



FORUM SYSTEMS SENTRY™ VERSION 9.1
NETWORK 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™ Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, 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 © 2002-2020 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9.1 HTTP Guide, July 2020.

D-ASF-SE-010238

Table of Contents

INTRODUCTION TO THE NETWORK POLICIES GUIDE.....	1
Conventions Used	1
Network Policies Referenced in the HTTP Guide.....	1
HTTP POLICIES	2
Listener Policy.....	2
Remote Policy.....	2
HTTPS Policies and SSL.....	2
Network Policy Wizard.....	2
Network Policies Overview Screen – Terms for HTTP Policies	4
HTTP Listener Network Policy Terms	5
HTTP Remote Network Policy Terms.....	7
How the System Manages Requests and Responses	9
HTTP Policy Wizard Examples.....	9
Add an HTTP Listener Policy	10
Adding the HTTP Listener Policy	10
Associating an ACL for Password Auth to an HTTP Policy	10
Associating an Error Template to an HTTP Policy.....	10
Add an HTTP Remote Policy.....	10
REDIRECT POLICIES	11
Redirect Policy Events.....	11
Authentication Success	11
Authentication Fails	11
No Credentials.....	12
On Error.....	12
Redirect Policies Details Screen Terms	12
Make a Redirect Policy Active for a Policy	13
IBM WEBSHERE MQ POLICIES	14
Network Policies Overview Screen - Terms for MQ Policies.....	15
MQ Policy Details	16
MQ Messaging Modes.....	16
Simple Authentication with MQ Policies	17
HTTP Headers.....	17
MQ Error Handling.....	17
MQ Policy Examples.....	17
Prerequisites for MQ Policies with SSL.....	18
MQ Policy Wizard Terms and Definitions	19
TIBCO-EMS POLICIES.....	22
Simple Authentication with Tibco-EMS Policies	22
Network Policy Overview Screen - Terms for Tibco-EMS Policies	23
Tibco-EMS Policy Wizard Terms and Options	24
Tibco-EMS Policies Examples.....	25
Tibco-EMS Policy with SSL Prerequisites.....	25
ORACLE JMS POLICIES.....	26
Network Policy Overview Screen - Terms for ORACLE JMS Policies	27
ORACLE JMS Policy Wizard Terms and Options	28
ORACLE JMS Policies Examples.....	29
ORACLE JMS Policy with SSL Prerequisites.....	29
SOLACE JMS POLICIES.....	30
Network Policy Overview Screen - Terms for SOLACE JMS Policies	31
SOLACE JMS Policy Wizard Terms and Options	32
ACTIVE MQ POLICIES.....	34
Simple Authentication with Active MQ Policies	34
Network Policy Overview Screen - Terms for Active MQ Policies.....	35

Active MQ Policy Wizard Terms and Options.....	36
Active MQ Policies Examples.....	38
Active MQ Policy with SSL Prerequisites.....	38
RabbitMQ AMQP.....	39
RabbitMQ AMQP Listener Policy.....	39
RabbitMQ AMQP Remote Policy.....	40
Network Policy Overview Screen - Terms for RabbitMQ AMQP Policies.....	40
RabbitMQ AMQP Policy Wizard Terms and Definitions.....	41
AMQP V1.0 Proxy.....	43
Network Policy Overview Screen - Terms for AMQP V1.0 Proxy Policies.....	43
AMQP V1.0 Proxy Policy Wizard Terms and Options.....	45
AMQP V1.0 Proxy Policy with SSL Prerequisites.....	47
AMQP V1.0 Protocol Mixing.....	47
JBOSS JMS POLICIES.....	48
Simple Authentication with JBOSS JMS Policies.....	48
Network Policy Overview Screen - Terms for JBOSS JMS Policies.....	49
JBOSS JMS Policy Wizard Terms and Options.....	50
JBOSS JMS Policies Examples.....	51
JBOSS JMS Policy with SSL Prerequisites.....	51
SUN JAVA MQ POLICIES.....	52
Simple Authentication with SUN JAVA MQ Policies.....	52
Network Policy Overview Screen - Terms for SUN JAVA MQ Policies.....	53
SUN JAVA MQ Policy Wizard Terms and Options.....	54
SUN JAVA MQ Policies Examples.....	55
SUN JAVA MQ Policy with SSL Prerequisites.....	55
SMTP POLICIES.....	56
Network Policies Overview Screen – SMTP Policies Screen Terms.....	56
SMTP Listener Policy.....	56
SMTP Remote Policy.....	56
SMTP Response Policy.....	56
SMTP Architecture.....	56
Typical Email Delivery Architecture.....	57
Typical SMTP Architecture with Forum Sentry.....	58
SMTP Policies and Protocol Mixing.....	59
Transmission Protocols Supported.....	59
SMTP Policy Wizard.....	59
SMTP Policy Examples.....	59
SMTP Listener Policy Terms.....	60
SMTP Remote Policy Terms.....	61
FTP POLICIES.....	62
FTPS, SFTP, and OpenPGP Security.....	62
GROUP REMOTE POLICIES.....	63
Group Remote Failover Behavior.....	63
Load Balancing Strategies with Group Remote Policies.....	63
Failover Strategy.....	63
Round Robin Strategy.....	63
Random Strategy.....	64
Document Size Strategy.....	64
Transfer Throughput Strategy.....	64
Active Requests Strategy.....	64
Weighted Random Strategy.....	64
Response Time Strategy.....	64
Group Remote Policies Wizard Terms.....	65
PROXY POLICIES.....	66
Proxy Policy Details Screen Terms.....	66
Global Proxy System Setting.....	66

ERROR TEMPLATES.....	67
Error Template Details Screen Terms	67
Replacement Variables in Templates	68
Overview of the Attribute Replacement Variable	68
System Error Templates	69
The Default Template	69
The SOAP 1.1 Fault Template.....	70
The SOAP 1.2 Fault Template.....	70
The XML Template	70
Error Template Examples	70
Add an Error Template	70

INTRODUCTION TO THE NETWORK POLICIES GUIDE

Conventions Used

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 Systems API Security Gateway™ is referred to as the Sentry, '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.
- 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 9.1 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.

Network Policies Referenced in the HTTP Guide

The Network Policies screen displays policies and settings for HTTP/HTTPS, FTP/FTPS, Tibco-EMS, IBM MQ, JBOSS JMS, sFTP, and SMTP listener and remote policies. You may create, edit, delete, enable and disable Network policies.

HTTP POLICIES

The Network policies screen manages HTTP/S listener and HTTP/S remote Network policies, their settings and status in the system. Combining an HTTP Listener Policy with a Remote Policy provide the ability to consume requests on the HTTP protocol and reverse proxy these to the target Remote Policy.

Settings on the HTTP policies types are related to HTTP protocol based items such as HTTP identity formats, IP and User Access Control, Error Templates, Timeout Settings, and SSL/TLS.

Listener Policy

A Network listener policy defines an IP, port and protocol used for incoming traffic and an IP ACL policy to apply to this listener. The IP ACL policy is an access control list that filters which IP ranges are allowed or denied on the listener. Other settings are presented in the configuration wizard and shown in the sections below.

Remote Policy

A Remote Network policy defines an IP, Port and protocol of a back-end server used to proxy incoming traffic. Timeout values are provided to enable connection and read-timeouts for how long to wait for back-end systems to respond.

HTTPS Policies and SSL

Any protocol policy supported on Forum Sentry can be protected via an SSL/TLS tunnel. For HTTP, this provides the ability to set any listener or remote policy as HTTP or HTTPS.

The sequence for creating an HTTPS network policy listener is:

1. From the Keys screen, generate or import a PKCS key pair. For more information how to manage or create keys, please refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide*.
2. From the SSL policies screen, create an SSL Termination policy that uses the PKCS key pair from step 1. For more information how to create SSL policies, please refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide*.
3. Create a Network policy listener that refers to the SSL Termination policy created during step 2.

Network Policy Wizard

The Network Policy Wizard guides Administrators through a series of configuration details to provide local and / or remote connection points for the system as well as configuring the type of protocol and access control.

NETWORK POLICIES > HTTP LISTENER POLICY

POLICY NAME

Policy Name*:

Labels:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	HttpListenerPolicy-0
<u>IP ACL Policy:</u>	Unrestricted
<u>Inbound Protocol:</u>	HTTP (chunked)
<u>Listener:</u>	10.5.1.13:9080
<u>Timeout:</u>	
<u>Password Authentication:</u>	
<u>Error Handling:</u>	Default Template

Network Policies Overview Screen – Terms for HTTP Policies

The following table describes each term and definition for the categories displayed above.

TERM	DEFINITION
Name	The identifier for this Network policy.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Red status light = disabled policy. <p>Network policies are automatically enabled upon creation.</p>
Protocol	HTTP or HTTPS
Listener Address	The IP address used to listen for a connection.
Remote Address	The IP address of the back end Server.
Authentication	The types of authentication used or required by the Network policy. The HTTP policy supports Basic Auth, Digest Auth, Form Post Auth, and Cookie Auth. If no Password Authentication is required, the field is empty. SSL Client Auth is configured separately, on the SSL Termination Policy.
ACL	Used to authorize the request. If the setting is Allow All, no authorization is performed. The ACL is also used to restrict the Groups used for authentication. When using an external Identity Server, only Groups with access to the ACL are checked for authentication.
Process Response	Used to display if the response processing option is switched ON or OFF.
Date Modified	Displays the date this Network policy was last changed after creation

HTTP Listener Network Policy Terms

The following table displays all the terms and options in an HTTP Listener Policy. Because each policy is unique, WebAdmin users will not encounter every term or option, and the sequence in which terms appear in the HTTP Policy Wizard may vary. After the Wizard has captured these configuration options, they are visible in the policy details screen:

TERM	DEFINITION
Policy Name	The identifier for the Network policy.
IP ACL Policy	The identifier for the IP Access Control policy associated with this HTTP/S listener policy. This setting is optional and if unset, there will be no limit placed on the client IPs that can connect to the IP:Port defined.
Inbound Protocol	For requests coming from clients set for HTTP or HTTPS. It is strongly recommended to enable the HTTP Chunking option for optimal performance and memory consumption when reading the HTTP requests.
Listener	
Use Device IP	The listener will use the IP address of the system to listen for connections. Forum Systems recommends leaving this setting checked. If the configuration is transferred to a different system, this listener policy can then automatically associate with the IP address of the target Sentry instance with no additional configuration required.
Listener IP	With Use Device IP checked, the current device IP address will be used With Use Device IP unchecked, specify the IP or Hostname for the listener. If this IP is different from the device IP, a new alias will be created for the IP and the WAN network interface will have this new IP address added to it.
Listener Port	Port used to listen for connections.
Use Basic Authentication	When checked, basic authentication can be used to authenticate the user.
Use Digest Authentication	When checked, digest authentication can be used to authenticate the user.
Use Cookie Authentication	When checked, cookie authentication can be used to authenticate the user.
Use Form Post Authentication	When checked, will use credentials from an HTTP Form Post to authenticate the user. A subsequent screen will appear to define how to map the username and password fields to the inbound posted Form.
Require Password Authentication (any type)	<ul style="list-style-type: none"> When checked, a password-authenticated user is required for all requests on this listener. When not checked, the above authentication schemes are used only if the credentials are present on the request, but not enforced. This setting is often used when the Virtual Directories that are associated with this policy are where the ACL to enforce authentication and authorization is set.
Password Authentication Realm	The authentication realm for password authentication. Clients expect to be able to reuse the same credentials for all listeners in the same authentication realm. Additionally, the realm name may be displayed when a client prompts the user to enter a Username and Password.

TERM	DEFINITION
System SSL Termination	The SSL Termination policy used to authenticate the listener to clients.
Password Authentication Access Control	<p>The ACL Policy drop down list is used to select an Access Control List (ACL) specific to password authentication. When Allow All is selected, no Forum access control is active, and all users may have access to the HTTP Listener policy.</p> <p>An Access Control List used to authorize clients. When Allow All is selected, no Forum access control is active, and all users may have access to the HTTP Listener policy. The ACL is also used to restrict the Groups used for authentication. When using an external Identity Server, only Groups with access to the ACL are checked for authentication.</p>
Error Handling	An Error Template to format error responses to the client.

