **WSDL policy name** link.
- Select an **Operation name** link.
- From the ACL drop down list, select an **ACL Policy** to associate with the selected operation, and then click **Save**.
- From the top right section of the screen, click **Export**.
- Select the **Export operations based on ACL(s)** radio button, and then click **Export**.
- The File Download screen appears.
- Click **Save**, and the Save as screen appears.
- Navigate your file system to the directory in which to save this file. Click **Save**.

Upgrade a WSDL by File, URL or UDDI Search

From the WebAdmin, you may upgrade a WSDL by file, URL or by searching a UDDI server while retaining the applied IDP Group, Virtual Directory and any tightened schema constraints previously created on the system.

If Upgrading a WSDL Policy by File

- Upgrade a WSDL by selecting the **File** radio button from the WSDL Source area.
- Click **Browse** and the Choose file screen appears.
- Navigate your file system, locate and click to highlight the new **WSDL file source**.
- Click **Open** and the Choose file screen closes.
- Click **Next**.

Note: The SET LISTENER POLICY and SET REMOTE POLICY screen appears only when the endpoint location (remote policy IP/port) has changed; otherwise, this screen does not appear.

- Choose to **Create a new HTTP listener policy**, or select an **existing policy**.
- Enter the **Use Device IP**.
- Choose to **Create a new HTTP remote policy for this remote server**, or select an **existing policy**.
- Click **Next**.

If Upgrading a WSDL Policy by URL

- Upgrade a WSDL by URL by selecting the **URL** radio button from the WSDL Source area.
- Enter a **username** and **password** in the Username and Password fields (if required).
- In the text box, enter a URL (<http://10.5.6.85/qaservice/qaservice.asmx?WSDL>), and then click Next.

If Upgrading a WSDL Policy by UDDI Search

The Search UDDI screen provides the means for entering standardized search criteria for UDDI registries. (For more information on UDDI data structures, refer to the UDDI SDK section at the web resource <http://msdn.microsoft.com/library/default.asp?url=/nhp/default.asp?contentid=28001204>.) Follow these steps to upgrade a WSDL project by a UDDI search:

WSDL POLICY > UPGRADE WSDL POLICY

UPGRADE WSDL POLICY

Name*: Cust FS WSDL

WSDL Source:

- ☐ File: Choose File No file chosen
- ☒ URL: <http://10.5.1.17/qaservice/qaservice.asmx?WSDL> Browse UDDI
- ☐ WSDL Library: DEFAULT Edit

☐ Automatically load imported files.

Next

- Navigate to the WSDL Policies screen and select a **WSDL policy name** link.
- From the top right section of the screen, click the **Upgrade** button.
- From the WSDL Source section of the screen, select the **URL** radio button.
- In the Username field, enter a **username**.
- In the Password field, enter a **password**, and then click **Browse UDDI**.
- In the UDDI Server URL field, enter the **URL** of a UDDI server. This field may pre-populate with the last URL entered.
- Select the **type of search** to conduct on the UDDI server. This field may pre-populate with the last Search Type entered.
- Select the method by which to search the UDDI server. This field may pre-populate with the last Name entered.
- The remaining fields are optional based on settings.
- Click **Next**.
- The SEARCH UDDI SELECT BUSINESS screen appears with search results which match your criteria. Click the **link** produced to obtain the WSDL.

About UDDI Searches

When searching a UDDI server, you will select a Search Type from the Search Type drop down listing and a Search by criteria. Depending on which **Search Type** is selected, a number of fields will be prefaced by an asterisk (*), and are required to complete the search successfully. Depending on which **Search By** is selected, a number of fields will be prefaced by an asterisk (*), and are required to complete the search successfully.

It is not necessary to fill in every field presented in this dialog.

Enable or Disable Operations on a WSDL Policy

You may disable or enable one or more operations in a WSDL policy. Follow these steps to disable operations on a WSDL policy:

- Navigate to the **WSDL Policies** screen and select a **WSDL policy name** link. The WSDL POLICY screen appears with the Services tab visible.
- A listing of operations appears under the OPERATION tab.
- The status light aligned with each operation displays which operations are currently enabled (green status light).
- Check the checkbox aligned with an **input message** or **output message** and then select **Enable** or **Disable**.

WSDL Same-name Operations Support

The System supports WSDL same-name operations for both DOC-style and RPC-style operations. Within a WSDL port type, the combination of WSDL operation name and Input Message name is used to uniquely identify the operation.

The system supports two RPC-style operations with the same name, unless they have the same number of parameters, and the same parameter names but with different parameter types. Examples of supported RPC-same-name operations include:

```
getStockPrice(String symbol)
getStockPrice(String symbol, int quantity)
```

The system also supports DOC-style WSDL operations with the same name, but it does not support DOC-style run-time operations with the same name.

When the system detects a subsequent operation with the same name, it appends a number after the subsequent operation name, as shown in the following graphic. This graphic displays examples of same-name operations as they appear in a WSDL policy, in an Audit log and on the WS Monitoring screen:

WSDL Policy Services Tab

SERVICE	PORT	STATUS	VIRTUAL URI
ServiceName	PortName	●	http://10.5.6.92:8011/qaservice/qaservice.asmx

Service: ServiceName — Port: PortName

OPERATION	STATUS	ACL	INPUT MESSAGE
OperationName	●	[Allow All]	InputMessage
OperationName	●	[Allow All]	InputMessage2

Audit Log Screen

Code	Level	Message
0E80E	I	Update succeeded - operation: Name: /overloadedRpc/WSDL Services/ServiceName/PortName/OperationName(InputMessage2) Description: Enabled: true Remote policy: overloadedRpc-Remote Real path: /qaservice/qaservice.asmx ACL policy: IDF Group: Default Operation Group
0E80E	I	Update succeeded - operation: Name: /overloadedRpc/WSDL Services/ServiceName/PortName/OperationName(InputMessage) Description: Enabled: true Remote policy: overloadedRpc-Remote Real path: /qaservice/qaservice.asmx ACL policy: IDF Group: Default Operation Group

Web Services Monitoring Screen

OPERATION	TRAFFIC	INVOCATIONS	SUCCESSES	FAILURES	LAST INVOCATION
OperationName	0	0	0	0	
OperationName	0	0	0	0	

Web Services Monitoring Details Screen

WEB SERVICES MONITORING > OPERATION DETAIL

OPERATION DETAIL

Policy: overloadedRpc
Service: ServiceName
Port: PortName
Operation: OperationName
Input Msg: InputMessage

WEB SERVICES MONITORING > OPERATION DETAIL

OPERATION DETAIL

Policy: overloadedRpc
Service: ServiceName
Port: PortName
Operation: OperationName
Input Msg: InputMessage2

Figure 1: The System Distinguishes Between Same-name Operations on Various Screens

WSDL Policy Access Control

You may apply access control to a WSDL Policy at the WSDL level, the WSDL operation level, and the WSDL message level.

- Navigate to the **WSDL Policies** screen and select a **WSDL policy name** link.
- Select the **Service name link** under **Port**.
- From the ACL drop down list, select an **Access Control List** to apply to this WSDL Policy.
- You can also set an IP ACL at the WSDL Policy level.

Apply Intrusion Detection and Prevention to a WSDL Policy

Intrusion Detection and Prevention (IDP) Rules define a set of identified criteria used by the system to detect intrusion. You may associate one or more IDP Rules to a WSDL Policy via an IDP Group. A collection of IDP Rules is known as an IDP Group.



- Navigate to the WSDL Policies screen and select a **WSDL policy name** link.
- Select the **IDP Rules** tab.
- From the IDP Group drop down list, select an **IDP Group** (to associate with this WSDL Policy).

Note: Add more IDP Rules beyond those that are part of the IDP Group by selecting **Edit**, and the IDP Group Details screen appears. Check the **checkboxes** prefacing any IDP Rules to add, and select **Save**. For more information about IDP Rules, refer to the *Forum Systems Sentry™ Version 9 IDP Rules Guide*.

Enable WS-ReliableMessaging for a WSDL policy

You may enable WS-ReliableMessaging manually for a WSDL Policy at the WSDL level or the WSDL virtual directory level.

- Navigate to the **WSDL Policies** screen and select a **WSDL policy name** link.
- Select the **Service name link** under **Port**.
- From the Reliable Messaging Policy drop down list, select the **DEFAULT Reliable Messaging Policy**. The DEFAULT WS-RM policy proxies WS-RM messages and headers through Sentry instead of blocking those messages and headers.
- You can also set a Reliable Messaging Policy at the WSDL Policy level.

Note: WS-ReliableMessaging is enabled automatically in Sentry when a WSDL file contains a standard WS-RM Policy assertion. The steps described here allow for enabling WS-RM when the WSDL does not indicate WS-RM.

Virtualized WSDL Policies Examples

Examples for virtualized WSDL policies include:

- Create a WSDL Library.
- Create a Virtualized WSDL Policy.
- Upgrade a WSDL File from the WSDL Library.
- Update Remote Policy on a WSDL Policy.

Create a WSDL Library

Follow these steps to create a WSDL library:

WSDL LIBRARIES > WSDL LIBRARY

WSDL LIBRARY

Library Name: WebServicesLibrary

Library Description: WebServicesLibrary

Save

<input type="checkbox"/> WSDL NAME	WSDL DESCRIPTION	
<input type="checkbox"/> WSDLServiceA	WSDLServiceA	Upgrade WSDL
<input type="checkbox"/> WSDLServiceB	WSDLServiceB	Upgrade WSDL

Remove Add

- Navigate to the **WSDL Libraries** screen.
- Click **New**.
- In the Library Name field, enter a **name** for this WSDL library.
- In the Library Description field, enter a **description** for this WSDL library.
- Click **Create**.
- Click **Add**
- In the WSDL Name field, enter the **name** of a WSDL file to add to this library.
- In the WSDL Description field, enter a **description** for this WSDL file.
- From the WSDL Source area, click the **File** or **URL** radio button.
- Enter a **URL** in the URL field or click **UDDI**.
- In the Username and Password field, enter a **username** and **password** (if required).
- Click **Next**.
- Click **Add** to add a second WSDL policy to this library.
- In the WSDL Name field, enter the **name** of a WSDL file to add to this library (optional).
- In the WSDL Description field, enter a **description** for this WSDL file.
- From the WSDL Source area, click the **File** or **URL** radio button.
- Enter a URL in the URL field or click **UDDI**. This example adds a URL in the URL field.
- In the Username and Password field, enter a **username** and **password**.
- Click **Next**.
- Click **Save**.

Namespace Prefix When Creating a WSDL Policy from a WSDL Library

When a WSDL library is used to create a single WSDL policy, different namespace prefixes may appear in the resulting WSDL and schema than in the original WSDL files, and namespace declarations may be relocated. These namespace prefix and declaration changes may occur even when only a single WSDL file from the WSDL library is used. The resulting WSDL file is canonically equivalent to the original, but not syntactically identical. These changes should have no effect on client applications which consume the resulting WSDL.

Create a Virtualized WSDL Policy

Follow these steps to create a WSDL policy from the WSDL Library and select WSDL operations from a WSDL library to create a virtualized WSDL policy:

WSDL POLICIES > NEW WSDL POLICY

NEW WSDL POLICY

Name*:

WSDL Source: ☐ File

☐ URL

☐ WSDL Library

☐ Automatically load imported files.