HTTP Remote Network Policy Terms

The following table displays all the terms and options in an HTTP Remote Policy. WebAdmin users may not encounter every term or option as the options in the HTTP Policy Wizard vary based on selections. After the wizard has captured these configuration options, they are visible in the Network policy details screen:

TERM	DEFINITION
Policy Name	The identifier for the Network policy.
Outbound Protocol	<p>Protocol used to communicate with the back end server: HTTP or HTTPS.</p> <p>The Use HTTP Chunking is an additional option. The system supports HTTP 1.1 chunk-encoding which is strongly recommended to enable for performance and optimal memory consumption.</p>
Remote Server	IP address or Host name used to communicate with the back end server.
Remote Port	Port used to communicate with the back end server.
Proxy Policy	Determines whether to use a configured proxy policy to communicate with the HTTP endpoint. No proxy is used when the pull-down reads [No Proxy].
Provide Basic Authentication Credentials	<ul style="list-style-type: none"> When checked, the system will authenticate to the back end sever using credentials chosen in the Remote Authentication screen. When unchecked, the system will not provide password authentication to the remote server.
Provide Digest Authentication Credentials	<ul style="list-style-type: none"> When checked, the system will authenticate using digest auth to the back end sever using credentials chosen in the subsequent Remote Authentication section. When unchecked, the system will not provide digest authentication to the remote server.
TCP Timeouts	<p>With Custom connect timeout <n> seconds checked and a value added to the seconds field, the Transmission Control Protocol (TCP) will timeout if a connection to the system is not successful within the <n> seconds provided.</p> <p>With Custom Read Timeout <n> seconds checked, and a value added to the seconds field, the Transmission Control Protocol (TCP) will timeout if a connection to the system is not read or discovered within the <n> seconds provided.</p>
TERM	DEFINITION
Remote Authentication	<ul style="list-style-type: none"> With Static credentials from User Policy selected, the system will authenticate to the back end server using Basic Auth with the credentials from a specified local user. With Dynamic credentials from authenticated user selected, the system will authenticate to the back end server using Basic Auth with the credentials of the authenticated user. With Propagate client's credentials selected, the system will send credentials provided by the client, verbatim, to the back end server, regardless of local authentication.

TERM	DEFINITION
Basic Authentication	The User policy whose credentials are presented when authenticating to the back end server when the Static credentials from User Policy option is enabled. The User policy needs to be created with the Store recoverable password option checked.
User Policy	The username and password for the User policy will be used to authenticate to the back end server. The User policy needs to be created with the Store recoverable password option checked.
Response Processing	When checked, the response from the back end server is processed before being sent to the client.
SSL Initiation	The SSL Initiation policy used to authenticate the remote server and/or to authenticate to the remove server.

How the System Manages Requests and Responses

The following figure displays the path of a client request and response:

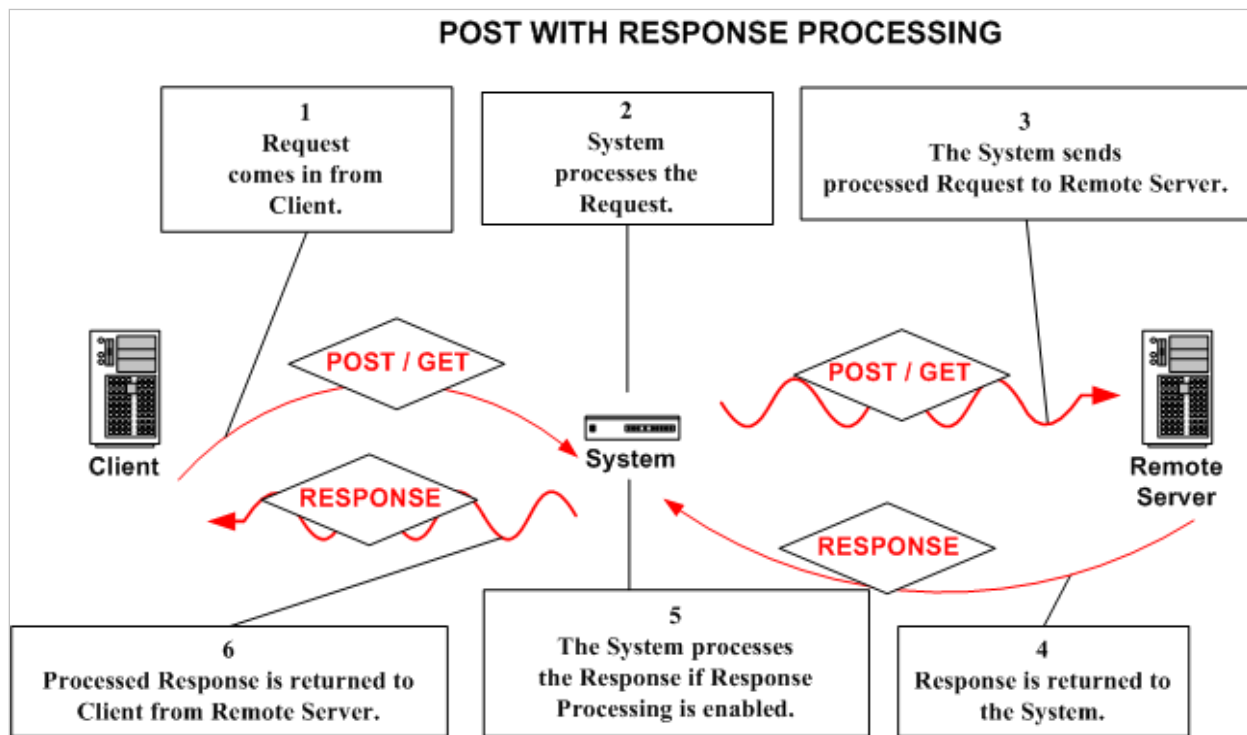


Figure 1: How the System Manages Requests and Responses.

HTTP Policy Wizard Examples

Examples for the common for HTTP policies include:

- Add an HTTP Listener Policy.
- Associate an ACL for Password Auth to an HTTP Policy.
- Associate an Error Template to an HTTP Policy.
- Add an HTTP Remote Policy.

Add an HTTP Listener Policy

Follow these steps to create a listener policy. When binding the SSL Termination policy to your HTTP policy, you are defining the settings for enforcing security between the system and an INBOUND client. This HTTP listener policy uses an SSL Termination policy to authenticate the client. This HTTP listener policy uses Basic Auth and a Password Auth Access Control List (ACL) to authenticate the back end server.

This operation assumes that the WebAdmin user has: 1) created a PKCS key pair in the Keys screen either by generating or importing the key pair, and 2) created an SSL Termination policy in the SSL policies screen by assigning the key pair to an SSL Termination policy before creating this HTTP policy.

Adding the HTTP Listener Policy

- From the Navigator, select the **Network Policies** screen and select **New**.
- Select the **HTTP** radio button and then click **Next**.
- Follow the wizard while referring to the definitions provided in the HTTP Listener Network Policy Terms in the HTTP Policy Wizard section.

Associating an ACL for Password Auth to an HTTP Policy

- From the Password Auth Access Control screen, select an **ACL Policy** from the ACL Policy drop down list. Once associated, this will point to the list of Identity policies to use to authenticate and authorize the credentials.

Associating an Error Template to an HTTP Policy

- From the Template Name drop down list, select an **Error Template name**, and then click **Finish**.

Add an HTTP Remote Policy

Follow these steps to create a remote policy.

- From the Navigator, select the **Network Policies** screen and select **New**.
- Select the **HTTP** radio button and then click **Next**.
- Follow the wizard while referring to the definitions provided in the HTTP Remote Network Policy Terms in the HTTP Policy Wizard section.

REDIRECT POLICIES

The Redirect Policies provide the event settings to accomplish portal federation identity and single-sign on use-cases. The redirect policies are often used in conjunction with HTML based transaction types where a client web browser is the client side of the transaction.

Redirect policies allow the setting of an HTTP Redirect response based on conditions related to the current transaction authentication event. Redirect Policies are configured under the Resources->Redirect Polices menu.

REDIRECT POLICIES > REDIRECT POLICY

REDIRECT POLICY

Name*:

Description:

Labels:

Include Original URI:

URI Parameter Name*:

REDIRECT POLICY EVENTS

Authentication Success

Enabled:

URL*:

Use Host Header:

Processing:

Authentication Failure

Enabled:

URL*:

Use Host Header:

Processing:

No Credentials

Enabled:

URL*:

Use Host Header:

Processing:

On Error

Enabled:

URL*:

Use Host Header:

Processing:

Redirect Policy Events

A redirect event is classified in 4 primary event categories:

Authentication Success

This redirect event will trigger when the current authentication Access Control setting associated with the policy is successful. Associating a Redirect Policy with an HTML, XML, or WSDL Policy will result in this rule to trigger when the policy authentication is successful.

A common use case for Authentication Success is to redirect a successfully authenticated user to the private, secured location of a portal.

Authentication Fails

This redirect event triggers when the current authentication Access Control setting associated with the policy fails. Associating a Redirect Policy with an HTML, XML, or WSDL Policy will result in this rule to trigger when the policy authentication fails.

A common use case for Authentication Fails is to redirect an attempted access to the private, secured located of a portal back to the login page when the provided credentials are invalid or have expired.

No Credentials

This redirect event triggers when the current authentication Access Control setting associated with the policy fail to find any user credentials. Associating a Redirect Policy with an HTML, XML, or WSDL Policy will result in this rule to trigger if no authentication is provided.

On Error

This redirect event triggers whenever there is an error in the processing of the authentication token. Associating a Redirect Policy with an HTML, XML, or WSDL Policy will result in this rule to trigger if there is an error attempting to authenticate the client.

Redirect Policies Details Screen Terms

FIELD NAME	DEFINITION
Name	The identifier for the policy.
Description	Description of current policy
Event	The type of authentication event currently associated with the state of the current transaction. This can be Authentication Success, Authentication Failure, No Credentials, or On Error.
URL	The full URI target to include in the issued HTTP redirect back to the client.
Use Host Header	This option will override the URI hostname defined and instead always ensure redirection occurs back to the client on the same domain name / IP address that was used for the initial request.
Include Original URI	This option will take the entire original inbound URI and include it as a query string parameter on the issued redirect.
URI Parameter Name	Used in conjunction with the Include Original URI setting. This setting defines the name of the query string parameter rule to issue in the redirect.
Task List Group	Enables processing a Task List Group prior to the URL redirect being issued. The most common use case for this is to use Mapping Tasks to dynamically map information into the URL.

Make a Redirect Policy Active for a Policy

The Redirect Policies are consumed from the virtual directory screen of HTML, XML, and WSDL Polices. To enable a Redirect Policy, simply choose the policy from the “Redirect Policy” pull-down. A value of none means that there is no associated Redirect Policy active

[XML POLICIES](#) > [XML POLICY](#)

XML POLICY

Policy Name: New XML Policy

Virtual Directories | Task Lists | Settings | IDP Rules | Logging

[Virtual Directories](#) > **Virtual Directory: New Virtual Directory**

VIRTUAL DIRECTORY

Name*: New Virtual Directory

Description:

Virtual URI: amqp://192.168.1.42:5672(/.*)?

Remote URI: http://10.5.1.41

VIRTUAL URI SETTINGS

Listener Policy: Amqp10ListenerPolicy [Edit](#)

Virtual Host:

Use virtual host as a regular expression

Virtual Path:

Enable Virtual Path Case Insensitivity

Filter Expression: (/.*)?

Replace Expression: \$0

Request Filter Policy: Default [Edit](#)

Error Template: [From Listener Policy]

Google Analytics: [None]

ACCESS CONTROL

IP ACL Policy: Unrestricted [Edit](#)

ACL Policy: [Allow All]

XACML Policy: [None]

Password Authentication: [From Listener Policy]

Redirect Policy: [None]

VIRTUAL DIRECTORY TASKS

IBM WEBSPHERE MQ POLICIES

IBM Websphere MQ policies represent an active connection to a channel and queue manager running on the target WebSphere instance. IBM Websphere MQ is a reliable messaging platform that uses a queue manager to allow for reliable message delivery between client applications. MQ policies support TCP/IP and SSL-based connections to the queue manager.

To support authentication and access control of users, the system provides a simple user/password-based access control paradigm, and supports the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the IBM Websphere MQ infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into MQ-based messages. Forum Sentry has support for JMS-based messages (MQRFH2) including JMSTextMessages and JMSTextMessages. Sentry also supports the MQSTR native message type to support messages sent from non-JMS-based clients. Forum Sentry is able to mix any of those types for inbound traffic or for sending the message outbound.

Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session. This mode leverages the MQI Synchpoint technology within IBM Websphere MQ to guarantee message delivery. The system also supports reading the "Backout Requeue Name" and "Backout Threshold" values directly from the queue. These values can be set to allow for error messages to be placed in the designated error queue; and in the special case of receiving a poison message, the backout threshold will specify how many times to retry the operation before shutting down the MQ listener. All of these precautions are used to guarantee that messages can never be lost.

The Network Policies screen manages MQ policies that are used to specify how to connect to the Websphere MQ instance. The system provides a means of creating Listener and Remote policies, their settings and status in the system. Users may create, edit, delete, disable and enable MQ Listener and Remote policies.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system. These policies may use SSL Policies as well to provide an additional layer of security between the product and the queue manager.

Network Policies Overview Screen - Terms for MQ Policies

The Network Policies screen includes a listing of all existing MQ policies. The following table describes the terms and definitions for MQ policies:

TERM	DEFINITION
Name	The identifier for this Network policy.
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. <p>Network policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this Network policy, or MQ.
Listener Address	The IP address of the system.
Remote Address	The IP address of the back end server.
Mode	<p>The mode of operation for the Network policy: synchronous or asynchronous.</p> <ul style="list-style-type: none">• If checked, and there is an error, the error message is returned to the client.• If unchecked, then the message is processed asynchronously. If there is an error, the error message is sent to the error queue.

MQ Policies connect to a queue manager and listen for messages on a specified queue. After receiving a message and processing it, the message is then placed back on a queue manager queue as defined in the remote policy, or mixed in real-time to the target protocol based on the type of selected remote policy that has been associated. MQ messages can be protocol mixed in either direction.

MQ Policy Details

View the details of an MQ policy by clicking on an MQ policy name from the Network Policies screen. The following details screen divides into two sections. This example displays an MQ Listener policy and details of the listener host name value. Clicking on a link under the POLICY SELECTIONS section brings up the values pertinent to that element name, for example, Host. The Network Policy details screen includes all the values relevant for this specific MQ policy.

POLICY NAME

Policy Name*:

Labels:

Next

POLICY SELECTIONS

Policy Name:	MqListenerPolicy
Server:	10.5.6.85
Port:	1414
Channel:	S_RMU
Queue Manager:	QM_qa_client_85
Queue:	Queue2.inbound.queue
MQ Message Format:	JMS Format (MQRFH2)
Message Type:	JMS Map Message
Allowed Message Types:	Text,Bytes
Field:	Client_Data
User Id:	mquser1
Password:	*****
Requires SSL:	Off
Authenticate Message:	Off
Synchronous Policy:	On
Reply Delivery Mode:	Persistent
Error Handling:	Default Template

SERVER

Server*:

Next

POLICY SELECTIONS

Figure 2: Example MQ Listener Policy Details Screen.

MQ Messaging Modes

MQ messages may be processed in synchronous or asynchronous modes. Synchronous mode refers to a JMS-correlated request/reply pattern where the JMSReplyTo header field is used to tell the ultimate recipient where to send a reply to. Error processing in synchronous mode is very simple because all SOAP Fault messages are returned to the JMSReplyTo queue.

Simple Authentication with MQ Policies

In the case where the product is going to be used to generate a security assertion, the system adds the ability to authenticate each message at runtime. The system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity. The identity can be used in the processing to generate a WS-Security and/or SAML assertion representing that authentication event. This is a proprietary mechanism because the JMS specification does not have any provision for passing credentials and identity information.

An ideal architecture, of course, would be the receipt of a standards-based security assertion such as a WS-Security token, but since many clients are not capable of generating these, the Forum system offers this service.

HTTP Headers

When mixing an MQ WebSphere policy with an HTTP-based policy, any HTTP headers that are passed will be automatically converted to JMS headers by encoding all of the dashes to underscores and vice-versa. This enables an HTTP response to be populated with headers that correspond with the request. In addition, the MQ client can add JMS header fields that will be ultimately placed into the HTTP messages.

If Administrators do not set the `content_type` or `Content_type` property on MQ requests, then the default content type will be `application/x-www-form-urlencoded`.

MQ Error Handling

When the messages cannot be delivered to a known location a session recovery is attempted. The recovery is only attempted under the following conditions:

- The message is not a redelivery. Redelivery is defined as the message having the redelivery flag set. i.e. `JMSRedelivered` property is true
- The backout threshold is used to decide to trigger a recovery. If the threshold has not been exceeded, the JMS client redelivers the message.

When MQ is not properly configured, every message not delivered will be retried at least once. If the queue has no Backout Queue (BOQ) or Dead Letter Queue (DLQ) defined, the message will be lost. This case is a misconfiguration as the administrator of MQ should have defined a BOQ or DLQ.

When MQ is properly configured with a backout queue, a dead letter queue and a backout threshold, every time the session is recovered, the `JMSXDeliveryCount` is increased. Once the delivery count reaches the threshold the queue manager automatically moves the message to the BOQ or DLQ. If the queue does not have BOQ defined, the message ends up at the DLQ. Having a proper threshold is imperative for the Queue Manager to know when to move the message to the proper queue. If the threshold is not defined, Sentry will fallback by moving the messages to the DLQ and BOQ as defined. However, this is a misconfiguration and will be missing the DLQ header. With a properly configured Sentry and MQ server, no messages will ever be lost, and messages moved to the BOQ or DLQ would be properly written.

MQ Policy Examples

Examples for MQ policies include:

- Add an MQ Listener Policy With or Without SSL.
- Add an MQ Remote Policy With or Without SSL.

Prerequisites for MQ Policies with SSL

Follow the listed sequence to create an MQ policy with SSL:

1. Create a key pair (for more information, refer to *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide*).
2. Create an SSL policy that refers to the key pair (for more information, refer to *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide*).
3. Create an MQ policy that refers to an SSL policy.

MQ Policy Wizard Terms and Definitions

The following table displays all the terms and definitions in the MQ Policy Wizard that appear under the Policy Selections section of the screen. Because each policy is unique, you will not encounter every term, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the NETWORK POLICY details screen:

TERM	DEFINITION
Policy Name	The identifier for this MQ policy.
Host	A valid host name or IP address that represents the name or address of the machine that is hosting the channel, queue manager & queue.
Port	A valid port number (as defined in HTTP Policy) that represents the TCP/IP port.
Channel	A channel is used to specify a logical communication link between WebSphere components. The Forum Systems system supports TCP/IP channels.
Queue Manager	The Queue Manager provides queuing services to client applications and provides the application programming interface to PUT and GET messages to and from queues.
Queue	A Queue provides a named destination to which messages can be sent or retrieved.
MQ Message Format	<ul style="list-style-type: none"> • With MQRFH2 checked, supports the MQ JMS message format. • With MQSTR checked, supports the native MQ message format. This option is used by customers whose infrastructure is not using Java and JMS, but still want to interface with the Forum Systems system.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
Message Type	Message Types values are Text Message, Map Message or Bytes Message. These correspond to JMS message types that are appropriate for carrying XML data.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the mqm Group on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none"> • With Requires SSL checked, the message is processed via SSL. • With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message. Note that this is an initiation policy because all MQ connections are considered to be client connections
SSL Cipher Spec	From the SSL Cipher Spec drop down list, select an SSL Cipher

TERM	DEFINITION
	<p data-bbox="516 226 1333 254">Specification to match for the inbound SSL message, which includes:.</p> <ul data-bbox="565 289 911 541" style="list-style-type: none"> <li data-bbox="565 289 857 317">• RC4 / MD5 EXPORT <li data-bbox="565 321 786 348">• RC4 / MD5 US <li data-bbox="565 352 740 380">• NULL SHA <li data-bbox="565 384 911 411">• DES SHA EXPORT 1024 <li data-bbox="565 415 870 443">• TRIPLE DES SHA US <li data-bbox="565 447 842 474">• DES SHA EXPORT <li data-bbox="565 478 769 506">• RC4 SHA US <li data-bbox="565 510 740 537">• NULL MD5
Authenticate Message	<ul data-bbox="565 579 1365 730" style="list-style-type: none"> <li data-bbox="565 579 1365 699">• If checked, the incoming message should have the header fields fs_user and fs_password populated with appropriate credentials. They will be used to authenticate the message and establish the proper identity. <li data-bbox="565 703 1224 730">• If unchecked, the message will not be authenticated.
Synchronous Policy	<ul data-bbox="537 768 1382 919" style="list-style-type: none"> <li data-bbox="537 768 1382 825">• Synchronous mode (Synchronous Policy checked) means that reply messages will be returned to the source. <li data-bbox="537 863 1365 919">• Asynchronous mode (Synchronous Policy unchecked) means that communications are event driven and can be long running.
Template Name	<p data-bbox="492 957 1344 1014">The error handling template selected to capture a returned, unprocessed message.</p>
SSL Initiation Policy	<p data-bbox="492 1052 1349 1108">With the outbound Requires SSL option checked, select an SSL Initiation policy to apply to this outbound message.</p>
Delivery Modes	<p data-bbox="492 1146 1414 1203">Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul data-bbox="537 1234 1414 1444" style="list-style-type: none"> <li data-bbox="537 1234 1414 1325">• Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage. <li data-bbox="537 1329 1414 1444">• Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Process Response	<ul data-bbox="537 1482 1398 1602" style="list-style-type: none"> <li data-bbox="537 1482 1398 1539">• When checked, xml data in the response message can be processed by a task list. <li data-bbox="537 1543 1398 1602">• When unchecked, xml data in the response message will be proxied back to the requestor without being processed by a task list.
Synchronous Timeout (Seconds)	<p data-bbox="492 1640 1078 1663">The default Synchronous Timeout is five seconds.</p>
Template Name	<p data-bbox="492 1734 1403 1791">The Name of the Error Handling template to apply when Process Response is enabled.</p>

TERM	DEFINITION
Reply Queue Type	<ul style="list-style-type: none">• With Named selected, users can select an existing queue for the reply message to be placed on.• With Temporary selected, a temporary unique named queue will be generated on the fly for the reply to be placed on. The generated name can be obtained from the standard JMSReplyTo header field.
Reply Message Type	Reply Message Types values are Bytes Message, Text Message or Map Message. These correspond to JMS message types that are appropriate for carrying XML data. The system also supports the MQSTR message type.

TIBCO-EMS POLICIES

Tibco's Enterprise Messaging Service (Tibco-EMS) is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The Tibco EMS architecture relies on the use of a Tibco EMS server that sits between clients to coordinate the sending and receiving of data. Used with the system, Tibco-EMS policies work with and without SSL and can leverage the patented on-board crypto acceleration of the Sentry product. In addition, Sentry supports both the point to point messaging model and the publish / subscribe messaging model available in EMS.

To support authentication and access control of individual users, Sentry provide a simple user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the Tibco EMS infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with Tibco-EMS policies. For more information, refer to the Protocol Mixing section of the *Forum Systems Sentry™ Version 9.1 XML Policies Guide*.

The system provides the following for Tibco-EMS policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple "wizard" based configuration system.
- Supports point to point and publish/subscribe messaging models.

Simple Authentication with Tibco-EMS Policies

In the case where our product is going to be used to generate a security assertion, we added the ability to authenticate each message at runtime. The system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity. The identity can be used in the processing to generate a WS-Security and/or SAML assertion representing that authentication event. This is a proprietary mechanism because the JMS specification does not have any provision for passing credentials and identity information.

An ideal architecture of course would be the receipt of a standards based security assertion such as a WS-Security token, but since many clients are not capable of generating these we offer this service.

Network Policy Overview Screen - Terms for Tibco-EMS Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in Tibco-EMS policies.

TERM	DEFINITION
Name	The identifier for this Tibco-EMS policy.
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. <p>Tibco-EMS policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the Tibco EMS Server
Remote Address	The URI of the Tibco EMS Server

Tibco-EMS Policy Wizard Terms and Options

The following table displays all the terms and options in the Tibco-EMS Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the Tibco-EMS Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this Tibco-EMS Policy.
Server URL	The URL and Port of the Tibco-EMS server.
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none"> • Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage. • Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded Messages sent via the JMS Bytes binary message format.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the Tibco-EMS Group on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none"> • With Requires SSL checked, the message is processed via SSL. • With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message.

TERM	OPTIONS AVAILABLE
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier. • If unchecked, the message will not be authenticated.
ACL Policy	With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Template Name	The error handling template selected to capture a returned, unprocessed message.

Tibco-EMS Policies Examples

Examples for Tibco-EMS policies include:

- Add a Tibco-EMS Listener policy with or without SSL.
- Add a Tibco-EMS Remote policy with or without SSL.

URI Format without SSL: tcp://hostname:7222

URI Format with SSL: ssl://hostname:7243

Tibco-EMS Policy with SSL Prerequisites

Follow the listed sequence to create a Tibco-EMS policy with SSL:

1. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
2. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
3. Create a Tibco EMS policy that refers to the SSL policy.

ORACLE JMS POLICIES

Oracle's Enterprise Messaging Service (ORACLE JMS) is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The ORACLE JMS architecture relies on the use of a ORACLE JMS server that sits between clients to coordinate the sending and receiving of data. Used with the system, ORACLE JMS policies work with and without SSL and can leverage the patented on-board crypto acceleration of the Sentry product. In addition, Sentry supports both the point to point messaging model and the publish / subscribe messaging model available in EMS.

To support authentication and access control of individual users, Sentry provide a simple user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the ORACLE JMS infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with ORACLE JMS policies. For more information, refer to the Protocol Mixing section of the *Forum Systems Sentry™ Version 9.1 XML Policies Guide*.