WSDL POLICIES > NEW WSDL POLICY

NEW WSDL POLICY

Name: VirtualWSDL_A

WSDL Library: QA_WSLD_Library

SELECT OPERATIONS FOR WSDL POLICY

☒ qaservice

☒ QAServices

☒ QAServicesSoap

- ☒ BuildElementXML
- ☒ BuildNestedXML
- ☒ BuildSizeXML
- ☒ BuildValidateFailXML
- ☒ Echo
- ☒ SevrallInputs

WSDL POLICIES > NEW WSDL POLICY

NEW WSDL POLICY

Name:	VirtualWSDL_A
WSDL Library:	QA_WSLD_Library
WSDL Namespace*:	<input checked="" type="radio"/> Reuse namespace: <input type="text" value="http://qa.forumsys.com/ws"/> ▼ <input type="radio"/> New namespace: <input type="text"/>
WSDL Definition Name:	<input type="text"/>
WSDL Service Name*:	<input type="text" value="QAServices"/>
WSDL Port Name*:	<input type="text" value="QAServicesSoap"/>
WSDL Binding Name*:	<input type="text" value="QAServicesSoap"/>
WSDL PortType Name*:	<input type="text" value="QAServicesSoap"/>

Next 

WSDL POLICIES > NEW WSDL POLICY

SET LISTENER POLICY

Please specify a listener policy for service: QAServices, port: QAServicesSoap

- ☐ Select from existing listener policies

HttpListenerPolicy-1 (0.0.0.0:80) [Edit](#)

- ☒ Create a new HTTP listener policy

Listener Policy Name*: VirtualWSDL_A-Listener

Use Device IP: ☐

Listener IP*: 192.168.1.144

Listener Port*: 8039

SET VIRTUAL DIRECTORY PATH

Virtual Directory Path: /qaservice/qaservice.asmx

SET REMOTE POLICIES

- ☒ Send to remote server

Please specify a remote network policy for the URL: http://169.254.84.66:80/qaservice/qaservice.asmx

- ☐ Select from existing remote policies

D00-T00_CMN_Authenticate_9999_iFS_Remote (iFSGW-vip:9999) [Edit](#)

- ☒ Create a new HTTP remote policy for this remote server

Remote Policy Name*: VirtualWSDL_A-Remote

Remote Policy Host*: 169.254.84.66

Remote Policy Port*: 80

[Next](#)

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: VirtualWSDL_A

[Upgrade](#)[Export WSDL](#)[Publish WSDL](#)[WSI Validation](#)[Services](#)[Task Lists](#)[Settings](#)[IDP Rules](#)[Logging](#)[Documents](#)

<input type="checkbox"/>	SERVICE	PORT	STATUS	VIRTUAL URI	PHY
<input type="checkbox"/>	QAServices	QAServicesSoap		http://192.168.1.144:8039/qaservice/qaservice.asmx	http:

[Enable](#)[Disable](#)

Service: QA Services — Port: QA ServicesSoap

<input type="checkbox"/>	OPERATION	STATUS	ACL	INPUT MESSAGE	OUTPUT MESSAGE
<input type="checkbox"/>	BuildElementXML		[Allow All]	BuildElementXMLSoapIn	BuildElementXMLSoapOut
<input type="checkbox"/>	BuildNestedXML		[Allow All]	BuildNestedXMLSoapIn	BuildNestedXMLSoapOut
<input type="checkbox"/>	BuildSizeXML		[Allow All]	BuildSizeXMLSoapIn	BuildSizeXMLSoapOut
<input type="checkbox"/>	BuildValidateFailXML		[Allow All]	BuildValidateFailXMLSoapIn	BuildValidateFailXMLSoapOut
<input type="checkbox"/>	Echo		[Allow All]	EchoSoapIn	EchoSoapOut
<input type="checkbox"/>	SeverallInputs		[Allow All]	SeverallInputsSoapIn	SeverallInputsSoapOut

[Enable](#)[Disable](#)

- Navigate to the **WSDL Policies** screen. Click **New**.
- In the Name field, enter a **Name** for this WSDL policy.
- In the Description field, enter a **Description** for this WSDL policy.
- From the WSDL Source section, select the **WSDL Library** radio button.
- From the WSDL Library drop down list, select the name of a WSDL Library. Click **Next**.
- The WSDL Namespace section is used to assign a namespace to the new WSDL. From the WSDL Namespace section, either:
 - select the **Reuse namespace** radio button, and then from the drop down list, select a namespace.
 - or select the **New namespace** radio button, and in the text field, enter the **namespace**.
- The SELECT OPERATIONS FOR WSDL POLICY section allows selection of operations across WSDLs in the WSDL Library policy. Check the **checkbox** for each operation to include.
- Click **Next**.
- Enter **values** for Definition, Service, Port, Binding and Port Type.
- The SET LISTENER POLICY section allows the creation of a new server listener policy, or allows reusing an already defined policy. Select either:
 - the **Select from existing matching listener policies** radio button, and then from the drop down list, select an existing **policy**.
 - or the **Create a new HTTP listener policy** radio button,, and then in the Listener IP field, enter an **IP** for the listener, and in the Listener Port field, enter a **port** for this listener.
- In the SET VIRTUAL DIRECTORY PATH section, enter the **Virtual URI** for this WSDL.
- The SET REMOTE POLICIES section allows the creation of a new remote server policy, or the reusing of an already defined policy. Select either:
 - the **Select from existing matching remote policies** radio button, and from the drop down list, select an existing **Remote server policy**.
 - or the **Create a new HTTP remote policy for this remote server** radio button, and in the Remote Policy Name field, enter a **name**, **IP** and **Port** for the new Remote policy.
- Click **Next**.

Upgrade a WSDL File from the WSDL Library

Follow these steps to upgrade a WSDL file from the WSDL library:



- Navigate to the **WSDL POLICIES** screen, and click a **WSDL Policy name** link.
- Click **Upgrade**.
- From the WSDL Source area, select the **WSDL Library** radio button. In the drop down list, select the name of the **WSDL Library** that holds the WSDL file to be upgraded, and then click **Next**.
- From the SELECT OPERATIONS FOR WSDL POLICY section, expand nodes and check each **service** and **operation** to be upgraded. Click **Next**.
- From the WSDL Namespace area, provide the **namespace value**.
- Enter **values** for Definition, Service, Port, Binding and Port Type.
- Click **Next**.

Update Remote Policy on a WSDL Policy

Follow these steps to update the Remote policy on a WSDL Policy.

REMOTE SETTINGS

☒ Send to remote server
☒ Show all remote policies

Remote Policy: VirtualWSDL_A-Remote Edit for URI http://169.254.84.66:80/qaservice/qaservice.asmx

Remote Path: /qaservice/qaservice.asmx

Physical URI: http://169.254.84.66:80/qaservice/qaservice.asmx\$0

Process Response: Off

Apply Save

Services Task Lists Settings IDP Rules Logging Documents

<input type="checkbox"/>	SERVICE	PORT	STATUS	VIRTUAL URI	PHYSICAL URI	
<input type="checkbox"/>	QAServices	QAServicesSoap	●	http://192.168.1.144:8039/qaservice/qaservice.asmx	http://169.254.84.66:80/qaservice/q	Enable Disable

- Navigate to the **WSDL Policies** screen and click a **WSDL policy name** link.
- Click on the **element** under PORT and the VIRTUAL DIRECTORY screen appears.
- From the Remote Policy drop down list, select a **Remote Policy** link. The physical URI display will show the results of the selected endpoint path.
- Click **Save**.

SERVICES FOR WSDL POLICIES

The Services tab displays a summary of all the services contained in this WSDL policy, as well as the URI and various network settings used to access the service. Clicking on the **Service name** link listed under PORT reveals the Virtual Directory settings for this WSDL policy. Virtual directories are used as a proxy that maps a virtual URI (local) to the physical path and URI (remote, as defined in the WSDL document).

Virtual Directories

A Virtual Directory is a pattern which matches an incoming HTTP request URI. A Virtual Directory is defined on the port node in a WSDL policy. A WSDL policy may have more than one Virtual Directory, often with one being SOAP 1.1 and a second for SOAP 1.2.

Because the physical endpoint defined in the WSDL policy is static, virtual directories can be used to:

- Group different users according to their individual access control.
- Expose a different URI than the actual physical back end server URI (URI cloaking).

Services Tab Terms

The following table describes each term and definition for the Services tab in WSDL policies.

TERM	DEFINITION
SERVICES	
Service	The top level service that is provided by the actual web service.
Port	Where the virtual directory mappings are performed for the WSDL services.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Yellow status light = a required functional element of this policy is disabled.• Red status light = disabled policy.
Virtual URI	The Unique Resource Indicator (URI) path to the location of the local web service policy
Physical URI	Actual URI and server location of the physical web service server.
SERVICE	
Operation	The methods or operations provided by the web service.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Yellow status light = a required functional element of this policy is disabled.• Red status light = disabled policy.
ACL	The Access Control List associated with the provided operation.
Input Message	The SOAP request of the provided operation.
Output Message	The SOAP response of the provided operation.
IDP Group	The IDP Group associated with this service.

How Inbound and Outbound Messages Map to a Virtual Directory

The following graphic displays how inbound and outbound messages map to a Virtual Directory:

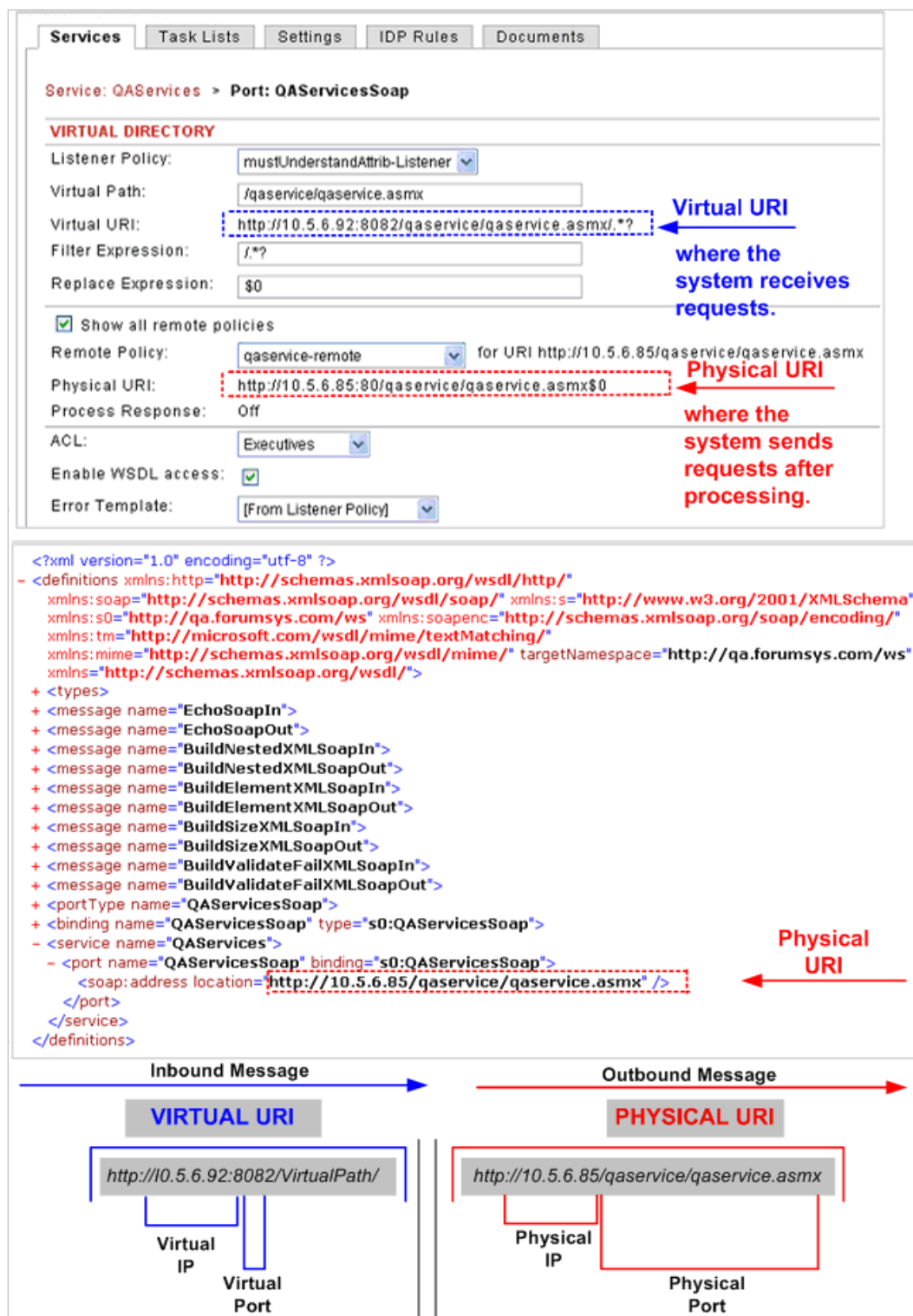


Figure 2: How Inbound and Outbound Messages Map to Virtual Directories.

Relationship Between HTTP Network Policies and WSDL Policies

While creating a WSDL policy, the system detects if there are any existing HTTP Listener and HTTP Remote policies whose IP:Port matches the physical URI defined on the WSDL. The system guides you to create or associate a Listener and Remote policy and assigns the matching IP:Port of the WSDL file to the Remote policy.

Default Filter Expression in a Virtual Directory

When a client request is received on a Virtual Directory at run time, the path of the client request URI consists of the Virtual Path followed by a trailing portion. The Filter Expression is an extended regular expression which the trailing portion must match before the request is accepted for processing.

To review the syntax of the Filter Expression follows Java's regular expression rules; refer to documentation at

<http://java.sun.com/j2se/1.5.0/docs/api/java/util/regex/Pattern.html>.

Note: The default Filter Expression `"/?"` is more restrictive than in some previous versions of the product. If you need to allow subdirectories or URI parameters (a query string), you can change the filter expression to the all-inclusive `".*"`.

Replace Expression in a Virtual Directory

When a client request starts with the virtual path and the trailing portion matches the Filter Expression, the trailing portion is replaced by the Replace Expression and appended to the physical URI (WSDL policies) or Remote URI (XML policies) when connecting to the remote server. In the Replace Expression, `$0` represents the entire trailing portion of the request URI. `$1` represents the portion of the request URL matched by the first set of `()` in the Filter Expression (first capture group), `$2` represents the portion matched by the second set of `()`, up through `$9`. See the example below.

The default Replace Expression `'$0'` means that the system will preserve the trailing portion of the client request URI in the remote request URI. The Replace Expression can be left empty to indicate that the Remote URI should not include the trailing portion at all.

Client requests are mapped to a virtual directory at run-time as follows:

1. The path of the client request URI is compared with the virtual path of each enabled Virtual Directory configured for the Listener policy the request was received on.
2. If more than one Virtual Directory matches, the most specific match is selected. For example, if Virtual Directories `'one'` and `'one/two'` are configured, a request for `'one/two/three'` will be processed by the Virtual Directory with path `'one/two'`, while a request for `'one/four'` will be processed by the Virtual Directory with path `'one'`. If the Virtual Directory with path `'one/two'` is subsequently disabled, both requests will now be processed by the Virtual Directory with path `'one'`.
3. If no Virtual Directories match the request URI, the request is rejected with an error message stating that the requested Virtual Directory is not found.
4. Once a Virtual Directory is selected, the trailing portion of the request URI is matched against the Filter Expression. If the match fails, the request is rejected with an error message stating that the path match has failed. Other, less-specific Virtual Directories found in step 2 are **not** used in this case.

Example:

WSDL port Virtual Directory is configured with:

```
[ HTTP Listener policy IP: 10.1.0.1, port: 80 ]  
Virtual Path: /virtual/service  
Filter Expression: \?id=(u[0-9]{2})&food=([a-z]+)  
Replace Expression: /fruit/$2;user=$1  
[ Remote Path from WSDL: /remote ]  
[ Physical URI: http://10.0.0.3/remote/fruit/$2;user=$1 ]
```

A client request comes in for the URL <http://10.1.0.1/virtual/service?id=u21&food=apple>.

The trailing portion is '?id=u21&food=apple' which matches the Filter Expression. In the Filter Expression, the first capturing group is '(u[0-9]{2})' which matches 'u21' from the request URL, and the second capturing group is '([a-z]+)' which matches 'apple' from the request URL.

Therefore, the request is proxied to a remote server using the Physical URI;
<http://10.0.0.3/remote/fruit/apple;user=u21>.

Task List Groups on WSDL Operations

Task List Groups on WSDL operations provide a means of applying various settings to a WSDL operation.

Note: Tasks are generated in Task Lists. Task Lists are then added to a Task List Group, and later consumed in WSDL policies. For full documentation that the product provides on Tasks, Task Lists and Task List Groups, refer to the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.

WSDL Schema Tightening

The Services tab in a WSDL policy provides a method for modifying the WSDL schema constraints attached to a WSDL policy. To constrain a schema for incoming or outgoing messages, select an Input Message or Output Message link respectively.

COMPLEX TYPES are displayed in their fully expanded form, including contained SIMPLE TYPES. The contained SIMPLE TYPES are displayed with their editable FACETS.

WSDL Schema Tightening, available in the system, adheres to the W3C XML Schema Requirements.

From <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/> you may view details of the XML Schema Data Types standard.

WSDL Schema Constraints Terms

When working with the WSDL schema constraints, consider the following terms and their definitions:

TERM OR FACET	DEFINITION
pattern	pattern is a constraint on the value space of a datatype which is achieved by constraining the lexical space to literals which match a specific pattern. The value of pattern must be a regular expression. Note: In order to modify the pattern facet in the WebAdmin UI, the user must fully erase what is in the pattern text box (if anything) before entering the value desired. The user must neither append text to existing text, nor partially delete the text in the pattern text box. In all cases, the user must fully erase the contents of the text box in the WebAdmin UI before entering the regular expression desired.
minInclusive	minInclusive is the inclusive lower bound of the value space for a datatype with the ordered property. The value of minInclusive must be in the value space of the base type.
minExclusive	minExclusive is the exclusive lower bound of the value space for a datatype with the ordered property. The value of minExclusive must be in the value space of the base type.
maxInclusive	maxInclusive is the inclusive upper bound of the value space for a datatype with the ordered property. The value of maxInclusive must be in the value space of the base type.
maxExclusive	maxExclusive is the exclusive upper bound of the value space for a datatype with the ordered property. The value of maxExclusive must be in the value space of the base type.
totalDigits	totalDigits is the maximum number of digits in values of datatypes derived from decimal. The value of totalDigits must be a positive integer.
fractionDigits	fractionDigits is the maximum number of digits in the fractional part of values of datatypes derived from decimal. The value of fractionDigits must be a non-negative integer.
length	length is the number of units of length, where units of length varies depending on the type that is being derived from. The value of length must be a non-negative integer.

Note: Each schema presents a unique mix of constraint terms or facets and your WSDL policy may not include all of the terms listed above. The facets displayed in the EDIT SCHEMA RULES screen depends on the datatype selected.

Virtual Directories Examples

Examples for Virtual Directories in a WSDL policy include:

- Configure a Virtual Directory.
- WSDL Port Level Access Control.
- WSDL Policy Dynamic WSDL Retrieval.
- Reconfigure a Virtual Directory.
- Edit the Filter Expression.
- WSDL Operation Level Access Control.
- WSDL Fault Policy Settings.
- Override WSDL Endpoint Location on Export.
- Edit WSDL Schema Constraints.
- Override WSDL Validation Settings on WSDL Operations.

WSDL Virtual Directory Settings

A Virtual Directory includes:

- Listener Policy and URI Settings.
- WSDL Access Control.
- Remote Policy and URI Settings.

From the WebAdmin, configure a Virtual Directory and associate an existing Network policy to this Virtual Directory:

Configure a Virtual Directory

VIRTUAL DIRECTORY

Virtual URI:

Physical URI:

WSDL SETTINGS

Enable WSDL access: ☒

☐ Publish a different location in exported WSDL

Published Protocol:

Published Host:

Published Port:

VIRTUAL URI SETTINGS

Listener Policy: [Edit](#)

Request Filter Policy: [Edit](#)

Virtual Host:

☐ Use virtual host as a regular expression

Virtual Path:

☐ Enable Virtual Path Case Insensitivity

Filter Expression:

Replace Expression:

Error Template: [Edit](#)

ACCESS CONTROL

IP ACL Policy: [Edit](#)

ACL Policy:

XACML Policy:

Password Authentication:

Redirect Policy:

REMOTE SETTINGS

☒ Send to remote server

☐ Show all remote policies

Remote Policy: [Edit](#)

Remote Path:

Physical URI:

Process Response:

- Navigate to the WSDL Policies screen and click a **WSDL policy name** link.
- Click on the **link** under PORT. The VIRTUAL DIRECTORY screen appears.
- From the Listener Policy drop down list, select a **Listener Policy**.

WSDL Port Level Access Control

- From the ACL drop down list, select an **ACL** to apply to this Virtual Directory.
- Skip the Enable WSDL access checkbox.
- Click **Save**.

Note: For more information on Access Control Lists or the Allow All ACL, refer to the *Forum Systems Sentry™ Version 9 Access Control Guide*.

Enable or Disable a Virtual Directory

- Navigate to the WSDL Policies screen and click a **WSDL policy name** link.
- Check the **checkbox** prefaced by the element under SERVICE.
- Click **Disable**.
- The Services tab refreshes, and displays the red status light for this Virtual Directory (disabled).

WSDL Policy Dynamic WSDL Retrieval with Enable WSDL Access

- Navigate to the WSDL Policies screen and click a **WSDL policy name** link.
- Click on the **element** under PORT.
- From the ACL drop down list, select an **Access Control List** policy name.
- Check the **Enable WSDL access** checkbox, and then click **Save**.

View or Reconfigure a Virtual Directory

From the WebAdmin, the elements that may be changed on a Virtual Directory are:

- enable / disable the Virtual Directory.
- add, edit or associate another Listener and/or Remote policy to the Virtual Directory.
- edit the virtual path for the Virtual Directory.
- edit the Filter Expression used.
- change the Replace Expression used.
- associate an ACL to the Virtual Directory.
- Configure a WSDL policy to use the Listener policy's Error Template or another Error Template.
- view the Process Response setting that is on the Remote Policy associated with the WSDL policy.
- propagate the WSDL project to other users via the Enable WSDL access option.
- export the WSDL to a different Publication IP/port.
- enable WS-ReliableMessaging

Reconfigure a Virtual Directory

Follow these steps to reconfigure a Virtual Directory and populate with new settings. This instruction also displays editing the Filter Expression used.

Note: If Administrators need to allow arbitrary sub-directories or URL parameters, the Filter Expression can be changed from the current default “/?” to “/.*?”.

Edit the Filter Expression

VIRTUAL URI SETTINGS

Listener Policy:	VirtualWSDL_A-Listener ▼	Edit
Request Filter Policy:	Request_Filter_Policy-14 ▼	Edit
Virtual Host:	<input type="text"/>	
	<input type="checkbox"/> Use virtual host as a regular expression	
Virtual Path:	<input type="text" value="/qaservice/qaservice.asmx"/>	
	<input type="checkbox"/> Enable Virtual Path Case Insensitivity	
Filter Expression:	<input type="text" value="(/.*)?"/>	
Replace Expression:	<input type="text" value="\$0"/>	
Error Template:	SOAP 1.1 Fault Template ▼	Edit

- Navigate to the WSDL Policies screen and click a **WSDL policy name** link.
- Click on the **element** under PORT. The VIRTUAL DIRECTORY screen appears.

Note: The Virtual URI is a read-only field because the system determines this value from the Server policy, virtual path, Filter and Replace Expression settings. The Physical Path may be edited to a different remote policy.

- Edit the Filter Expression from the current default “/?” to “/.*?”.
- From the ACL drop down list, select an **ACL** to associate with this Virtual Directory.
- Click **Save** and the WSDL POLICY screen refreshes.

Note: The WSDL service is not active until the configured Virtual Directory is saved and enabled. For more information on Access Control Lists, refer to an earlier section entitled WSDL Policy Access Control.

WSDL Operation Level Access Control

Access control can be performed at the operation message level as follows:

Service: QAServices > Port: QAServicesSoap > Operation: BuildElen

OPERATION SETTINGS

ACL:	Developers ▼
------	--------------

- Navigate to the **WSDL Policies** screen.
- Click a **WSDL Policy name** link.
- Select the **Services** tab.
- From the OPERATION section, select an **operation name** link.
- From the ACL drop down list, select an **ACL** to associate with this specified operation.
- Click **Save**.