The system provides the following for ORACLE JMS policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.

Network Policy Overview Screen - Terms for ORACLE JMS Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in ORACLE JMS policies.

TERM	DEFINITION
Name	The identifier for this ORACLE JMS policy.
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. <p>ORACLE JMS policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the ORACLE JMS Server
Remote Address	The URI of the ORACLE JMS Server

ORACLE JMS Policy Wizard Terms and Options

The following table displays all the terms and options in the ORACLE JMS Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the ORACLE JMS Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this ORACLE JMS Policy.
Server URL	The URL and Port of the ORACLE JMS server.
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none">• Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage.• Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded Messages sent via the JMS Bytes binary message format.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the ORACLE JMS Group on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none">• With Requires SSL checked, the message is processed via SSL.• With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message.

TERM	OPTIONS AVAILABLE
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier. • If unchecked, the message will not be authenticated.
ACL Policy	With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Template Name	The error handling template selected to capture a returned, unprocessed message.

ORACLE JMS Policies Examples

Examples for ORACLE JMS policies include:

- Add an ORACLE JMS Listener policy with or without SSL.
- Add an ORACLE JMS Remote policy with or without SSL.

ORACLE JMS Policy with SSL Prerequisites

Follow the listed sequence to create an ORACLE JMS policy with SSL:

4. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
5. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
6. Create an ORACLE JMS policy that refers to the SSL policy.

SOLACE JMS POLICIES

SOLACE JMS is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The SOLACE JMS architecture relies on the use of a SOLACE JMS server that sits between clients to coordinate the sending and receiving of data. Sentry supports Topics and Queues for publish / subscribe messaging.

To support authentication and access control of individual users, Sentry provide a user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the SOLACE JMS infrastructure, Sentry supports a flexible mechanism for retrieving and placing messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with SOLACE JMS policies. To Mix protocols, simply choose a different protocol for the listener or remote policy type and Sentry will automatically mix protocols as messages are processed.

The system provides the following for SOLACE JMS policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.

Network Policy Overview Screen - Terms for SOLACE JMS Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in SOLACE JMS policies.

TERM	DEFINITION
Name	The identifier for this SOLACE JMS policy.
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. <p>SOLACE JMS policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the SOLACE JMS Server to listen for published messages
Other	The URI of the SOLACE JMS Server to publish messages after processing

SOLACE JMS Policy Wizard Terms and Options

The following table displays all the terms and options in the SOLACE JMS Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the SOLACE JMS Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this SOLACE JMS Policy.
Addresses	One or more IP addresses or Host names for the target Solace Server. URL format can be used if a port needs to be specified, otherwise default 55555 is used when compression is not in use, or 55003 when compression is on. If using TLS, the default port is 55443.
Message VPN	Virtual private network name to use
Number of Sessions	The number of concurrent sessions to allow to be established
Connection Factory	Name of the connection factory
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none"> • Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage. • Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded messages sent via the JMS Bytes binary message format.
Allowed Message Type	Determines which among Text, Map, and Byte that are allowed
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the SOLACE JMS Group on the target machine.
Password	The password that corresponds to the User ID entered.
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier.

TERM	OPTIONS AVAILABLE
ACL Policy	<ul style="list-style-type: none"> • If unchecked, the message will not be authenticated. <p>With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener</p>
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Ignore JMS Reply To Header	Will not allow the JMS ReplyTo header to override the policy settings
Error Handling	The error handling template to use to format error messages

ACTIVE MQ POLICIES

Apache ActiveMQ™ (Active MQ) is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The Apache ActiveMQ™ architecture relies on the use of an ActiveMQ server that sits between clients to coordinate the sending and receiving of data. Used with the system, Active MQ policies work with and without SSL and can leverage the patented on-board crypto acceleration of the Sentry product. In addition, Sentry supports both the point to point messaging model and the publish / subscribe messaging model available in JMS.

To support authentication and access control of individual users, Sentry provide a simple user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent via the Apache ActiveMQ™ infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with Active MQ policies. To mix protocols, simply choose a different protocol for the listener or remote policy type and Sentry will automatically mix protocols as messages are processed.

The system provides the following for Active MQ policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.
- Stomp support so that clients can be written easily in C, Ruby, Perl, Python, PHP, ActionScript/Flash, Smalltalk to talk to ActiveMQ as well as any other popular Message Broker

Simple Authentication with Active MQ Policies

In the case where our product is going to be used to generate a security assertion, we added the ability to authenticate each message at runtime. The system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity. The identity can be used in the processing to generate a WS-Security and/or SAML assertion representing that authentication event. This is a proprietary mechanism because the JMS specification does not have any provision for passing credentials and identity information.

An ideal architecture of course would be the receipt of a standards based security assertion such as a WS-Security token, but since many clients are not capable of generating these we offer this service.

Network Policy Overview Screen - Terms for Active MQ Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in Active MQ policies.

TERM	DEFINITION
Name	The identifier for this Active MQ policy.
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. <p>Active MQ policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the Active MQ Server (Queue Manager)
Other	The URI of the Active MQ Server (Queue Manager)

Active MQ Policy Wizard Terms and Options

The following table displays all the terms and options in the Active MQ Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the Active MQ Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this Active MQ Policy.
Connection URL	The URL and Port of the Active MQ server.
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none"> • Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage. • Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded Messages sent via the JMS Bytes binary message format.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the Active MQ Group on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none"> • With Requires SSL checked, the message is processed via SSL. • With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message.

TERM	OPTIONS AVAILABLE
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier. • If unchecked, the message will not be authenticated.
ACL Policy	<p>With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener</p>
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Template Name	<p>The error handling template selected to capture a returned, unprocessed message.</p>

POLICY NAME

Policy Name*:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	ActiveMQListenerPolicy
<u>Connection URI:</u>	tcp://10.5.1.26:61616
<u>Destination Type:</u>	Queue
<u>Destination:</u>	ActiveMQ_Destination
<u>Message Type:</u>	JMS Text Message
<u>Username:</u>	admin1
<u>Password:</u>	*****
<u>Requires SSL:</u>	Off
<u>Authenticate Message:</u>	Off
<u>Synchronous Policy:</u>	Off
<u>Error Handling:</u>	Default Template

POLICY NAME

Policy Name*:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	ActiveMQRemotePolicy
<u>Connection URI:</u>	tcp://10.5.1.26:61616
<u>Destination Type:</u>	Queue
<u>Destination:</u>	ActiveMQ_Remote_Destination
<u>Delivery Mode:</u>	Non-Persistent
<u>Message Type:</u>	JMS Text Message
<u>Time To Live (seconds):</u>	0
<u>User Id:</u>	admin1
<u>Password:</u>	*****
<u>Requires SSL:</u>	Off
<u>Synchronous Policy:</u>	Off

Active MQ Policies Examples

Examples for Active MQ policies include:

- Add an Active MQ Listener policy with or without SSL.
- Add an Active MQ Remote policy with or without SSL.

Active MQ Policy with SSL Prerequisites

Follow the listed sequence to create an Active MQ policy with SSL:

1. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
2. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
3. Create an Active MQ policy that refers to the SSL policy

RabbitMQ AMQP

AMQP is an open standard for interoperable messaging implemented by several vendors. For the examples below, we will be using RabbitMQ one such implementation of an AMQP message queue server. Before configuring RabbitMQ AMQP listener and remote policies on Sentry, the following information needs to be obtained about the RabbitMQ AMQP server to be used:

1. Host and port
2. Is authentication required?
3. Virtual host
4. Queue name
5. Exchange type

RabbitMQ comes with default built-in setting that allows users to customize each connection parameter according to their specification. The connection settings is use to define the host and port for the RabbitMQ AMQP server. Users would have to specify a virtual host which provides a way to segregate applications using the same RabbitMQ instance. RabbitMQ also comes with a built in guest account which can be replaced with individual user accounts. Sentry supports authentication of individual users and provides a simple user/password based authentication credential.

When configuring RabbitMQ AMQP policies on Sentry, the default exchange type is automatically selected. User can either use the default setting or add a new Exchange type from the RabbitMQ AMQP server. Specify a queue name previously defined in the RabbitMQ AMQP server to complete the RabbitMQ AMQP listener and remote policy configuration on Sentry. Queue persistence and Synchronous policy are optional and are disabled by default.

The Network Policies screen manages RabbitMQ AMQP policies that are used to specify how to connect to the RabbitMQ AMQP server. The system provides a means for creating the RabbitMQ AMQP Listener and Remote policies, their settings and status in the system. Users may create, edit, delete, disable and enable RabbitMQ AMQP Listener and Remote policies from the network policies screen.

RabbitMQ AMQP Listener Policy

A RabbitMQ AMQP client connects to a RabbitMQ AMQP server for the following reasons:

1. Publish messages according to the messaging model
2. Consume messages according to the messaging model

The required parameters needed to establish connection to the AMQP server are available on the RabbitMQ AMQP Listener policy configuration screen. The following example displays a RabbitMQ AMQP Listener policy and details of the listener host name value.

NETWORK POLICIES > AMQP LISTENER POLICY

POLICY NAME

Policy Name*:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	AmqpListenerPolicy
<u>Connection Settings:</u>	10.5.1.37:5672
<u>Authenticate:</u>	No
<u>Virtual Host:</u>	/
<u>Requires SSL:</u>	No
<u>Exchange Type:</u>	default
<u>Queue Name:</u>	AMQP_Test
<u>Queue Persistence:</u>	Disabled
<u>Synchronous Policy:</u>	No
<u>Error Handling:</u>	Default Template

RabbitMQ AMQP Remote Policy

The RabbitMQ AMQP remote policy defines a policy configuration which proxies the RabbitMQ AMQP server. Like the RabbitMQ AMQP listener policy, the remote policy configuration screen contains the connection parameters needed to establish connection to the RabbitMQ AMQP server.

NETWORK POLICIES > AMQP REMOTE POLICY

POLICY NAME

Policy Name*:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	AmqpRemotePolicy
<u>Connection Settings:</u>	10.5.1.37:5672
<u>Authenticate:</u>	No
<u>Virtual Host:</u>	/
<u>Requires SSL:</u>	No
<u>Exchange Type:</u>	default
<u>Queue Name:</u>	AMQP_Test
<u>Queue Persistence:</u>	Disabled
<u>Synchronous Policy:</u>	No

Network Policy Overview Screen - Terms for RabbitMQ AMQP Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in RabbitMQ AMQP policies.

TERM	DEFINITION
Name	The identifier for this RabbitMQ policy.
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. <p>RabbitMQ AMQP policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	Address and port on Sentry for the RabbitMQ AMQP listener where messages will be received from clients.
Remote Address	Address and port of the remote RabbitMQ AMQP server that messages will be sent to

No Labels					
Listener Policies					
NAME	STATUS	PROTOCOL	LISTENER ADDRESS	OTHER	DATE MODIFIED
AmpqListenerPolicy	●	RabbitMQ	10.5.1.37:5672	Destination: Test Mode: Async	

Remote Policies					
NAME	STATUS	PROTOCOL	REMOTE ADDRESS	OTHER	DATE MODIFIED
AmpqRemotePolicy	●	RabbitMQ	10.5.1.37:5672	Destination: Test Mode: Async	

GDM Transfer GDM Export Delete Enable Disable Copy New

RabbitMQ AMQP Policy Wizard Terms and Definitions

The following table displays all the terms and options in the RabbitMQ AMQP Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the RabbitMQ AMQP Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this RabbitMQ AMQP policy.
Connection Settings	Defines the host and port for the connection to the RabbitMQ AMQP server.
Virtual Host	Provides a way to segregate applications using the same RabbitMQ instance.
Requires SSL	With Requires SSL checked, any messages received will be processed using SSL.
Exchange Type	Sent and received messages to and from a queue.
Queue Name	Identifier for the destination to which messages can be sent or received.
Queue Persistence	Prevents data lost when the queue is maxed out.
Synchronous Policy	With Synchronous Policy checked, error messages will be returned to their source.
Error Handling	The Error Template to be used for this policy.

AMQP V1.0 Proxy

AMQP V1.0 is an open standards based application layer protocol for message-oriented middleware. Sentry functions with AMQP V1.0 clients as a proxy to process incoming messages using both AMQP and AMQPS before they are sent on to the next hop in transit to their destination. This processing can include message conformity checks, security checks, and any other operation that Sentry can perform on a document or its protocol headers.

To support authentication and access control of individual requests, Sentry supports the full range document based authentication methods including WS-Security and SAML. The identity established during the authentication event can be used to support access control of services as well. Inbound requests can also be filtered by source IP using IP ACLs on the AMQP V1.0 listener policy.

The Network Policies screen displays existing policies, port settings and policy parameters that listener and remote policies are configured to use.

You may also mix protocols with AMQP V1.0 Proxy policies. For more information, refer to the Protocol Mixing section of the *Forum Systems Sentry™ Version 9.1 XML Policies Guide*.

The system provides the following for AMQP V1.0 Proxy policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.

Network Policy Overview Screen - Terms for AMQP V1.0 Proxy Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in AMQP V1.0 Proxy policies.

TERM	DEFINITION
Name	The identifier for this AMQP V1.0 Proxy policy.
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. <p>AMQP V1.0 Proxy policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	Address and port on Sentry for the AMQP V1.0 Proxy listener where messages will be received from clients.
Other	Address and port of the remote AMQP v1.0 server that messages will be sent to

No Labels

Listener Policies

<input type="checkbox"/> NAME	STATUS	PROTOCOL	LISTENER ADDRESS	OTHER
<input type="checkbox"/> Ampq10ListenerPolicy	●	AMQP 1.0	0.0.0.0:5672	N/A

Remote Policies

<input type="checkbox"/> NAME	STATUS	PROTOCOL	REMOTE ADDRESS	OTHER
<input type="checkbox"/> Ampq10RemotePolicy	●	AMQP 1.0	amqp-v1.example.org:5672	Process Response: Off

[GDM Transfer](#) [GDM Export](#) [Delete](#) [Enable](#) [Disable](#) [Copy](#) [New](#)

AMQP V1.0 Proxy Policy Wizard Terms and Options

The following table displays all the terms and options in the AMQP V1.0 Proxy Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the AMQP V1.0 Proxy Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this AMQP V1.0 Proxy policy.
IP ACL Policy	IP ACL that will limit clients that can connect based on their network address.
Inbound Protocol	Whether AMQP or AMQPS will be used for clients connecting to Sentry.
Outbound Protocol	Whether AMQP or AMQPS will be used to connect to the back-end AMQP v1.0 server.
Use Device IP	When enabled, Sentry will use the device IP (WAN on appliance and 0.0.0.0 on software ports) as the listener IP. Used for configuration portability.
Listener IP	The IP that Sentry will listen on for AMQP v1.0 clients.
Listener Port	The port that Sentry will listen on for AMQP v1.0 clients.
Idle Timeout	The amount of time a client can be idle before being disconnected.
Remote Server	The hostname or IP of the back-end AMQP v1.0 server.
Remote Port	The port to connect to on the back-end AMQP v1.0 server.
SSL Termination Policy	With the AMQPS Outbound Protocol option selected, the SSL Termination policy will be used for clients connecting to Sentry.
SSL Initiation Policy	With the AMQPS Inbound Protocol option selected, the SSL Initiation policy will be used when Sentry connects to the back-end AMQP v1.0 server.

TERM	OPTIONS AVAILABLE
Idle Timeout	<ul style="list-style-type: none"> • If checked, the connection will create a timeout error if it has been idle for the specified duration. • If unchecked, the connection will use the default values for connection duration before a timeout error occurs.
Transfer Timeout	<ul style="list-style-type: none"> • If checked, the transfer of data will timeout if it has been idle for the specified duration. • If unchecked, the timeout for data transfers will use the default values for connection duration before a timeout error occurs.
Process Response	<ul style="list-style-type: none"> • When checked, xml data in the response message can be processed by a task list. • When unchecked, xml data in the response message will be proxied back to the requestor without being processed by a task list.
Template Name	The error handling template selected to capture a returned, unprocessed message.

NETWORK POLICIES > AMQP 1.0 LISTENER POLICY

POLICY NAME

Policy Name*:

Labels:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	Amqp10ListenerPolicy
<u>IP ACL Policy:</u>	Unrestricted
<u>Inbound Protocol:</u>	AMQP
<u>Listener:</u>	0.0.0.0:5672
<u>Idle Timeout:</u>	30
<u>Error Handling:</u>	Default Template

NETWORK POLICIES > AMQP 1.0 REMOTE POLICY

POLICY NAME

Policy Name*:

Labels:

[Next](#)

POLICY SELECTIONS

<u>Policy Name:</u>	Amqp10RemotePolicy
<u>Outbound Protocol:</u>	AMQP
<u>Remote Server:</u>	amqp-v1.example.org:5672
<u>Timeouts:</u>	Idle: 30 Transfer: 30
<u>Process Response:</u>	Off

AMQP V1.0 Proxy Policies Examples
Examples for AMQP V1.0 Proxy policies include:

- Add an AMQP V1.0 Proxy Listener policy with or without SSL.
- Add an AMQP V1.0 Proxy Remote policy with or without SSL.

AMQP V1.0 Proxy Policy with SSL Prerequisites

Follow the listed sequence to create an AMQP V1.0 Proxy policy with SSL:

1. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
2. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
3. Create an AMQP V1.0 Proxy policy that refers to the SSL policy.

AMQP V1.0 Protocol Mixing

When protocol mixing with the AMQP V1.0 Proxy network policies the "To" and "From" protocol headers in the protocol you are mixing to or from can be used to specify the AMQP source and destination for a message. This allows, for example, a "To" header in an HTTP request to specify the AMPQ Queue to send the message to when protocol mixing to an AMQP V1.0 Proxy remote policy.

JBOSS JMS POLICIES

JBOSS Enterprise Messaging Service (JBOSS JMS) is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The JBOSS JMS architecture relies on the use of a JBOSS JMS server that sits between clients to coordinate the sending and receiving of data. Used with the system, JBOSS JMS policies work with and without SSL and can leverage the patented on-board crypto acceleration of the Sentry product. In addition, Sentry supports both the point to point messaging model and the publish / subscribe messaging model available in JMS.

To support authentication and access control of individual users, Sentry provides a simple user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the JBOSS JMS infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with JBOSS JMS policies. To mix protocols, simply choose a different protocol for the listener or remote policy type and Sentry will automatically mix protocols as messages are processed.

The system provides the following for JBOSS JMS policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.

Simple Authentication with JBOSS JMS Policies

In the case where our product is going to be used to generate a security assertion, we added the ability to authenticate each message at runtime. The system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity. The identity can be used in the processing to generate a WS-Security and/or SAML assertion representing that authentication event. This is a proprietary mechanism because the JMS specification does not have any provision for passing credentials and identity information.

An ideal architecture of course would be the receipt of a standards based security assertion such as a WS-Security token, but since many clients are not capable of generating these we offer this service.

Network Policy Overview Screen - Terms for JBOSS JMS Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in JBOSS JMS policies.

TERM	DEFINITION
Name	The identifier for this JBOSS JMS policy.
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. <p>JBOSS JMS policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the JBOSS JMS Server
Other	The URI of the JBOSS JMS Server

JBOSS JMS Policy Wizard Terms and Options

The following table displays all the terms and options in the JBOSS JMS Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the JBOSS JMS Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this JBOSS JMSPolicy.
Server URL	The URL and Port of the JBOSS JMSserver.
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none">• Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage.• Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded Messages sent via the JMS Bytes binary message format.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the JBOSS JMSGroup on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none">• With Requires SSL checked, the message is processed via SSL.• With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message.

TERM	OPTIONS AVAILABLE
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier. • If unchecked, the message will not be authenticated.
ACL Policy	With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Template Name	The error handling template selected to capture a returned, unprocessed message.

JBOSS JMSPolicies Examples

Examples for JBOSS JMS policies include:

- Add a JBOSS JMS Listener policy with or without SSL.
- Add a JBOSS JMS Remote policy with or without SSL.

JBOSS JMS Policy with SSL Prerequisites

Follow the listed sequence to create a JBOSS JMS policy with SSL:

1. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
2. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
3. Create a JBOSS JMS policy that refers to the SSL policy.

SUN JAVA MQ POLICIES

SUN MQ Enterprise Messaging Service (SUN JAVA MQ) is a JMS based messaging product that is used to guarantee delivery of messages throughout an enterprise. The SUN JAVA MQ architecture relies on the use of a SUN JAVA MQ server that sits between clients to coordinate the sending and receiving of data. Used with the system, SUN JAVA MQ policies work with and without SSL and can leverage the patented on-board crypto acceleration of the Sentry product. In addition, Sentry supports both the point to point messaging model and the publish / subscribe messaging model available in JMS.

To support authentication and access control of individual users, Sentry provides a simple user/password based access control paradigm, and of course we support the full range of WS-Security and SAML standards for authentication. The identity established during the authentication event can be used to support access control of services as well.

Since many different kinds of messages can be sent over the SUN JAVA MQ infrastructure, Sentry supports a flexible mechanism for retrieving and placing Messages into JMS based messages. Sentry has complete support for JMS based messages including JMSBytesMessages, JMSTextMessages and JMSMapMessages. Further, Sentry can mix any of those types for inbound traffic or for sending the message outbound. Forum Sentry uses the JMS ClientAcknowledgement mode to explicitly acknowledge a message or recover a session.

The Network Policies screen displays existing policies, port settings and policy parameters that listeners map to on the system.

You may also mix protocols with SUN JAVA MQ policies. To mix protocols, simply choose a different protocol for the listener or remote policy type and Sentry will automatically mix protocols as messages are processed.

The system provides the following for SUN JAVA MQ policies:

- Supports plaintext and SSL-based communication.
- Supports persistent and non-persistent message delivery.
- Supports synchronous and asynchronous communication modes.
- Includes a simple “wizard” based configuration system.
- Supports point to point and publish/subscribe messaging models.

Simple Authentication with SUN JAVA MQ Policies

In the case where our product is going to be used to generate a security assertion, we added the ability to authenticate each message at runtime. The system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity. The identity can be used in the processing to generate a WS-Security and/or SAML assertion representing that authentication event. This is a proprietary mechanism because the JMS specification does not have any provision for passing credentials and identity information.

An ideal architecture of course would be the receipt of a standards based security assertion such as a WS-Security token, but since many clients are not capable of generating these we offer this service.

Network Policy Overview Screen - Terms for SUN JAVA MQ Policies

The Network Policies screen includes a listing of all existing Network policies. The following table describes each term and definition for the categories displayed in SUN JAVA MQ policies.

TERM	DEFINITION
Name	The identifier for this SUN JAVA MQ policy.
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. <p>SUN JAVA MQ policies are automatically enabled upon creation when the network topology option matches the Network policy.</p>
Protocol	The protocol that is supported by this policy.
Listener Address	The URI of the SUN JAVA MQ Server
Other	The URI of the SUN JAVA MQ Server

SUN JAVA MQ Policy Wizard Terms and Options

The following table displays all the terms and options in the SUN JAVA MQ Policy Wizard that appear under the Policy Selections section of the screen. Because each Network policy is unique, you will not encounter every term or option, and the sequence in which terms appear in the Policy Wizard may vary. After the Policy Wizard has captured these configuration options, they are visible in the SUN JAVA MQ Policy details screen:

TERM	OPTIONS AVAILABLE
Policy Name	The identifier for this SUN JAVA MQ Policy.
Hostname	The target SUN JAVA MQ server.
Port	Static or Dynamic Port to use for SUN JAVA MQ Server
Destination Type	Destination Type may be a Topic or Queue.
Destination	The unique name to identify the queue or topic.
Delivery Mode	<p>Delivery Mode is used to specify the balance between message reliability and throughput.</p> <ul style="list-style-type: none">• Non-Persistent means that messages are delivered in an “at most once” fashion. It is the lowest overhead delivery mode because it does not require persistent storage.• Persistent means the message will be delivered in a “once and only once” fashion. It instructs the messaging infrastructure to write the message at the Queue Manager and send an acknowledgement to the client.
Message Type	Message Types values are JMS Text Messages, JMS Map Messages and JMS Bytes Messages. These correspond to JMS message types that are appropriate for carrying XML data. JMS Bytes Messages contain UTF-8 encoded Messages sent via the JMS Bytes binary message format.
Field	Field is only used for a map message to describe the field that contains the SOAP message.
User ID	Used to explicitly specify the user that the client should run as. The user should be part of the JBOSS JMS Group on the target machine.
Password	The password that corresponds to the User ID entered.
Requires SSL	<ul style="list-style-type: none">• With Requires SSL checked, the message is processed via SSL.• With Requires SSL unchecked, the message is processed without SSL.
SSL Initiation Policy	With the Requires SSL option checked, the SSL Initiation policy to apply to this message.

TERM	OPTIONS AVAILABLE
Authenticate Message	<ul style="list-style-type: none"> • If checked, the message will be authenticated against the User ID and Password supplied earlier. • If unchecked, the message will not be authenticated.
ACL Policy	With Require Authentication checked, the ACL Policy screen appears. The ACL Policy drop down defines the access control policy in the same way that it can be specified for HTTP based protocols. It can be used to authorize access to the listener
Synchronous Policy	<ul style="list-style-type: none"> • Synchronous Mode (with Synchronous Policy checked) means that error messages will be returned to their source. • Asynchronous mode (with Synchronous Policy unchecked) means that error messages are placed in an error queue.
Template Name	The error handling template selected to capture a returned, unprocessed message.