WSDL Fault Policy Settings

A fault is representation of an error that comes back from a WSDL service which defines the format, structure and content of that message. If the WSDL document defines known faults, these will appear in the WSDL policy similar to operation output messages. Follow these steps to view faults included in a WSDL policy:

OPERATION SETTINGS	
ACL:	[Allow All] ▼
Remote Policy:	VirtualWSDL_A-Remote
Physical URI:	http://169.254.84.66/qaservice
IDP Group:	Default Operation Group ▼ Edit

MESSAGES	
BuildElementXMLSoapIn	
BuildElementXMLSoapOut	

FAULTS	
No items to display	

Service: QAServices > Port: QAServicesSoap > Operation: BuildElementXML > **Input Message**

INPUT MESSAGE SETTINGS	
Message Name: BuildElementXMLSoapIn	
<input checked="" type="checkbox"/> Use WSDL Policy Validation Settings	
<input type="checkbox"/> Validate SOAP envelope	
<input type="checkbox"/> Validate SOAP headers defined in WSDL	
<input checked="" type="checkbox"/> Allow additional SOAP headers	
<input type="checkbox"/> Validate SOAP body from WSDL schema	
<input type="checkbox"/> Validate message using WSI Basic Profile	

- Navigate to the **WSDL Policies** screen.
- Click a **WSDL Policy name** link.
- Select the **Services** tab.
- Click an **operation** and the OPERATION SETTINGS screen appears, listing any faults under the FAULTS section of the screen.
- Click the **Fault** and the FAULT MESSAGE SETTINGS screen appears.

Override WSDL Endpoint Location on Export

The Virtual Directory screen provides a method of exporting a WSDL file and overriding the values for the Name/IP and Port of the service. This would be useful when distributing a WSDL service to a location outside a NAT firewall where different IP/Port or a different DNS server is used to resolve the IP of the WSDL Policy URI.

WSDL SETTINGS	
Enable WSDL access:	<input type="checkbox"/>
<input checked="" type="checkbox"/> Publish a different location in exported WSDL	
Published Protocol:	http ▼
Published Host*:	10.5.1.110
Published Port*:	8039

- Navigate to the **WSDL Policies** screen and click a **WSDL policy name** link.
- Click on the element under PORT.
- Check the **Publish a different location in exported WSDL** checkbox.
- Enter an **IP address** in the Publishes host field.
- Enter a **Port number** in the Published port field, and then click **Save**.

Edit WSDL Schema Constraints

Before starting this instruction, review the terms listed in the WSDL Schema Constraints Terms section. Follow these steps to edit WSDL schema constraints:

EDIT SCHEMA RULES

- **BuildElementXML**
 - **NumElements**
 - pattern

minInclusive

minExclusive

maxInclusive

maxExclusive

totalDigits

- Navigate to the **WSDL Policies** screen.
- Click a **WSDL Policy name** link.
- On the SERVICES tab, which lists all operations along with their input and output messages, click to select an **INPUT MESSAGE** or **OUTPUT MESSAGE** link.
- Uncheck the **Use WSDL Policy Validation Settings** checkbox.
- Check the **Validate SOAP body from WSDL schema** checkbox.
- Click **Save**.
- On the refreshed screen, select **Tighten Schema**.
- On the EDIT SCHEMA RULES screen, facet settings appear based on the XSD type of the element SOAP. Enter the **values** for constraining the schema elements in the fields provided.

Note: Valid setting can be referenced from the XSD DataType Part II Specification, Section List datatypes 2.5.1.2 at <http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/#datatype-dichotomies>.

- Click **Save**.

Override WSDL Validation Settings on WSDL Operations

The Use WSDL Policy Validation Settings checkbox on the WSDL Operation Message Details screen is a toggle which enables/disables the use of global validation settings for the selected WSDL message. To use local settings for the WSDL operation message, uncheck the **Use WSDL Policy Validation Settings** option on the input message of the WSDL policy and configure settings as needed.

Leaving the **Use WSDL Policy Validation Settings** option checked will default to the global settings on the WSDL policy Settings tab. Follow these steps to override validation settings on a WSDL message:

INPUT MESSAGE SETTINGS

Message Name: BuildElementXMLSoapIn

☐ Use WSDL Policy Validation Settings

- ☐ Validate SOAP envelope
- ☐ Validate SOAP headers defined in WSDL
- ☒ Allow additional SOAP headers
- ☐ Validate SOAP body from WSDL schema
- ☐ Validate message using WSI Basic Profile

Task List Group:

Task List Groups

[Create](#) [Create With Document](#) [Tighten Schema](#) [Save](#)

- Navigate to the **WSDL Policies** screen.
- Click a **WSDL Policy name** link. The WSDL POLICY screen appears with the SERVICES tab visible.
- Select an **INPUT MESSAGE** link.
- Uncheck the **Use WSDL Policy Validation Settings** checkbox.
- Configure message settings as needed.

Request Filters for WSDL Policies

HTTP requests contain a content-type header field that describes the data contained in the body of the message by means of an Internet media type (content type/subtype). Internet content types are also referred to simply as content types or as MIME types when used as part of a Multimedia Internet Message Extensions (MIME) email message. A Request Filter allows the system to select those HTTP requests that match selection criteria based on the HTTP headers and decode the request appropriately. Most request filters will only need to examine the content-type header, but any header may be used. Requests not matching the defined Request Filter policy will not be processed.

Note: Request filters are auto-generated based on WSDL bindings on the system. When all Request Filters on a WSDL are disabled, the status of the WSDL policy will also be disabled (yellow status light).

Request Filter Terms

The following table displays terms and description of elements of the Request Filter Properties screen:

TERM	DEFINITION
Name	The name given to the Request Filter.
Format	The following formats are available for Request Filters: <ul style="list-style-type: none">• Simple• Web Form• Multipart• DIME (Direct Internet Message Encapsulation)• Web Form Data• Streaming• REST• MTOM
Description	A description for the Request Filter.
Identification Expression	An expression using “request filter” syntax, used to match HTTP request to process with this filter.
Parameter	For “Web Form” request filters, the HTML form name parameter contains the data to process.
Convert Content-encoding	<ul style="list-style-type: none">• The No conversion option means that whatever compression (i.e. HTTP Transfer-encoding) was received from the client (compress, gzip, deflate, or none) will be retained and used for forwarding the XML message to the back end server.• The identity (uncompressed) option means that any compression used by the originating client will be removed before forwarding the uncompressed XML message to the back end server.• The gzip option means that whatever compression was received from the client (compress, gzip, deflate, or none) will be replaced with gzip compression before forwarding the XML message to the back end server.• The deflate option means that whatever compression was received from the client (compress, gzip, deflate, or none) will be replaced with deflate compression before forwarding the XML message to the back end server.

Default Local Request Filters with WSDL Policies

The default Request Filter that come pre-configured with WSDL policies may depend on the version of SOAP and the bindings in the WSDL. The most common to see by default after loading a WSDL are listed below.

DEFAULT REQUEST FILTER NAME	FORMAT	CONTENT TYPES SUPPORTED ON THE SYSTEM
SOAP 1.1 Filter	Simple	<ul style="list-style-type: none">• text/xml• application/xml
SOAP 1.2 Filter	Simple	<ul style="list-style-type: none">• text/xml• application/soap+xml
MTOM Filter	MTOM	<ul style="list-style-type: none">• multipart/related• application/xop+xml

TASK LISTS AND TASK LIST GROUPS FOR WSDL POLICIES

The Task List tab allows users to view all Tasks and Task Lists associated with a WSDL operation policy through Task List Groups.

Relationship Between Task List Groups and Elements of a WSDL Policy

The following graphic displays which elements of a WSDL policy can be associated with a Task List Group:

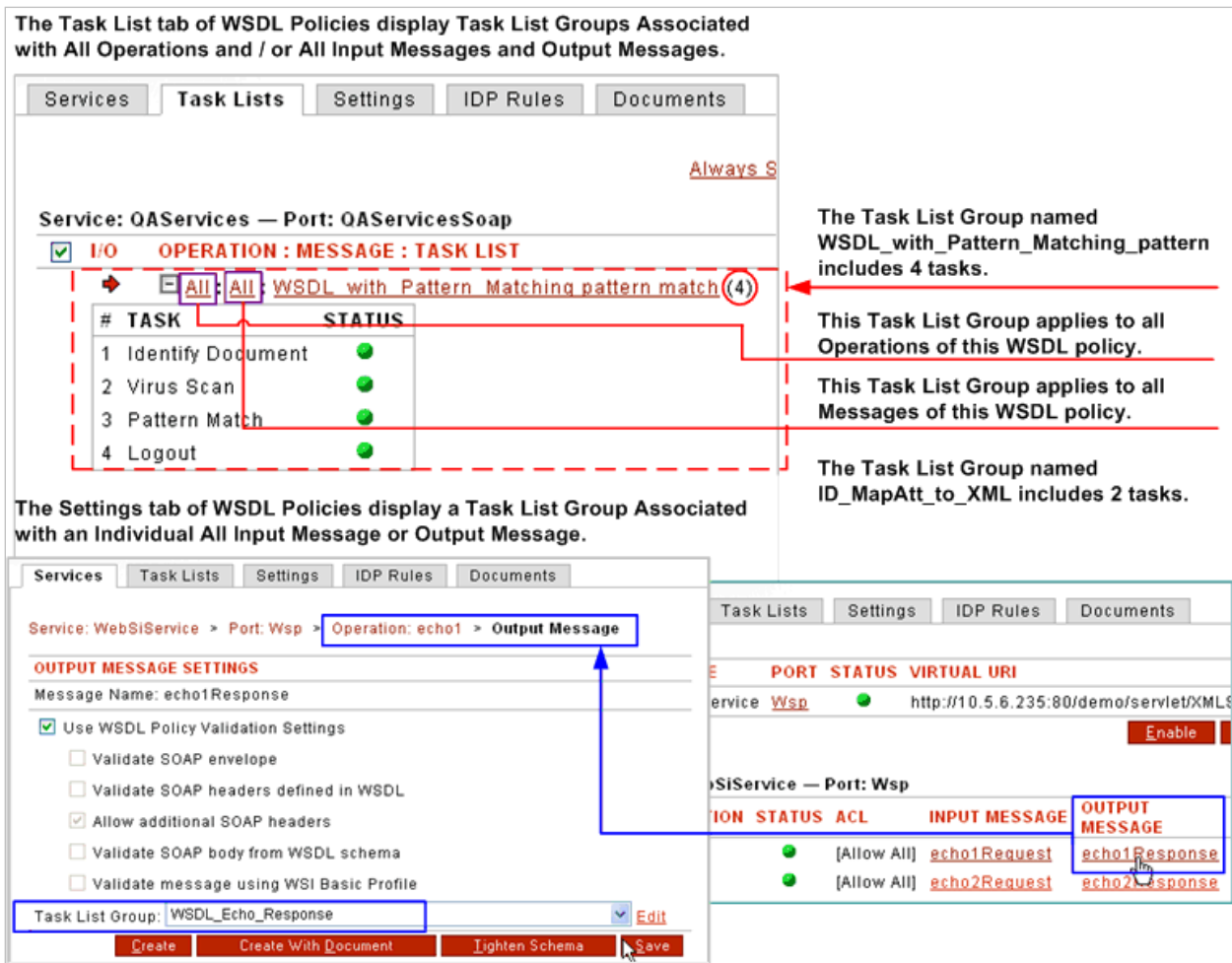


Figure 3: Relationship Between Task List Groups and Elements of a WSDL Policy.

Note: The Disassociate button also allows users of legacy systems to disassociate pre-existing Task Lists, associate these to new Task List Groups and re-apply them to WSDL policies.

Global Task List Groups For All WSDL Operations

Task List Groups can be set at the WSDL Policy level and the WSDL Operation Level. When set at the WSDL Policy level, these are considered global task list groups for all operations of the WSDL policy.

Task List Groups that will be set for all WSDL Operations are set on the **Settings** tab, specifically under the **Processing Settings** section.

In addition to setting the Task List Groups for all operations, the administrator can also specify when the Task List Group is run during the processing of the request or response message. There are four different options to choose when the Task List Group is run:

Pre-process requests

Post-process requests

Pre-process responses (Response processing must be enabled)

Post-process responses (Response processing must be enabled)

Note: For full documentation on Tasks, Task Lists and Task Lists Groups, refer to the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.

The screenshot displays the 'WSDL POLICY' configuration page for 'VirtualWSDL_A'. The 'Settings' tab is selected, showing the 'PROCESSING SETTINGS' section. Under 'VALIDATION SETTINGS', several checkboxes are present, with 'Allow additional SOAP headers' checked. The 'PROCESSING SETTINGS' section includes four options for task list groups: 'Pre-process requests', 'Post-process requests', 'Pre-process responses (Response processing must be enabled.)', and 'Post-process responses (Response processing must be enabled.)'. Each option has a 'Task List Groups' dropdown menu, a 'Type or select label' input field, and a '--NO' button.