SUN JAVA MQ Policies Examples

Examples for SUN JAVA MQ policies include:

- Add a SUN JAVA MQ Listener policy with or without SSL.
- Add a SUN JAVA MQ Remote policy with or without SSL.

SUN JAVA MQ Policy with SSL Prerequisites

Follow the listed sequence to create a SUN JAVA MQ policy with SSL:

4. Create a key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
5. Create an SSL policy that refers to the key pair. Refer to the *Forum Systems Sentry™ Version 9.1 Security Policies and PKI Guide* for more information.
6. Create a SUN JAVA MQ policy that refers to the SSL policy.

SMTP POLICIES

An SMTP policy encapsulates the configuration needed to proxy SMTP. The Network policies screen manages SMTP listener and SMTP remote policies, their settings and status in the system. You may create, edit, delete, disable and enable SMTP policies.

Network Policies Overview Screen – SMTP Policies Screen Terms

The following table describes each term and definition for the categories displayed above.

TERM	DEFINITION
Name	The identifier for this Network policy.
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. <p>Network policies are automatically enabled upon creation.</p>
Protocol	The protocol that is supported by this Network policy; SMTP.
Listener Address	The IP address of the system
Other	The IP address of the back end Server.
Authentication	This version of the product does not support SMTP Authentication. Use Client IP restriction instead.

SMTP Listener Policy

An SMTP Listener policy defines a listener IP/port used as an SMTP “gateway”, which can accept incoming SMTP traffic, and an IP ACL policy to apply to this listener. The IP ACL policy is a global Access Control List policy that filters IP ranges that are allowed or denied on the listener.

SMTP Remote Policy

An SMTP Remote policy defines a policy configuration which proxies SMTP traffic to a back-end server, an SMTP relay, gateway, or delivery system for traffic through the system.

SMTP Response Policy

An SMTP Response policy is a specific type of SMTP remote policy which is used to send responses back to the client.

SMTP Architecture

Email is sent via the SMTP protocol, but in the contemporary Internet, it is usually not delivered to the recipient via SMTP. Instead, an email message travels through a chain of SMTP relays or gateways to a

mail server, where it then sits, waiting for the recipient to retrieve it. This final retrieval to the recipient's inbox uses a different protocol – usually POP3 or IMAP.

Typical Email Delivery Architecture

The following graphic displays a typical email delivery scenario for home or office configurations, to provide a comparison with the Forum proxy setup in the Typical SMTP Architecture with a Forum Sentry section:

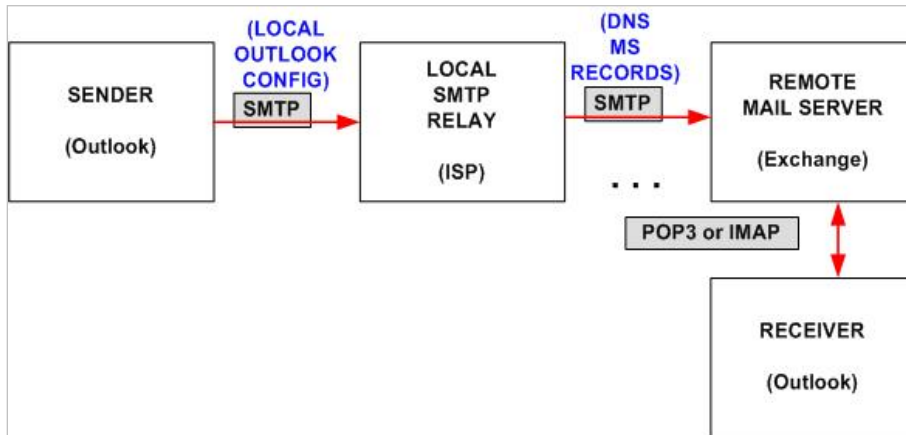


Figure 3: Sample Typical Email Delivery Architecture.

Because SMTP is essentially a one-way protocol, detailed error messages must be sent via a separate SMTP transaction, as configured in an SMTP Response Policy.

Typical SMTP Architecture with Forum Sentry

In the following graphic, the mail transfer agent program “sendmail” is shown as the sender. It is difficult to test an SMTP architecture using a GUI mail user agent such as Outlook because many such GUI programs do not provide the ability to change the content-type of the message.

While it is possible to configure the system to ignore an invalid content-type by disabling the “Invalid HTTP Message” IDP Rule, the remote web service will reject the request for having an invalid content-type. Normal email messages have a content-type of “text/plain” or “text/html” or “multipart/alternative”; however, most web services expect a content-type of “text/xml”.

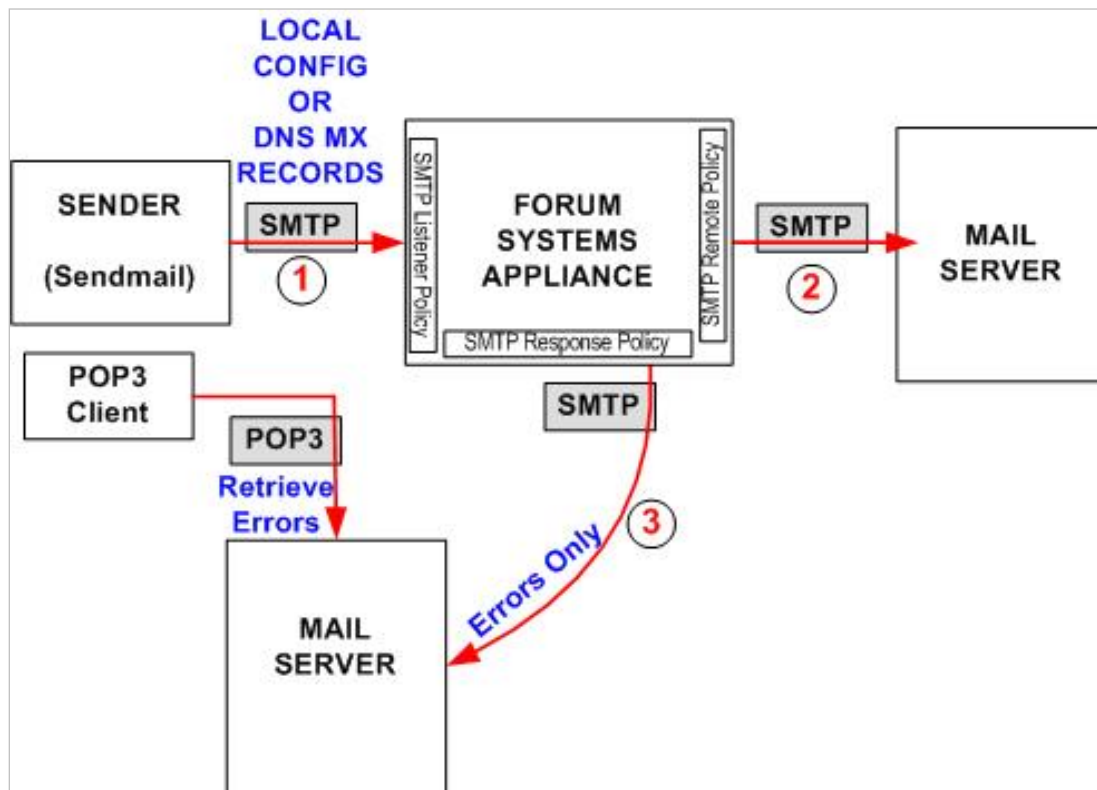


Figure 4: Sample Typical SMTP Architecture with a Forum Appliance.

SMTP Policies and Protocol Mixing

With SMTP policies, Administrators can mix protocols with other supported protocols on the system simply by associating the inbound (listener) or outbound (remote) policy independent of the protocol type of the policy. This association will trigger Sentry to perform the protocol mixing in real-time as message pass through.

The following graphic displays one scenario for protocol mixing on the system with SMTP policies:

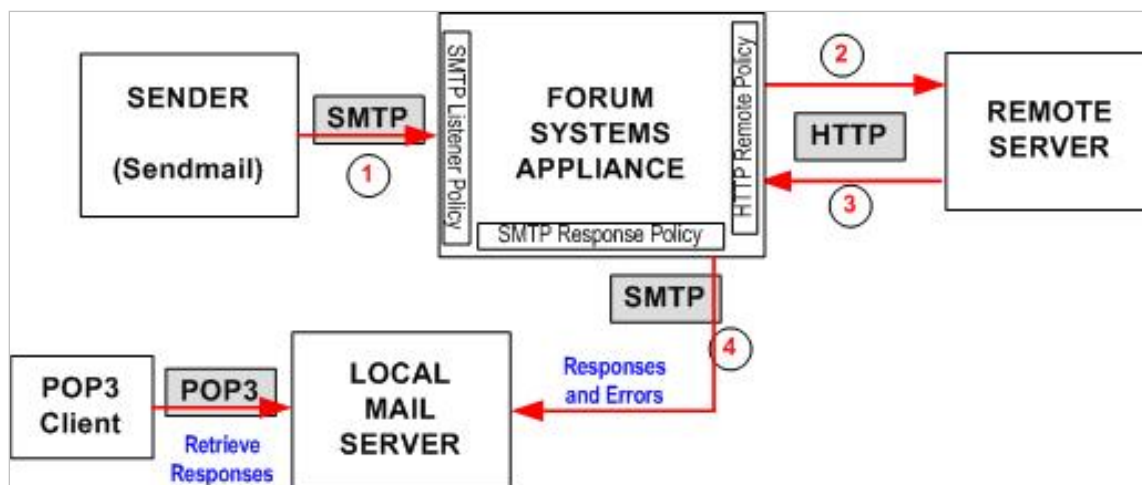


Figure 5: One Scenario for Protocol-Mixing with SMTP Policies.

Transmission Protocols Supported

SMTP policies use the SMTP transmission protocol.

SMTP Policy Wizard

The SMTP Policy Wizard guides Administrators through a series of configuration details to provide local and / or remote connection points for the system as well as configuring the type of protocol and access control.

SMTP Policy Examples

Examples for SMTP policies include:

- Add both SMTP Listener and Response Policies.
- Add an SMTP Listener Policy.
- Add an SMTP Remote Policy for SMTP Only.
- Add an SMTP Remote Policy for Protocol Mixing.
- Add an SMTP Remote Policy for SMTP Listener Policy Response.

SMTP Listener Policy Terms

The following table displays all the terms and options in the SMTP Listener Policy Wizard. Because each SMTP policy is unique, Administrators will not encounter every term or option, and the sequence in which terms appear in the SMTP Listener Policy Wizard may vary. After the Wizard has captured these configuration options, they are visible in the Network policy details screen:

TERM	DEFINITION
Policy Name	The identifier for this listener policy.
IP ACL Policy	The identified for the IP ACL policy associated with this SMTP listener policy.
Appliance Listener	<ul style="list-style-type: none">• With Use Device IP checked, the SMTP listener will always use the device IP address. This setting is useful for transferring policy configurations from one machine to another.• With Use Device IP unchecked, the IP of the SMTP listener policy must be configured manually. <p>The Listener IP is the IP address the system will receive SMTP messages on.</p> <p>The Listener Port is the TCP port the system will receive SMTP messages on.</p>
Response Handling	The name of the SMTP Remote policy that will deliver response messages via SMTP.
Error Handling	From the drop down list, select an Error Template to apply to this Network policy.

SMTP Remote Policy Terms

The following table displays all the terms and options in the SMTP Remote Policy Wizard. Because each SMTP policy is unique, Administrators will not encounter every term or option, and the sequence in which terms appear in the SMTP Remote Policy Wizard may vary. After the Wizard has captured these configuration options, they are visible in the Network policy details screen:

TERM	OPTIONS AVAILABLE
Policy Usage Type	Policy types include: <ul style="list-style-type: none">• Policy will be the remote side of an SMTP to SMTP proxy.• Policy will be the remote side of a non-SMTP to SMTP (protocol mixing) proxy.• Policy that will be used for SMTP Listener policy responses.
Policy Name	The identifier for this remote policy.
Remote Server	The IP address of the back end SMTP server.
Remote Port	The TCP port of the back end SMTP server.
From Address	The From Address field is used to set the "From" SMTP header field of the outgoing message.
To Address	The To Address field is used to set the "To" SMTP header field of the outgoing message.
Subject	The Subject field is used to set the "Subject" SMTP header field of the outgoing message.

FTP POLICIES

An FTP policy provides the means to intercept and proxy FTP transactions seamlessly between a client and a back-end FTP server. These types of policies also have comprehensive support for FTP security including SSL tunnel security for FTPS transactions and OpenPGP key support for encryption, decryption, verification, and signing policies to enable security functions on FTP data as it is streamed from the client to the back-end FTP server. User policies can be set up to map OpenPGP keys and policies based on the identified user such that the security and behavior is dynamic per the logged in user.