Setting	Task List Groups	Type or select label	--NO
<input type="checkbox"/> Pre-process requests	Task List Groups	Type or select label	--NO
<input type="checkbox"/> Post-process requests	Task List Groups	Type or select label	--NO
<input type="checkbox"/> Pre-process responses (Response processing must be enabled.)	Task List Groups	Type or select label	--NO
<input type="checkbox"/> Post-process responses (Response processing must be enabled.)	Task List Groups	Type or select label	--NO

Task List Group to Pre-Process Requests

When a Task List Group is specified at the Pre-process requests level, the Task List Group is run before the document enters WSDL validation. If a Task List Group will be modifying the document such that the

WSDL validation will fail, the Task List Group SHOULD NOT be associated at the Pre-process requests level.

Task List Group to Post-Process Requests

When a Task List Group is specified at the Post-process requests level, the Task List Group is run after the document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD be associated at the Pre-process requests level. This will ensure that properly formatted requests will pass WSDL validation before the Task List Group is run and the document is modified.

An example of this is a Task List Group that encrypts a request. If the request is encrypted before WSDL validation, Sentry will not be able to validate the structure of the request and WSDL validation will fail.

Task List Group to Pre-Process Responses

Note: Processing of response messages requires that Response Processing be enabled on the Remote Policy.

When a Task List Group is specified at the Pre-process responses level, the Task List Group is run before the response document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD NOT be associated at the Pre-process responses level.

Task List Group to Post-Process Responses

Note: Processing of response messages requires that Response Processing be enabled on the Remote Policy.

When a Task List Group is specified at the Post-process requests level, the Task List Group is run after the response document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD be associated at the Pre-process requests level. This will ensure that properly formatted requests will pass WSDL validation before the Task List Group is run and the document is modified.

An example of this is a Task List Group that encrypts a response message. If the response is encrypted before WSDL validation, Sentry will not be able to validate the structure of the response and WSDL validation will fail.

Task List Groups can also be set for each Input or Output message at the WSDL policy Operation level. On the WSDL Policy Services Tab, each Operation is listed with both Input and Output Messages.

- Click the appropriate link under either the INPUT MESSAGE or OUTPUT MESSAGE column.

- Select the appropriate Task List Group from the drop-down menu and click Save.

Forum Sentry™ WSDL Policies Guide | 45

SETTINGS FOR WSDL POLICIES

The Settings tab includes a name and description for the WSDL policy, and a variety of SOAP settings for this policy. When validating SOAP documents, you are validating that the SOAP messages are as defined in the WSDL document (see table below).

The Settings Screen Terms

The following table describes each term and definition for the Settings tab in WSDL policies.

TERM	DEFINITION
WSDL POLICY SETTINGS	
Policy Name	The identifier for this WSDL policy.
Policy Description	A description for this WSDL policy.
Protect virtual resource	<p>When checked, the system uses the Sentry Virtual Directory when authenticating and authorizing against the back end server.</p> <p>When unchecked, the system uses the Sentry physical URI when authenticating and authorizing against the back end server.</p>
Enable session cookies	<p>When the Enable session cookies option is checked, Sentry will automatically set a cookie (often the FSSESSION cookie) for authentication and cache it for the duration noted. The cookie can be used in a Single Sign On paradigm.</p> <p>When the Enable session cookies option is unchecked, cookie is set.</p> <ul style="list-style-type: none">• Cookie Parameters include:• Cookie Name• Cookie Path• Cookie Domain• Session Timeout (mins)• Session Idle Timeout (mins)
Enable Persistent Sessions	When the Enable Persistent Sessions option is checked, Sentry will store the cookie information in a database, using the selected Data Source. This allows for persistent sessions across multiple Sentry instances that all use the same database.
WSDL EXPORT SETTINGS	
Include WSS Policy	When checked, the exported WSDL will contain the WSS Policy information defined in the WSDL policy.
SECURITY SETTINGS	
Validate SOAP Envelope	Check to validate the SOAP Envelope defined in the WSDL.
Validate SOAP headers defined in WSDL	Check to validate the SOAP headers defined in the WSDL.

Allow additional SOAP headers	Check to allow requests and responses to have SOAP headers outside the SOAP definitions within the WSDL. This is enabled by default.
Validate SOAP body from WSDL schema	Check to validate the SOAP body against the schema(s) defined in the WSDL. This option is also applicable to WSDL documents that include other WSDL documents, standalone or compound schemas.
Validate message using WS-I Basic Profile	Check to validate the SOAP body complies with WS-I Test Tools for WS-I Basic Profile 1.0. (For more information on WS-I Basic Profile 1.0, review the WS-I Profile Test Assertion Document contained in the WSI test tool package at http://ws-i.org/implementation.aspx .)
PROCESSING SETTINGS	
Pre-process requests	When a Task List Group is specified at the Pre-process requests level, the Task List Group is run before the document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD NOT be associated at the Pre-process requests level.
Post-Process requests	When a Task List Group is specified at the Post-process requests level, the Task List Group is run after the document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD be associated at the Pre-process requests level This will ensure that properly formatted requests will pass WSDL validation before the Task List Group is run and the document is modified.
Pre-Process responses (Response processing must be enabled.)	When a Task List Group is specified at the Pre-process responses level, the Task List Group is run before the response document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD NOT be associated at the Pre-process responses level.
Post-process responses (Response processing must be enabled.)	When a Task List Group is specified at the Post-process requests level, the Task List Group is run after the response document enters WSDL validation. If a Task List Group will be modifying the document such that the WSDL validation will fail, the Task List Group SHOULD be associated at the Pre-process requests level This will ensure that properly formatted requests will pass WSDL validation before the Task List Group is run and the document is modified.
WEB SERVICES RELIABLE MESSAGING	
Reliable Messaging Policy	When reliable messaging is enabled, a Reliable Messaging Policy is selected.

WSI Validation Features and Examples with WSDL Policies

The system also provides validation for WS-I Basic Profile 1.0 Assertion on WSDL policies through the following methods:

- Review the WS-I Basic Profile 1.0 Test Assertion Report for Design-Time Validation.
- Set up WSI Basic Profile 1.0 Test Assertions used during Design-time Validation of WSDL Policies.
- Set up WSI Basic Profile 1.0 Run-Time Validation of SOAP Messages.
- Customize WSI Basic Profile 1.0 Test Assertions used during Run-Time Validation for SOAP Messages.
- Use the Import Wizard to import a WSDL file and validate against WSI Basic Profile 1.0.

Review WSI Basic Profile 1.0 Validation Report

The WSDL Policies screen includes a WSI Validation button that yields a report of passed, failed and not applicable validation tests constructed according to the WS-I Basic Profile 1.0 Test Assertions standard. To help ensure interoperability among clients who will be using the WSDL policy document, WSI validation is provided as a diagnostic tool which can be used during design-time when creating WSDL policies.

WSDL POLICIES > WSDL POLICY

WSDL POLICY

Policy Name: QAService
Policy Description: WSDL service for QA

[Upgrade](#) [Export](#) [WSI Validation](#) [Publish WSDL](#)

WSDL POLICY > WSI VALIDATION REPORT

TEST RESULT

WSI Basic Profile validation succeeded for WSDL Policy QAService: No failures

WSI ASSERTION	RESULT
WSI2110 ArrayOf naming convention not used	Warning

[Show All Results](#)

WSDL POLICY > WSI VALIDATION REPORT

TEST RESULT

WSI Basic Profile validation succeeded for WSDL Policy QAService: No failures

WSI ASSERTION	RESULT
WSI2010 Unique operation names	Passed
WSI2011 Imported schemas are good XML 1.0	N/A
WSI2012 Document literal bindings have element parts	Passed
WSI2013 RPC literal bindings refer to type defined parts	N/A
WSI2014 parameterOrder omits at most one part	N/A
WSI2017 All binding operations are the same valid style	Passed
WSI2018 wsdl:types follows only import and documentation	Passed
WSI2019 Namespace not specified in document literal soap binding children	Passed
WSI2700 wsdl:definitions is good XML 1.0	Passed
WSI2701 Appropriate wsdl:definitions namespace	Passed
WSI2703 Namespaces imply conformance to schemas	Passed

[Show Only Errors](#)

Note: If your business is committed to WS-I Basic Profile 1.0, then this analytical tool will be useful in finding failures for this standard; otherwise, ignore this command and its report.

Each WSI Validation Report is displayed for a WSDL policy. You may review any failures that are generated from these WSI BP tests by selecting any WSDL policy link, and then clicking the WSI VALIDATION button. The WSI VALIDATION REPORT appears.

Reconfigure Validation Tests

You can correct any failures by correcting your WSDL files, reloading them and performing the WSI validation again. The WSI Validation settings can be selectively enabled from the WSDL policy screen by selecting **Settings** from the WSDL screen.

Set Up WSI Assertions for Design-Time Validation

Follow these steps to set up which tests are used for WSI Basic Profile 1.0 validation during design-time:

WSI ASSERTION	ENABLE TEST
WSI2010 Unique operation names	<input checked="" type="checkbox"/>
WSI2011 Imported schemas are good XML 1.0	<input checked="" type="checkbox"/>
WSI2012 Document literal bindings have element parts	<input checked="" type="checkbox"/>
WSI2013 RPC literal bindings refer to type defined parts	<input checked="" type="checkbox"/>
WSI2014 parameterOrder omits at most one part	<input checked="" type="checkbox"/>
WSI2017 All binding operations are the same valid style	<input checked="" type="checkbox"/>
WSI2018 wsdl:types follows only import and documentation	<input checked="" type="checkbox"/>
WSI2019 Namespace not specified in document literal soap binding children	<input checked="" type="checkbox"/>
WSI2020 RPC bindings are literal	<input checked="" type="checkbox"/>
WSI2021 Inputs and outputs use proper part, parts, and schemas	<input checked="" type="checkbox"/>
WSI2022 soapbind:fault has a name	<input checked="" type="checkbox"/>
WSI2032 soapbind:fault name matches parent	<input checked="" type="checkbox"/>
WSI2098 WSDL imports have a location	<input checked="" type="checkbox"/>

Save

- Navigate to the WSDL Policies screen and select **WSI Settings**.

Note: By default, all WSI Assertions tests are enabled. This listing of tests applies to all WSDL policies listed on the WSDL Policies screen. This listing of WSI Assertion tests, used during design-time validation, is for validating the WSDL against the assertions relevant against the WSDL. You are free to disable as many tests as you like. The design-time validation performed is purely informational.

- In the Enable Test column, deselect those **WSI BP Assertions** that you do not want enabled.
- Scroll to the bottom of the screen, and click **Save**.

Set Up WSI Basic Profile Run-Time Validation

Run-time WSI validation is validating SOAP messages' requests and responses against the specified assertions. Follow these steps to enable WS-I SOAP message validation enforcement:

The screenshot shows the 'Settings' tab of the WSDL Policies configuration interface. It includes fields for 'Cookie Path', 'Cookie Domain', 'Session Timeout (mins)' (set to 120), and 'Session Idle Timeout (mins)' (set to 60). There is a checkbox for 'Enable persistent sessions' and a dropdown menu currently set to 'QA_MySQL' with an 'Edit' link. Below these are sections for 'WSDL EXPORT SETTINGS' with an 'Include WSS policy' checkbox, and 'VALIDATION SETTINGS' with checkboxes for 'Validate SOAP envelope', 'Validate SOAP headers defined in WSDL', 'Allow additional SOAP headers' (checked), 'Validate SOAP body from WSDL schema', and 'Validate message using WSI Basic Profile' (unchecked). A 'Configure Tests' link is next to the last checkbox.

- Navigate to the **WSDL Policies** screen and select the **Settings** tab.
- Scroll to the bottom of the screen and check the **Validate messages using WSI Basic Profile** checkbox and then click **Save**.

Checking the **Validate message using WSI Basic Profile** checkbox means SOAP messages accessing this WSDL policy will be tested versus WSI Basic Profile. Failed WSI Validation will result in a SOAP fault message to the client.

Note: Forum Systems recommends that you turn on the SOAP Message validation tests by checking the Validate message using WSI Basic Profile checkbox during testing only due to the impact of WSI validation on throughput performance.

Not checking the **Validate message using WSI Basic Profile** checkbox means that no WSI validation will occur.

Customize WSI Assertions for Run-Time Validation

You may customize WSDL assertions by clicking the **Configure Test** link, and from the listing of WSI Tests, enable/disable assertions. This customization applies to the currently-edited WSDL policy.

This is a close-up of the 'VALIDATION SETTINGS' section from the previous screenshot. It shows the same list of checkboxes: 'Validate SOAP envelope', 'Validate SOAP headers defined in WSDL', 'Allow additional SOAP headers' (checked), 'Validate SOAP body from WSDL schema', and 'Validate message using WSI Basic Profile' (checked). The 'Configure Tests' link is now underlined and highlighted with a mouse cursor. A red 'Save' button is visible at the bottom right of the settings area.

Import and Validate WSDL Documents Wizard

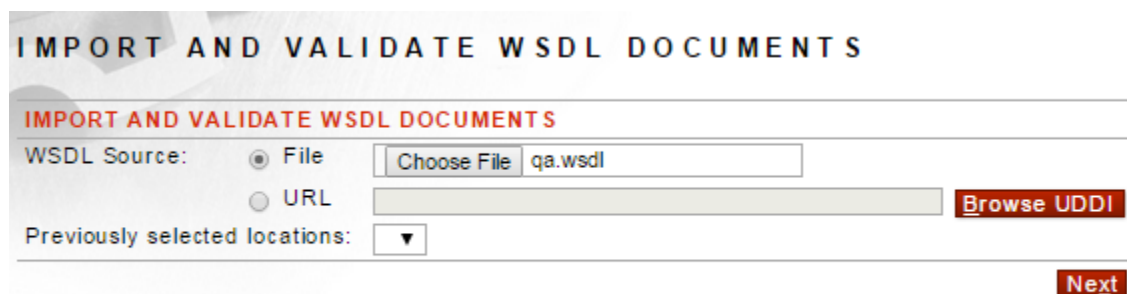
The Import and Validate WSDL Documents Wizard found in the Getting Started screen, provided a means of both importing and validating a WSDL from a file, URL or UDDI search, and then viewing any failures resulting from validation against WSI Basic Profile 1.0.



The wizard allows you to:

- Import a WSDL document from file or URL.
- View the failed or succeeded WSI Basic Profile assertions that were validated.
- Retain or discard a WSDL document in the default WSDL Library.
- Retain or discard a WSDL document the WSDL policy from the WSDL document.

Follow these steps to use the Import and Validate WSDL Documents Wizard:



- From the Navigator, select the **Getting Started** screen.
- Select the **IMPORT AND VALIDATE WSDL DOCUMENTS** option.
- Select the **File** radio button, and click **Browse**.
- The Choose File screen appears. Choose or enter a location for retrieving the WSDL.

Note: The Previously selected locations field is for previous locations and paths.

- The **IMPORT AND VALIDATE WSDL DOCUMENTS** screen refreshes with a notification message about the WSDL failure or success.
- To save the WSDL document, click **Keep**. To remove the WSDL document, click **Discard**.

SOAP XSD Validation Enforcement Examples

The example configuration for validating SOAP Documents in a WSDL policy in the WebAdmin is Validate SOAP Documents.

Validate SOAP Documents

From the WebAdmin, follow these steps to validate SOAP documents in a WSDL policy:

VALIDATION SETTINGS	
Validate SOAP envelope:	<input checked="" type="checkbox"/>
Validate SOAP headers defined in WSDL:	<input checked="" type="checkbox"/>
Allow additional SOAP headers:	<input checked="" type="checkbox"/>
Validate SOAP body from WSDL schema:	<input checked="" type="checkbox"/>
Validate message using WSI Basic Profile:	<input checked="" type="checkbox"/> Configure Tests

- Navigate to the WSDL Policies screen and click a **WSDL policy name** link.
- Select the **Settings** tab.
- Scroll to the bottom of the screen, and check:
 - **Validate SOAP envelope** checkbox to validate the SOAP Envelope defined in the WSDL.
 - **Validate SOAP headers defined in WSDL** checkbox to validate the SOAP headers defined in the WSDL.
 - **Allow additional SOAP headers** checkbox to requests and responses to have SOAP headers outside the SOAP definitions within the WSDL.
 - **Validate SOAP body from WSDL schema** checkbox to validate the SOAP body against the schema(s) defined in the WSDL. This option is also applicable to WSDL documents that include other WSDL documents, standalone or compound schemas.
 - **Validate message using WSI Basic Profile** checkbox to validate the SOAP body complies with WS-I Test Tools for WS-I Basic Profile 1.0. (For more information on WS-I Basic Profile 1.0, review the WS-I Profile Test Assertion Document contained in the WSI test tool package at <http://ws-i.org/implementation.aspx>.)
- Click **Save**.

Access Control with WSDL Policies

User Access Control Lists (ACLs) are created in the USER ACLs screen, and may be applied to WSDLs and Network policies to allow or restrict access based on the Execute privilege. USER ACLs may be applied to a Listener network policy, at the WSDL Policy Virtual Directory level, and/or to an operation on a WSDL policy.

Note: For more information, refer to the USER ACLs section of the *Forum Systems Sentry™ Version 9 Access Control Guide*.

Relationship of ACLs to WSDL and Listener Policies

The following graphic displays the relationship of ACLs to WSDL and Listener policies:

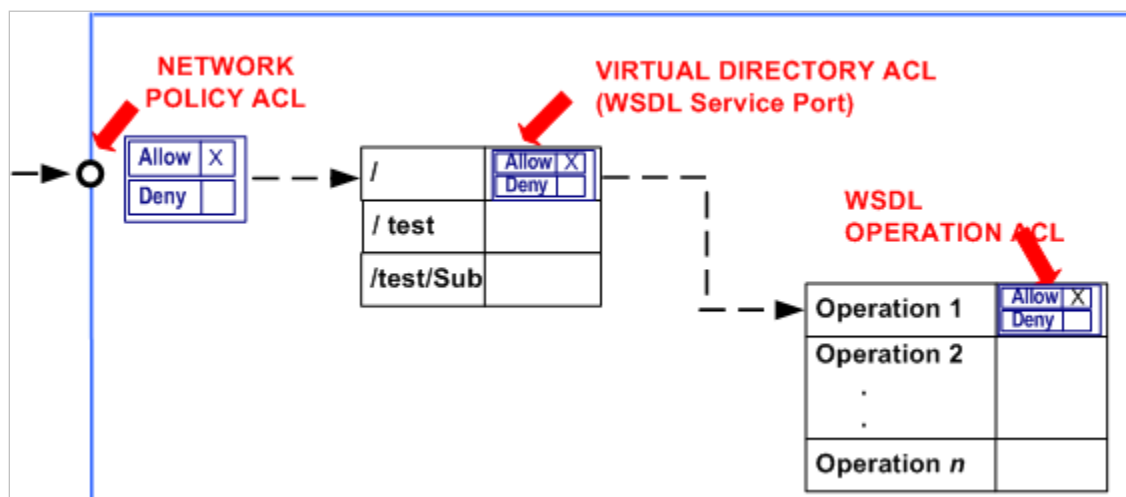


Figure 4: Relationship of USER ACLs to WSDL and Listener Policies.

IDP RULES FOR WSDL POLICIES

Intrusion Detection and Prevention (IDP) Rules define a set of criteria which can be associated with a WSDL policy. IDP Groups represent a reusable collection of IDP Rules that may be applied to this WSDL policy. Under the IDP Group drop down list is a listing of all the IDP Rules included in the selected IDP Group.

Note: For full documentation that the product provides on IDP Rules, refer to the *Forum Systems Sentry™ Version 9 IDP Rules Guide*.

IDP Rules also allow throttling and black listing based on identity, IP and traffic load. IDP Rules can be scheduled based on expected traffic to throttle back transactions or reroute messages.

IDP Rules have actions associated with them that can generate an email alert or invoke a specified web service, triggering any event programmed into the web service.

IDP Rules define a set of identified criteria used by the system to detect intrusion. Once created, IDP Rules may be reused.

IDP Groups can be set at both the WSDL Policy level and at the WSDL Operation level.

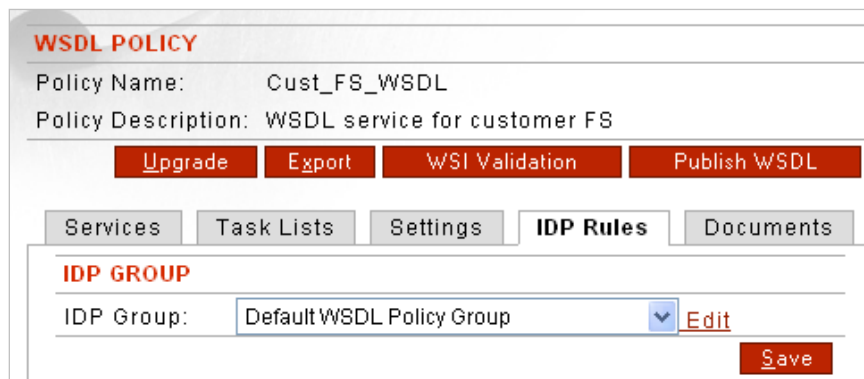
IDP Rules Tab Screen Terms for WSDL Policy

The following table describes each term and definition found on the IDP Rule tab.

TERM	DEFINITION
IDP Group	The identifier for this IDP Group.
IDP Rule	IDP Rules that is included in this IDP Group.
IDP Criterion	Description of the type of IDP Rule.
Threshold	Any constrained value, period or rate applied to the detection settings of the IDP Rule.
User Group	The name of the User group for which the IDP Rule applies.
Enforce By	<ul style="list-style-type: none">• If User, the IDP Rule is enforced on a per User basis. If IP, the IP address that is defined in the detection settings of the IDP Rule.• If IP, the IDP Rule is enforced on a per IP address User basis.
IDP Action	The name of the IDP Action policy applied to the IDP Rule.
IDP Schedule	The name of the IDP Schedule policy applied to the IDP Action.

Edit WSDL IDP Group

To choose a new IDP Group to enforce, select an **IDP Group name** from the drop down list.



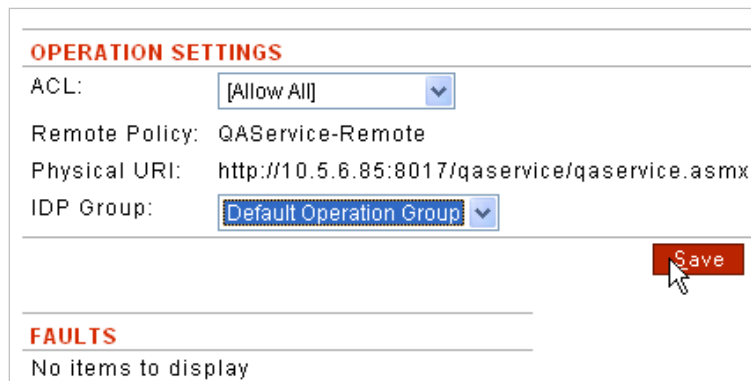
The screenshot shows the 'WSDL POLICY' configuration page. At the top, the 'Policy Name' is 'Cust_FS_WSDL' and the 'Policy Description' is 'WSDL service for customer FS'. Below these are four red buttons: 'Upgrade', 'Export', 'WSI Validation', and 'Publish WSDL'. A row of tabs includes 'Services', 'Task Lists', 'Settings', 'IDP Rules' (which is selected), and 'Documents'. Under the 'IDP Rules' tab, there is a section titled 'IDP GROUP'. It contains a dropdown menu labeled 'IDP Group:' with 'Default WSDL Policy Group' selected. To the right of the dropdown is an 'Edit' link. At the bottom right of this section is a red 'Save' button.

This instruction assumes the IDP Group was created previously. Follow these steps to associate an IDP Group to a WSDL policy:

- From the Navigator, select **WSDL Policies**.
- Click a **WSDL policy name** link.
- Select the **IDP Rules** Tab.
- From the IDP Group drop down list, select an **IDP Group name** to associate to this WSDL, and then click **Save**.