FTPS, SFTP, and OpenPGP Security

FTP policies are described in full detail in a separate document from the documentation set. For more information about FTP, FTPs, sFTP, and OpenPGP Policies, please refer to the *Forum Sentry 9.1 FTP OpenPGP Guide*.

GROUP REMOTE POLICIES

A Group Remote policy is a collection of Remote network policies that provides failover for redundancy in the case of a remote server failure and can optionally use one of several strategies for remote load balancing. They might be associated with a WSDL or XML policy.

Group Remote Failover Behavior

All Group Remote policies, regardless of the load balancing strategy they use, include failover functionality that works as follows:

- The list of policies available for a Group Remote policy to send client requests to initially include all the Remote policies configured for the Group Remote policy. From this list are removed all Remote policies which have been manually disabled via the WebAdmin. Also removed from the list are all the Remote policies which are known to be inaccessible.
- The Group Remote Policy discovers that a Remote policy is inaccessible only after the policy is chosen for use by a client request and cannot be reached. If the Remote policy is reachable but returns an error, it is still considered to be accessible - only an unreachable Remote policy is removed from consideration. Once a Remote policy is discovered to be inaccessible and removed from the list, the Group Remote policy will begin trying to connect to the remote server of the Remote policy in the background, with a retry delay as configured in the Group Remote policy. The Remote policy will be returned to the list once it can be reached to process requests.
- Once all the disabled and inaccessible Remote policies have been removed, the list contains only eligible Remote policies. The Group Remote policy's strategy chooses a single Remote policy from among the eligible policies to send each client request to.

Load Balancing Strategies with Group Remote Policies

The load balancing strategies available on the system for a Group Remote Network policy include:

PASSIVE LOAD BALANCING STRATEGIES	ADAPTIVE LOAD BALANCING STRATEGIES
<ul style="list-style-type: none">• Failover• Round Robin• Random• Weighted Random• Document Size	<ul style="list-style-type: none">• Transfer Throughput• Active Requests• Response Time

Passive strategies choose a Remote policy without reference to the traffic passing through the system. Adaptive strategies gather statistics about current and past traffic passing through the system and choose a remote server based on the traffic patterns."

Failover Strategy

The Failover strategy uses the order of the configured Remote policies to signify priority. It always chooses the first Remote policy from the list of eligible Remote policies. In other words, it always chooses the first Remote policy unless it is disabled or inaccessible, in which case it moves to the second, etc.

Round Robin Strategy

The Round Robin strategy initially chooses an eligible Remote policy at random and then rotates through the list of eligible Remote policies in order, choosing the next eligible Remote policy for each new client request.

Random Strategy

The Random strategy chooses an eligible Remote policy at random for each new client request.

Document Size Strategy

The Document Size strategy chooses an eligible Remote policy based on the size of the request and the max size configured for each Remote policy. Only eligible policies with a max size configured larger than the request are chosen. If the request is larger than any of the configured max size in all of the Remote policies, the Remote policy with the largest max size is chosen.

Transfer Throughput Strategy

The Transfer Throughput strategy chooses the highest performing eligible Remote policy. Performance is measured by the average transfer throughput of the last 100 requests, in bits per second.

Active Requests Strategy

The Active Requests strategy chooses the eligible Remote policy which is the least busy, based on the number of concurrent requests the Remote policy is servicing.

Weighted Random Strategy

The Weighted Random strategy chooses an eligible Remote policy at random for each new client request, using the relative weights configured for each Remote policy. The configured weights set the relative odds that each Remote policy will be selected if eligible. For example:

If all Remote policies are configured with the same weight, they are all equally likely to be selected and the Weighted Random strategy is equivalent to the Random strategy. 2:1 odds can be configured by giving a weight of 2-to-1 policy and 1 to another policy. With this configuration, 2/3 of incoming requests will be routed to the first policy and 1/3 to the second policy.

REMOTE POLICIES		
<input type="checkbox"/> CONTAINS POLICIES		WEIGHT
<input type="checkbox"/> BostonEast-Remote	11.11.11.19:8091	<input type="text" value="2"/>
<input type="checkbox"/> Kerberos1500-Remote	11.11.11.40:8048	<input type="text" value="1"/>
<input type="button" value="Remove"/>		
<input type="checkbox"/> REMAINING POLICIES		
<input type="checkbox"/> ChunkTest1	11.11.11.11:80	
<input type="checkbox"/> ChunkTest2	11.11.11.11:443	
<input type="checkbox"/> ChunkTest3	11.11.11.11:80	
<input type="checkbox"/> Cust_FS_WSDL-Remote	10.5.6.115:8015	
<input type="checkbox"/> GoogleSearch-Remote	api.google.com:8000	
<input type="checkbox"/> HoustonRemote	11.11.11.71:8071	
<input type="checkbox"/> HttpRemotePolicy_0	11.11.11.33:8033	
<input type="button" value="Add"/>		

Response Time Strategy

The Response Time strategy chooses the highest performing eligible Remote policy, measuring performance by the average response time of the last 100 requests. The Response Time strategy chooses the Remote policy with the lowest average response time.

Group Remote Policies Wizard Terms

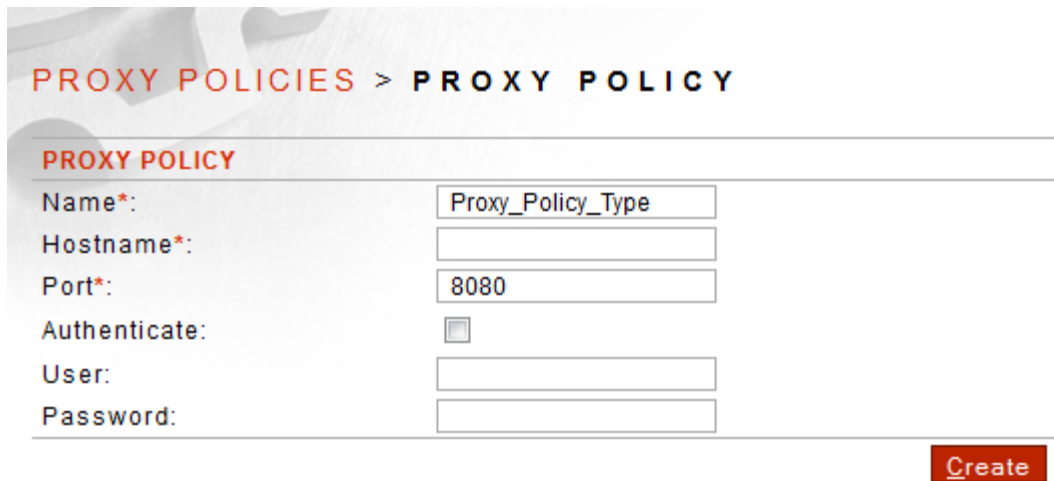
The following table describes terms and definitions in the Group Remote Policy Wizard for both the Group Remote policies wizard and on the Network screen:

TERM	DEFINITION
Policy Name	The identifier for the Group Remote policy.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Red status light = disabled policy. <p>Group Remote policies are automatically enabled upon creation.</p>
Protocol	The protocols supported by the Group Remote policy are. <ul style="list-style-type: none">• HTTP• SMTP• JBOSS JMS• SUN JAVA MQ• IBM Websphere MQ• TIBCO EMS• Apache MQ• BEA WebLogic
Strategy	<ul style="list-style-type: none">• Failover• Round Robin• Random• Transfer Throughput• Active Requests• Weighted Random• Response Time
Weight	For the Weighted Random load balancing strategy option, enter a value for the odds that this Remote Policy will be chosen relative to the odds of other configured Remote policies.
Retry Delay in seconds	The number of seconds that the system should delay in between attempts to contact a Remote policy marked as unavailable.
Contains Policies	A collection of Remote policies of the specified protocol from which the system will select one to use, refer to the section of this document for the strategy of this Group Remote policy.
Active Remote Policy	The Remote policy currently in use by the system to service requests.

PROXY POLICIES

The Proxy policies provide the settings for proxy server(s) that can be set up for remote HTTP policies to use to communicate with the endpoints. Multiple proxy configurations can be defined and include Hostname, port, and authentication credentials.

Defined proxy policies are then consumed by other policies such as HTTP Remote Policies when a proxy server is required to communicate with the end point.



The screenshot shows a web interface for configuring a proxy policy. At the top, there is a breadcrumb navigation: "PROXY POLICIES > PROXY POLICY". Below this is a section titled "PROXY POLICY" with a form containing the following fields:

- Name*: Proxy_Policy_Type
- Hostname*: (empty)
- Port*: 8080
- Authenticate:
- User: (empty)
- Password: (empty)

A red "Create" button is located at the bottom right of the form.

Proxy Policy Details Screen Terms

FIELD NAME	DEFINITION
Name	The name of the Proxy policy.
Hostname	The target proxy server IP or hostname
Port	The target port on the proxy which should be used to communicate.
Authenticate	Proxy authentication can be enabled or disabled.
User	If Authenticate setting is enabled, this field is the username to use to authenticate to the target proxy server
Password	If Authenticate setting is enabled, this field is the password to use to authenticate to the target proxy server

Global Proxy System Setting

The Proxy Settings section on the System Settings screen allows a global definition for an HTTP proxy server that will result in all HTTP outbound requests from Sentry to use the proxy setting, with the exception of the bypass settings configured.

ERROR TEMPLATES

Error handling template allows Administrators to customize the content and HTTP error code that is returned when errors occur while processing a client request. Administrators may also customize the formatted error to reflect meaningful and precise error faults for the Administrators who must maintain network logs. Subsequently, HTTP policies may be set to include system or custom templates which capture and report these exceptions to the client.

Templates are associated with Network policies. Each Network policy may have one error handling template associated with it. Error Templates include the following major components:

- Default Format
- SOAP Fault Detail Format
- SOAP Header Fault Detail Format

Administrative actions for Error Templates include:

- add / edit / delete / rename a Template
- associate a system or custom Template with a Network policy
- restore default Templates while retaining any custom-added Templates

Error Template Details Screen Terms

FIELD NAME	DEFINITION
Template Name	The identifier for the Error Template policy.
Default Error Code	The default error code which the server returns when a request fails. If unsure of which Error Code to use, Forum Systems recommends using 500.
Default Format	A text box where the HTTP or XML content of the error may be added, edited, cut or pasted. Used for all errors that are not specified to be SOAP faults, i.e., the "virtual directory not found" error.
SOAP Fault Detail Format	A text box where the SOAP Fault Detail content of the error may be added, edited, cut or pasted. This format specifies the content of the SOAP fault detail element for faults pertaining to the SOAP Body that are generated locally on the system.
SOAP Header Fault Detail Format	A text box where the SOAP Header Fault Detail content of the error may be added, edited, cut or pasted. This format specifies a SOAP header for faults pertaining to the SOAP Header that are generated locally on the system.

Replacement Variables in Templates

The following table displays the replacement variables found in Error Templates. These variables will be replaced with their dynamic values for each template substitution event that occurs on each transaction.

VARIABLE NAME	REPLACEMENT
%abortmsg%	The custom error message displayed when the error is triggered from an IDP Rule violation. This custom error message is returned to the client, not the Administrator. For more information, refer to the Add an IDP Rule Policy with a Custom Error Message section of other <i>Forum Systems Sentry™ Version 9.1 IDP Rules Guide</i> .
%attr.<attribute name>%	The value of the session attribute. In the example %attr.sessionnum%, the attribute name is sessionnum. The attribute name can be a defined attribute on a Map Attribute to XML task, a Map Attribute from XML task or it can be a user attribute.
%date%	The date (year, month and day) displayed when the Task generated the error.
%datetime%	The date (year, month and day) and time (hour, minute and second) displayed when the Task generated the error.
%errorcode%	The error code returned by the server or a system error matched to an HTTP error code.
%errormsg%	The detailed error message displayed when the error is triggered.
%policy%	The policy name that generated the error.
%sysname%	The name of the system. This name is added in the Network screen or through the network config name command from the CLI. <div style="background-color: yellow; border: 1px solid black; padding: 2px;">Note: If a System Name (found on the Network screen) has not been added, then the default template will display the %sysname% tag as blank.</div>
%task%	The name of the Task that generated the error.
%tasklist%	The name of the Task List that generated the error.
%time%	The time (hour, minute and second) displayed when the Task generated the error.
%transaction%	The document ID of the request.
%username%	The user name for the user that generated the error.

Overview of the Attribute Replacement Variable

Most replacement variables are pre-defined and have fixed names. However, the syntax %attr% creates a user-defined replacement variable which is replaced at run-time by the value of a session attribute. Session attributes can be created from XML content using a Task List with the Map XML task.

System Error Templates

The system Error Templates that reside on the product may not be deleted. They include:

- Default Template
- SOAP 1.1 Fault Template
- SOAP 1.2 Fault Template
- XML Template

Each of these templates provides a different formatted response to the client. Select a template based on the client.

The Default Template

The Default Template is used as a starting point for custom error templates created on the system. It is also the template selected by default when creating a new Listener policy. In its system default state, the Default Template has a Default Format for returning general errors as HTML documents, SOAP Fault Detail Format and SOAP Header Fault Detail Format; all of which add useful detail information to SOAP faults returned by the system. To view the Default Template, from the **Templates** screen, either:

- Click the **Default** Template name link, or
- Select **New**.

Note: Any new error templates created are based on the Default Template. Selecting **New** on the **Templates** screen opens a pre-populated template ready to be renamed and edited.

The SOAP 1.1 Fault Template

The SOAP 1.1 Fault Template is the template assigned by default to SOAP 1.1 ports in WSDL policies created on the system, as well as to HTTP Listener policies auto-created for SOAP 1.1 ports by the WSDL Policy Wizard. In its system default state, the SOAP 1.1 Fault Template has a Default Format that returns errors as valid SOAP 1.1 faults; thus ensuring that all errors returned to clients of network policies are valid SOAP faults. This template also has a SOAP Fault Detail Format and SOAP Header Fault Detail Format which are identical to those of the Default Template in its system default state.

The SOAP 1.2 Fault Template

The SOAP 1.2 Fault Template is the template assigned by default to SOAP 1.2 ports in WSDL policies created on the system, as well as to HTTP Listener policies auto-created for SOAP 1.2 ports by the WSDL Policy Wizard. In its system default state, the SOAP 1.2 Fault Template has a Default Format that returns errors as valid SOAP 1.2 faults; thus ensuring that all errors returned to clients of network policies are valid SOAP faults. This template also has a SOAP Fault Detail Format and SOAP Header Fault Detail Format which are identical to those of the Default Template in its system default state.

The XML Template

The XML template can be used to return errors as a simple XML document. It is an example of what a custom error template for an XML policy might look like. To view the XML template, from the **Templates** screen, click on the **XML Template** name link.

Error Template Examples

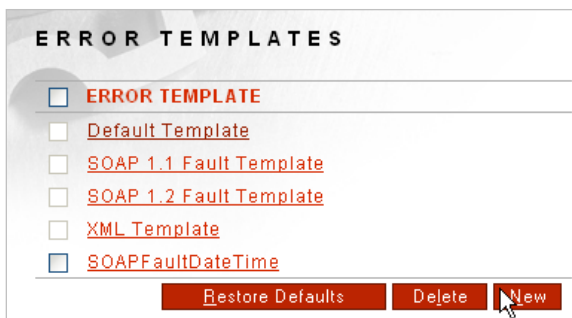
The example for Templates includes:

- Add an Error Template.

Note: Restore default system Error Templates by selecting **Restore Defaults**. All system Templates are restored back to their original factory state while any added Templates are retained.

Add an Error Template

Follow these steps to create an Error Template. This operation starts creating a new Template, making modifications and saving it.



ERROR TEMPLATES > ERROR TEMPLATE DETAILS

ERROR TEMPLATE DETAILS

Template Name*:

Default Error Code*:

Default Format:

```
<fs:Error xmlns:fs="http://www.forumsystems.com/2004/04/error">
  <fs:Message>%abortmsg%</fs:Message>
  <fs:SystemName>%sysname%</fs:SystemName>
  <fs:User>%username%</fs:User>
  <fs:Policy>%policy%</fs:Policy>
  <fs:TaskList>%tasklist%</fs:TaskList>
  <fs:Task>%task%</fs:Task>
  <my:SessionId xmlns:my="http://my.company.com/2004/04/error">%
attr.SessionId%</my:SessionId>
</fs:Error>
```

SOAP Fault Detail Format:

```
<fs:Detail
xmlns:fs="http://www.forumsystems.com/2004/04/soap-fault-detail">
  <fs:SystemName>%sysname%</fs:SystemName>
  <fs:User>%username%</fs:User>
  <fs:Policy>%policy%</fs:Policy>
  <fs:TaskList>%tasklist%</fs:TaskList>
  <fs:Task>%task%</fs:Task>
</fs:Detail>
```

SOAP Header Fault Detail Format:

```
<fs:FaultDetail
xmlns:fs="http://www.forumsystems.com/2004/04/soap-fault-detail">
  <fs:SystemName>%sysname%</fs:SystemName>
  <fs:User>%username%</fs:User>
  <fs:Policy>%policy%</fs:Policy>
  <fs:TaskList>%tasklist%</fs:TaskList>
  <fs:Task>%task%</fs:Task>
</fs:FaultDetail>
```

- From the Navigator, select the **Templates** screen.
- Select **New**.
- On the ERROR TEMPLATE DETAILS screen, in the Template Name field, enter a **Template name**.
- In the Default Error Code field, enter an **HTTP Error Code**. This example uses **500**.
- In the Default Format text box, make any desired modifications. This instruction adds the following content:

```
<my:SessionId xmlns:my="http://my.company.com/2004/04/error">%attr.SessionId%</my:SessionId>
```

- In the SOAP Fault Detail Format text box, make any desired modifications.
- In the SOAP Header Fault Detail Format text box, make any desired modifications.
- Click

Save.

- %abortmsg%, 68
- ACLPolicy
 - ORACLE JMS, 29, 33
 - Tibco-EMS, 25, 37, 51, 55
- ACLs
 - about Allow All, 6
 - referenced in an HTTP/S policy, 4
- Active Remote Policy for Group Remote policy, 65
- Active Requests strategy for load balancing, 64
- add Error Templates, 70
- associate ACL for Password Auth to HTTP policy, 10
- associate Error Template to HTTP policy, 10
- Authenticate Message
 - MQ, 20
 - ORACLE JMS, 29, 32
 - Tibco-EMS, 25, 37, 51, 55
- Backout Requeue Name, 14
- Channel
 - MQ, 19
- contains policies for Group Remote policy, 65
- conventions used, 1
- default error code, 67
- default format, 67
- Delivery Mode
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- Delivery Modes
 - MQ, 20
- Destination
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- Destination Type
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- dynamnic auth mode, 7
- Error Handling, 6
- Error Handling template
 - MQ, 20
- Error Handling Template
 - MQ, 20
- error template name, 12, 66, 67
- Error Template variable
 - % attr.<attribute name>%, 68
- Error Templates, 6, 60
 - examples, 70
- Failover strategy for load balancing, 63
- field
 - MQ, 19
- Field
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- From Address, 61
- Group Remote policy, 63
- Group Remote Policy Wizard terms, 65
- Host
 - MQ, 19
- HTTP policy
 - adding HTTP listener policy, 10
 - adding HTTP remote policy, 10
- HTTP policy screen terms, 4
- HTTP Policy Wizard terms and options for HTTP Listener policy, 5
- HTTP Policy Wizard terms and options for HTTP Remote policy, 7
- HTTP/S policy
 - examples in Wizard, 9
- inbound protocol options, 5
- IP ACL policy name associated with HTTP/S listener, 5
- IP ACL policy name associated with SMTP listener, 60
- JMSBytesMessages, 14
- JMSMapMessages, 14
- JMSReplyTo header, 16
- JMSTextMessages, 14
- listener address for an MQ policy, 15
- listener address for HTTP/S policy, 4
- listener address for SMTP policy, 56
- listener IP, 5, 60
- listener Port, 5, 60
- Message Type
 - MQ, 19
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- MQ
 - asynchronous mode, 15
 - synchronous mode, 15
- MQ Message Format
 - MQ, 19
- MQ policies
 - examples, 17
- MQ policy
 - fs_user, 17, 22, 34, 48, 52
- MQ Policy Wizard terms and options, 19
- MQRFH2
 - MQ, 19
- MQSTR
 - MQ, 19
- network Listener policy, 2
- Network Policies screen terms for MQ policies, 15
- network Remote policy, 2
- Non-Persistent delivery mode, 20
- ORACLE JMS
 - JMS Map Messages, 28, 32
 - Non-Persistent delivery mode, 28, 32
 - Persistent delivery mode, 28, 32
 - User ID, 28, 32

- ORACLE JMS policies
 - examples, 29
- ORACLE JMS policy terms, 27, 31
- ORACLE JMS policy with SSL
 - prerequisites, 29
- outbound protocol options, 7
- Password
 - MQ, 19
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- Password Authentication Access Control, 6
- Password Authentication Realm, 5
- Persistent delivery mode, 20
- policy name, 7
- Policy Name
 - MQ, 19
 - ORACLE JMS, 28, 32
 - Tibco-EMS, 24, 36, 50, 54
- policy name for Group Remote policy, 65
- policy name for ORACLE JMS policy, 27, 31
- policy name for Tibco-EMS policy, 23, 35, 41, 43, 49, 53
- Policy will be the remote side of a non-SMTP to SMTP proxy (protocol mixing), 61
- Policy will be the remote side of an SMTP to SMTP proxy, 61
- Policy will be used for SMTP Listener Policy response, 61
- Port
 - MQ, 19
- Process Response
 - MQ, 20
- propagate basic auth, 7
- protocol for Group Remote Network policy, 65
- protocol for MQ policy, 15
- protocol for ORACLE JMS policy, 27, 31
- protocol for SMTP policy, 56
- protocol for Tibco-EMS policy, 23, 35, 41, 43, 49, 53
- Queue
 - MQ, 19
- Queue Manager
 - MQ, 19
- Random strategy for load balancing, 64
- remote address for an MQ policy, 15
- Remote address for HTTP/S policy, 4
- remote address for SMTP policy, 56
- Remote Authentication, 7
- Remote Policy terms for SMTP policies, 61
- remote port, 7
- Remote server, 61
- Remote Server, 7
- replacement variable
 - Attribute, 68
- Reply Message Types
 - MQ, 21
- Reply Queue Type
 - Named reply queue
 - MQ, 21
- Require Password Authentication, 5
- Requires SSL
 - MQ, 19
 - ORACLE JMS, 28
 - Tibco-EMS, 24, 36, 50, 54
- Response handling, 60
- response processing, 8
- Response Time strategy for load balancing, 64
- retry delay in seconds for Group Remote policy, 65
- Round Robin strategy for load balancing, 63
- Server URL
 - ORACLE JMS, 28
 - Tibco-EMS, 24, 36, 50, 54
- SMTP Listener policy, 56
- SMTP Listener Policy terms, 60
- SMTP policy
 - examples, 59
- SMTP policy screen terms, 56
- SMTP Policy terms, 61
- SMTP Remote policy, 56
- SMTP Response policy, 56
- SOAP 1.2 Fault Template, 70
- SOAP Fault Detail format, 67
- SOAP Header Fault Detail format, 67
- specify basic auth, 7, 8
- SSL Cipher Specifications
 - MQ, 19
- SSL Initiation policy, 8
- SSL Initiation Policy, 20
 - MQ, 19
 - ORACLE JMS, 28
 - Tibco-EMS, 24, 36, 50, 54
- SSL Termination policy, 6
- status for Group Remote policy, 65
- status of a Network policy, 15
- status of a ORACLE JMS policy, 27, 31
- status of a Tibco-EMS policy, 23, 35, 41, 43, 49, 53
- status of HTTP/S Network policy, 4
- status of SMTP policy, 56
- strategy for Group Remote policy, 65
- Subject, 61
- synchronous mode, 16
- Synchronous mode
 - MQ, 20
- Synchronous Policy
 - ORACLE JMS, 29, 33
 - Tibco-EMS, 25, 37, 51, 55
- Synchronous Timeout, 20
- system Error Templates, 69
- System SSL Termination, 6
- TCP Timeouts

- connect timeout, 7
- read timeout, 7
- Template Name
 - ORACLE JMS, 29, 33
 - Tibco-EMS, 25, 37, 46, 51, 55
- the Default Template, 69
- the SOAP 1.1 Fault Template, 70
- the XML Template, 70
- Tibco/ EMS Policy Wizard terms and options,
 - 24, 28, 32, 36, 45, 50, 54
- Tibco-EMS
 - JMS Map Messages, 24, 36, 50, 54
 - Non-Persistent delivery mode, 24, 36, 50, 54
 - Persistent delivery mode, 24, 36, 50, 54
 - User ID, 24, 36, 50, 54
- Tibco-EMS policies
 - examples, 25, 38, 47, 51, 55
 - Tibco-EMS policy terms, 23, 35, 40, 43, 49, 53
 - Tibco-EMS policy with SSL
 - prerequisites, 25, 38, 51, 55
 - To Address, 61
 - Transfer Throughput strategy for load balancing,
 - 64
 - Use Basic Authentication, 5
 - Use Cookie Authentication, 5
 - Use Device IP, 5
 - Use Digest Authentication, 5
 - User ID, 19
 - User Policy, 8
 - weight value for Group Remote policy, 65
 - Weighted Random strategy for load balancing,
 - 64