Edit WSDL Operation IDP Group

IDP Groups may also be applied to a WSDL operation by selecting the **Services** tab of a WSDL policy, and then selecting an Operation name link.



The screenshot shows the 'OPERATION SETTINGS' page. It has several fields: 'ACL:' with a dropdown set to '[Allow All]', 'Remote Policy:' set to 'QAService-Remote', and 'Physical URI:' set to 'http://10.5.6.85:8017/qaservice/qaservice.asmx'. The 'IDP Group:' field has a dropdown menu with 'Default Operation Group' selected. A red 'Save' button is located to the right of the IDP Group dropdown. Below the settings section is a section titled 'FAULTS' which displays 'No items to display'.

The Default WSDL Operation Group does not contain any IDP Rules. Administrators may add IDP Rules to this group whenever appropriate.

- From the Navigator, select **WSDL Policies**.
- Click a WSDL policy name **link**.
- Under the OPERATION column, click an **Operation name** link.
- From the IDP Group drop down list, select an **IDP Group name** to associate to this WSDL operation and then click **Save**.

LOGGING SETTINGS FOR WSDL POLICIES

Policy level logging can be set for each WSDL Policy. This allows for logging different policies with different log levels.

Logging Tab Screen Terms for XML Policy

The following table describes each term and definition found on the IDP Rule tab.

TERM	DEFINITION
Enable Policy Level Logging Settings	When checked, policy level logging is enabled for the WSDL Policy.
	When not checked, policy level logging is disabled for the WSDL Policy.
Policy Log Level	When policy level logging is enabled, this is the log level set for this policy.
Always Log the Following Code	When policy level logging is enabled, this is a list of error codes that will always be logged regardless of the log level set for this policy.
Pattern Match Policy	When policy level logging is enabled, and the Always log the following codes option is enabled, a pattern match policy can be used to log messages based on a pattern match policy (regex).

Note: For more information on logging with Sentry, please see the [Forum Sentry v9 Logging Guide](#). For more information on Pattern Match policies, see the [Forum Sentry v9 IDP Rules Guide](#).

DOCUMENTS FOR WSDL POLICIES

The Documents tab displays the WSDL document that this WSDL policy is based upon and any referenced document used to create this WSDL policy.

WSDL PUBLISHING

WSDL policies and virtual WSDL policies may be published in the following ways:

- Dynamic WSDL retrieval (with optional Access Control).
- Publish to UDDI
- Export

Dynamic WSDL Retrieval

A WSDL policy can be enabled to allow users to dynamically retrieve the associated WSDL document by setting the “Enable WSDL access” checkbox on the WSDL port Virtual Directory. Once the checkbox is enabled, the WSDL can be obtained by accessing the Virtual URI shown with “?WSDL”, i.e., <http://<IP>virtualURI?WSDL>.

In the following example, the WSDL document for this policy could be retrieved by using the URI <http://<IP>/qaservice/qaservice/asmx?WSDL>

Service: QAServices > Port: QA Services Soap

VIRTUAL DIRECTORY

Virtual URI:

Physical URI:

WSDL SETTINGS

Enable WSDL access: ☐

☐ Publish a different location in exported WSDL

Published Protocol:

Published Host:

Published Port:

VIRTUAL URI SETTINGS

Listener Policy: [Edit](#)

Request Filter Policy: [Edit](#)

Virtual Host:

☐ Use virtual host as a regular expression

Virtual Path:

☐ Enable Virtual Path Case Insensitivity

Filter Expression:

Replace Expression:

Error Template: [Edit](#)

ACCESS CONTROL

IP ACL Policy: [Edit](#)

ACL Policy:

XACML Policy:

Password Authentication:

Redirect Policy:

REMOTE SETTINGS

☐ Send to remote server

☐ Show all remote policies

Remote Policy:

Remote Path:

Physical URI:

Process Response:

[Apply](#) [Save](#)

Dynamic WSDL retrieval with access control provides credential-based access control to expose only operations within the WSDL document based on ACL membership.

Business Keys

When publishing a WSDL project to a UDDI server, entering a Business Key ensures that one location and one UDDI entry exists for this WSDL project. When publishing a WSDL project to a UDDI server, and leaving the Business Key field blank ensures that multiple locations and multiple UDDI entries will exist for this WSDL project. Deleting a published WSDL using the WebAdmin is not possible. Publishing the same WSDL with the same name twice is not possible.

Publish WSDL Screen Terms

The following table describes each term and definition for the Publish WSDL screen displayed in the Publish a WSDL Policy to UDDI figure.

TERM	DEFINITION
CONFIGURE CONNECTION	
UDDI Server Publish URL*	The URL to publish the WSDL project to. This field must always use the https transport protocol.
Username*	The user credentials to access the UDDI server.
Password	The password for the user accessing the UDDI server.
BUSINESS RELATED INFORMATION	
Business Name*	This field may contain any Business name appropriate for the business entity/client.
Business Description*	This field may contain any Business description appropriate for the business entity/client.
Business Key	Leave the Business Key field blank when initially publishing the WSDL project. Enter the Business UDDI Key name in this field whenever updating the entry in the UDDI.
SERVICE RELATED INFORMATION	
Use WSDL Port URL to access WSDL	When checked, the system uses the WSDL port SOAP address location in the WSDL document for specifying how UDDI users will obtain this WSDL. This option and the Overview Document URL option are mutually exclusive.
ACL Options	<ul style="list-style-type: none"> To publish all operations of the WSDL service, select the Publish all operation radio button. To publish only those operations of the WSDL service that are based on specific ACL(s), select the Publish operations based on ACL(s) radio button, and then select one or more ACLs from the text box.
WSDL Service Name	This field is pre-populated from the WSDL.
Service Name	User-assigned UDDI service name.
Service Description	User-assigned UDDI service description.
Overview Document URL	<p>The address at which the user can expect to find the complete WSDL file for this WSDL project. This field must be a valid URL, i.e.:</p> <p>HTTP(S)://<IP><Port><Context></p> <p>The transport protocol may be http or https, and the Port is optional. This option and the Use WSDL Port URL to access WSDL option are mutually exclusive.</p>
Overview Document Description	This field may contain any user-defined description of the overview document URL.

Publish a WSDL Policy to UDDI

When publishing a WSDL policy, the system provides two options for access control; publishing all the operations in the WSDL or publishing operations based on the ACL of the user in the system. When using specified ACLs, only the operations and schema allowed by the selected ACLs will appear on the exported WSDL document.

To publish a WSDL project to a UDDI server, credentials to access the UDDI server are required. From the WebAdmin, users configure the UDDI connection credentials.

Publish WSDL

WSDL POLICY > PUBLISH WSDL

CONFIGURE CONNECTION

UDDI Server Publish URL*:

Username*:

Password:

BUSINESS RELATED INFORMATION

Business Name*:

Business Description*:

Business Key:

SERVICE RELATED INFORMATION

Use WSDL Port URL to access WSDL: ☒

ACL Options:

☒ Publish all operations

☐ Publish operations based on ACL(s):

WSDL Service Name:

Service Name*:

Service Description:

Overview Document URL:

Overview Document Description:

Next

This operation assumes you have created a WSDL policy and that the service is enabled. Follow these steps to publish a WSDL policy to UDDI:

- Navigate to the **WSDL Policies** screen.
- On the WSDL POLICIES screen, click a **WSDL policy name** link.
- On the WSDL POLICY screen, click the **Publish WSDL** button.

- On the PUBLISH WSDL screen, in the UDDI Server Publish URL field, enter the **URL** to publish the WSDL project to. This field must always use the https transport protocol.
- In the Username field, enter the **username** to access the UDDI server.
- In the Password field, enter the **password** for the user accessing the UDDI server.
- In the Business Name field, enter any **Business name** appropriate for the business entity/client.
- In the Business Description field, enter any **Business description** appropriate for the business entity/client.
- In the Business Key field, enter the **Business UDDI Key** name.
- Check the **Use WSDL Port URL to access WSDL** checkbox to use the WSDL port SOAP address location in the WSDL document.

Note: If checking the **Use WSDL Port URL to access WSDL** checkbox, then the Overview Document URL field, presented later, will be disabled. These options are mutually exclusive for specifying how UDDI users should obtain a WSDL.

- Aligned with ACL Options, decide to select the **Publish all operations** radio button to publish all operations of this WSDL, or select the **Publish operations based on ACL(s)** radio button to publish only those operations that are associated with the selected User ACL.
- The WSDL Service Name field is pre-populated from the WSDL.
- In the Service Name field, enter a user-assigned UDDI service **name**.
- In the Service Description field, enter a user-assigned UDDI service **description**.
- Skip the Overview Document URL field.

Note: If you have not checked the Use WSDL Port URL to access WSDL checkbox, then enter the **address** at which the user can expect to find the complete WSDL file for this WSDL project in the Overview Document URL field. These options are mutually exclusive for specifying how UDDI users should obtain a WSDL. The Overview Document URL field must be a valid URL, i.e.: HTTP(S)://<IP><Port><Context>. The transport protocol may be http or https, and the Port is optional.

- In the Overview Document Description field, enter any user-defined **description** of the overview document URL.
- Click **Next**, and the screen refreshes.

WS-RM (Reliable Messaging) POLICIES

The Settings tab includes a name and description for the WSDL policy, and a variety of SOAP settings for this policy. When validating SOAP documents, you are validating that the SOAP messages are as defined in the WSDL document (see table below).

WS-RM License Feature

The use of WS-RM in Sentry requires a license for the Web Services Reliable Messaging feature. If you do not see this feature listed under your General Info screen available features, please contact support at support@forumsys.com to request this license feature to be added to your existing license key.

Forum Sentry supports the Web Services Reliable Messaging specification (see the WS-ReliableMessaging specification at <http://docs.oasis-open.org/ws-rx/wsrn/200702/wsrn-1.2-spec-os.html> for more details).

Reliable Messaging - WSRM Policies

Selecting the **DEFAULT** WS-RM policy displays the policy settings. The DEFAULT policy is set to the Proxy role. Other settings are not relevant to the Proxy role and are disabled. The Proxy role configures Sentry to proxy WS-RM messages and headers for both requests and responses, thus allowing all variations of WS-RM delivery guarantees to traverse through a Sentry WSDL policy. By default without the WS-RM policy, a Sentry WSDL Policy disallows WS-RM traffic.

TRANSFERRING EXPORTING AND IMPORTING WSDL POLICIES

Users may transfer one or more WSDL policies (and all its dependencies) from one Agent machine to another Agent machine with the **GDM Transfer** command visible on the WSDL Policies screen. This type of transfer is referred to as a GDM partial configuration transfer.

Users may export one or more WSDL policies (and all its dependencies) to a local file system via an FSG file using the **GDM Export** command visible on the WSDL Policies screen. This type of export is referred to as a GDM partial configuration export.

Through the Import / Export screen, users may import WSDL policies with all their dependencies into the product using the **Import** command from the **GDM IMPORT** section of the screen. This type of import is referred to as a GDM partial configuration import.

For information on the following features:

- To transfer a WSDL policy to an Agent Group, refer to the GDM Partial Configuration Transfer section of the *Forum Systems Sentry™ Version 9 System Management Guide*.
- To export a WSDL policy, to a local file system via an FSG file, refer to the GDM Partial Configuration Export section of the *Forum Systems Sentry™ Version 9 System Management Guide*.

WSDL POLICIES

Search

Search Usage: type any text Filter Usage: type or select the label

Always Show Expanded

No Labels

☐

NAME

PORT

STATUS

VIRTUAL URI

IDP GROUP

DATE MODIFIED

☐

qaservice



 QAServicesSoap



http://192.168.1.79/qaservice/qaservice.asmx

 Default WSDL Policy Group (8)

2017/11/01 15:34

WSI Settings

GDM Transfer

GDM Export

Delete

Enable

Disable

Copy

New

- To Import a WSDL policy with all its dependencies to the current machine via an FSG file, refer to the GDM Partial Configuration Import section of the *Forum Systems Sentry™ Version 9 System Management Guide*.

GDM IMPORT	
Password*:	<input type="password"/>
<input checked="" type="radio"/> From file (.fsg)*:	<input type="button" value="Choose File"/> wsd_policy_01.fsg
<input type="radio"/> From database	
Configuration Name:	<input type="text"/> <input type="button" value="Browse"/>
New domain:	<input type="button" value="Do not change"/>
<input type="button" value="Import"/>	

APPENDIX

Appendix A - Constraints in WSDL Policies Guide

ELEMENT	CONSTRAINTS	CHARACTER COUNT
WSDL Policy Names	Unique and case sensitive. Must start with an alpha character. Accepts underscores and dashes.	1-32
Virtual Directory name in WSDL policy	Unique and case sensitive	1-256
WSDL Library name	Unique and case sensitive. Must start with an alpha character. Accepts the "@" character, underscores, and dashes. However, no leading spaces are allowed.	5-32

Appendix B - Specifications in WSDL Policies Guide

ELEMENT SUPPORTED	SPECIFICATIONS
WSDL Policies	Unlimited *
Virtual Directories	Depending on the WSDL, there may be more than one Virtual Directory per WSDL Policy. Most common example is having SOAP 1.1 and SOAP 1.2 Virtual Directories.
Task Lists allowed per WSDL policy	Unlimited * Task Lists are associated to Task List Groups, not directly to XML Policies. Task List Groups can contain multiple Task Lists.
Standards	WSDL 1.1, SOAP 1.1, SOAP 1.2, SwA MIME, SwA DIME, MTOM, WS-Addressing, WS-Policy

* Limited only by disk space.

Appendix C - Virtual Directory Reference Chart in WSDL Policies Guide

Click on the **element** link under Port to view the Virtual Directory and available options.

Services | **Task Lists** | **Settings** | **IDP Rules** | **Documents**

Service: **WebSIService** > Port: **Wsp**

VIRTUAL DIRECTORY

Listener Policy: **mustUnderstandAttrb-Listener**

Virtual Path: **/demo/servlet/XMLSimpleServlet**

Virtual URI: **http://10.5.6.92:80/demo/servlet/XMLSimpleServlet(/.*)?**

Filter Expression: **{/.*}**

Replace Expression: **\$0**

☒ Show all remote policies

Remote Policy: **HoustonRemote** for URI **http://127.0.0.4:8080/demo/servlet/XMLSimpleServlet**

Physical URI: **http://11.11.11.71:8071/demo/servlet/XMLSimpleServlet/\$0**

Process Response: **off** This setting is mirrored from the Remote Policy.

ACL: **Default**

Enable WSDL access: ☐

Error Template: **[From Listener Policy]**

☐ Publish a different location in exported WSDL

Published host*:

Published port*:

Save

#	HTTP REQUEST FILTER	FORMAT	DESCRIPTION	STATUS
1	SOAP 1.1 Filter	Simple	WSDL 1.1 SOAP 1.1 HTTP Filter	

Annotations:

- From the Listener Policy drop down list, select an **HTTP Listener Policy** to associate with this WSDL Policy.
- The Virtual Path field allows users to customize this WSDL's Virtual Path.
- With the **Show all remote policies** checkbox checked, the Remote Policies drop down list displays all Remote Policies on the appliance.
- From the Remote Policies drop down list, select an **HTTP Remote Policy** to associate with this WSDL Policy.
- From the ACLs drop down list, select an **ACL** to associate with this WSDL. The selected ACL grants access of this WSDL Policy to any member of the ACL.
- With the **Enable WSDL access** checkbox checked, this WSDL Project may be propagated to system users.
- From the Error Template drop down list, select **From Listener Policy** to apply the Error Template from the associated Listener Policy to this WSDL, or select **another** Error Template.
- With **Publish a different location in exported WSDL** checked and values in the **Host / Port** fields, this WSDL will be exported with the endpoints set to the entered IP / Port (10.5.6.99 / 8099).
- Select a **Request Filter** link to view details.

HTTP REQUEST FILTER

Name: **SOAP 1.1 Filter**

Format: **Simple**

Description: **WSDL 1.1 SOAP 1.1 HTTP Filter**

Identification Expression*: **(Content-Type ==~ "(?i)text/xml.*") && (method == "POST")**

Parameter:

Convert Content-Encoding: **[No conversion]**

Figure 5: The Virtual Directory Screen and Associated Options.

INDEX

ACLs	
create and apply	49
add a WSDL policy from a WSDL file	10
add a WSDL policy from URI	10
add a WSDL policy from WSDL Library	10
allow additional SOAP headers defined in WSDL	43
apply access control to WSDL Policy	19
applying ACLs to WSDL policies	49
associate ACL to Virtual Directory at operation level in WSDL policy	32
associate existing Network policy to a Virtual Directory in WSDL policy	30
associate IDP Group to WSDL Policy	19
associate IDP Rule to WSDL Policy	19
Automatically load imported files	12
Business Description in Publish WSDL screen	54
Business Key in Publish WSDL screen	54
Business Name in Publish WSDL screen	54
configure Virtual Directory in WSDL policy and associate existing Network policy	30
content type header	36
content types supported for Request Filters	36
content-encoding conversion options with request filters	36
conventions used	1
convert content-encoding options with request filters	36
create a Listener policy	11
create a WSDL library	20
default Filter Expression	27
default Request Filter	36
deflate content-encoding conversion option with request filters	36
Documents tab	53
edit Filter Expression used	32
edit WSDL IDP group	51
edit WSDL Operation IDP Group	51
edit WSDL schema constraints	34
Enable WSDL access of Virtual Directory of a WSDL policy	9
enable WSDL policy for dynamic retrieval	31
enable/disable operation in a WSDL policy	17
enable/disable Virtual Directory in WSDL policy	31
Error Template of Virtual Directory of a WSDL policy	9
examples for single WSDL policy	10
examples for Virtual Directory	30
examples for virtualized WSDL policy	20
examples for WSI Validation on WSDL policy	44
export all operation into a WSDL policy	14
export specific WSDL operations based on ACL	15
export WSDL and specify endpoint location	33
export WSDL policies	57
Filter Expression default in WSDL policy	27
editing	32
Filter Expression of Virtual Directory of a WSDL policy	8
gzip content-encoding conversion option with request filters	36
identity (uncompressed) content-encoding conversion option with request filters	36
IDP Rules tab terms	50, 52
import WSDL policies	57
import WSDLs previously selected locations field	47
legacy systems and disassociate button on Task List tab	38
Listener Policy of Virtual Directory of a WSDL policy	7
MIME types	36
no conversion content-encoding conversion option with request filters	36
override validation settings for WSDL operations	35
Overview Document Description in Publish WSDL screen	54
Overview Document URL in Publish WSDL screen	54
Password in Publish WSDL screen	54
Physical URI of Virtual Directory of a WSDL policy	8
previously selected locations field	47
Process Response of Virtual Directory of a WSDL policy	8
Publish a different location in exported WSDL	9
publish a WSDL policy to UDDI	55
Publish WSDL project terms	54
Published host for exported WSDL policy	9
Published port for exported WSDL policy	9
Published protocol for exported WSDL policy	9
reconfigure Virtual Directory in WSDL policy	32

Remote Policy of Virtual Directory of a WSDL policy	8
Replace Expression of Virtual Directory of a WSDL policy	8
Request Filters	
content types supported	36
default	36
same-name operations support with WSDL policies	18
sample configurations	
for validating SOAP document.....	47
select WSDL operations from a WSDL library ..	21
Service Description	
in Publish WSDL screen	54
Service Name	
in Publish WSDL screen	54
Services tab in WSDL policy	25
Services tab screen terms.....	6
Services tab terms	25
set WSI Basic Profile 1.0 Test Assertions to use during design-time validation	45
set WSI Basic Profile 1.0 test assertions to use during run-time validation for SOAP messages.....	46
Settings tab in WSDL policy.....	42
Settings tab terms	42
Show all remote policies of Virtual Directory of a WSDL policy	8
specify WSDL endpoint location upon export ..	33
Task List Group	
Disassociate button on Task List tab and legacy systems	38
terms	
in IDP Rules tab	50, 52
in Publish WSDL screen	54
in Services tab for WSDL policy	25
in Settings tab for WSDL policy	42
on Services tab for WSDL policy	6
on Virtual Directory of a WSDL policy	7
terms of WSDL schema constraints.....	29
transfer WSDL policies.....	57
update Remote Policy on a WSDL Policy.....	24
upgrade WSDL by File	15
upgrade WSDL file by a UDDI search	15
upgrade WSDL file by URL	15
upgrade WSDL file from WSDL library	23
Use Device IP option	
on Listener Policy	32
use existing Listener policy for WSDL policy ...	12
User ACL of Virtual Directory of a WSDL policy	8
validate message using WS-I Basic Profile 1.0	43
validate SOAP body from WSDL schema defined in WSDL.....	43
validate SOAP document	
sample configurations	47
validate SOAP documents in WSDL policy.....	48

validate SOAP Envelope defined in WSDL	42
validate SOAP headers defined in WSDL	42
view faults in a WSDL policy.....	33
view WSDL operations in a WSDL policy	12
view WSDL ports and virtual directories	12
view WSDL services	12
Virtual Directory	25
associating at operation level in WSDL policy	32
associating existing Network policy in WSDL policy	30
configuring and associating existing Network policy in WSDL policy.....	30
editing Filter Expression used	32
Enable WSDL access.....	9
enabling/disabling in WSDL policy	31
Error Template.....	9
examples	30
Filter Expression.....	8
Listener Policy	7
Physical URI	8
Process Response	8
Publish a different location in exported WSDL	9
Published host	9
Published port.....	9
Published protocol	9
reconfiguring in WSDL policy	32
Remote Policy	8
Replace Expression.....	8
Show all remote policies.....	8
User ACL	8
Virtual Path	7
Virtual URI	7
Virtual Directory terms	7
Virtual Path of Virtual Directory of a WSDL policy.....	7
Virtual URI of Virtual Directory of a WSDL policy	7
virtualized WSDL policy	
examples	20
WSDL	
allowing additional SOAP headers defined in WSDL	43
exporting all operation into a WSDL policy .	14
exporting specific WSDL operations based on ACL	15
same-name operations support.....	18
validate SOAP headers defined in WSDL...	42
validating message using WS-I Basic Profile 1.0	43
validating SOAP body from WSDL schema defined in WSDL	43
validating SOAP Envelope defined in WSDL	42
WSDL file	

Automatically load imported files	5	WSDL policy	
AutomaticallyLoad by secure URL (https)	5	default Filter Expression	27
WSDL library	3	WSDL policy	
creating	20	enabling for dynamic retrieval	31
selecting operations from.....	21	WSDL policy	
upgrading WSDL file from.....	23	viewing faults in	33
WSDL operation		WSDL policy	
editing WSDL Operation IDP Group	51	specifying WSDL endpoint location upon	
WSDL policies		export	33
Automatically load imported files	12	WSDL policy	
WSDL policy		editing WSDL schema constraints	34
upgrading WSDL file by URL.....	15	WSDL policy	
WSDL policy.....	4	overriding validation settings for WSDL	
adding from URI.....	10	operations.....	35
adding from WSDL file.....	10	WSDL policy	
adding from WSDL Library	10	Settings tab.....	42
creating Listener policy	11	WSDL policy	
examples for single	10	setting WS-I Basic Profile 1.0 Test Assertions	
upgrading by File	15	during design-time validation	45
upgrading WSDL file by a UDDI search	15	WSDL policy	
using existing Listener policy	12	setting WS-I Basic Profile 1.0 test assertions	
viewing operations	12	during run-time validation for SOAP	
viewing ports and virtual directories	12	messages.....	46
viewing services.....	12	WSDL policy	
WSDL policy		editing WSDL IDP Group.....	51
enabling/disabling operations	17	WSDL policy	
WSDL policy		Documents tab	53
applying access control to WSDL Policy	19	WSDL policy	
WSDL policy		publishing to UDDI.....	55
associating IDP Rule to WSDL Policy	19	WSDL schema constraints terms	29
WSDL policy		WSDL Service Name	
associating IDP Group to WSDL Policy.....	19	in Publish WSDL screen.....	54
WSDL policy		WSDL validating SOAP documents in WSDL	
updating Remote Policy on a WSDL Policy.....	24	policy.....	48
WSDL policy		WSI Validation on WSDL policy	
Services tab	25	examples	44