

# FORUM SYSTEMS SENTRY VERSION 9.1 IDP RULES 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<sup>™</sup> Firmware, Forum Systems XMLSec<sup>™</sup> WebAdmin, Forum Systems XML Security Appliance<sup>™</sup>, Forum Sentry<sup>™</sup>, Forum Presidio<sup>™</sup>, Forum XWall<sup>™</sup>, Forum Sentry<sup>™</sup> Web Services Gateway, Forum Systems Sentry Security Token Service®, Forum Presidio<sup>™</sup> OpenPGP Gateway, Forum FIA Gateway<sup>™</sup>, Forum XWall Type-PCI<sup>™</sup>, Forum XWall® Web Services Firewall and Forum XRay<sup>™</sup> 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 Systems Sentry Version 9.1 IDP Rules Guide, published July 2020.

D-ASF-SE-018779

### **Table of Contents**

INTRODUCTION TO THE IDP GUIDES GUIDE	1
IDP RULES	2
The IDP Rule Policies Examples	12
Add an IDP Rule Policy	13
Add an IDP Rule Policy with a Custom Error Message	14
IDP GROUPS	16
IDP Groups Overview	16
The IDP Groups Examples	19
Add an IDP Group Policy	20
Add or Remove IDP Rules in an IDP Group Policy	21
IDP ACTIONS	23
IDP Actions Overview	23
The IDP Action Policies Examples	27
Add an IDP Action Policy	27
IDP SCHEDULES	
IDP Schedules Overview	
The IDP Schedules Examples	
Add an IDP Schedule Policy	
IDP BLOCKING	
IDP Blocking Overview	
The IDP Blocking Examples	
View IDP Blocking or Throttling Details	
Remove IDP Blocking or Throttling Restriction	
IDP Config – Aggregate IDP Across Multiple Sentry Instances	35
IDP Config Overview	
IDP Config Configuration	35

# List of Figures

Figure 1:	IDP Rules and Consequences to Document Processing	8
Figure 2:	Example 1 of Enforcement Settings between an IDP Rule and an IDP Action.	9
Figure 3:	Example 2 of Enforcement Settings Betwen an IDP Rule and an IDP Action.	10

# INTRODUCTION TO THE IDP GUIDES GUIDE

# Audience for the IDP Rules Guide

The Forum Systems Sentry Version 9.1 IDP Rules Guide is for System Administrators who will manage:

- Intrusion Detection and Prevention (IDP) Rule policies.
- IDP Group policies.
- IDP Action policies.
- IDP Schedule policies to restrict the time frame where an IDP Rule applies.
- IDP Rule violations by user, IP, or IDP Group that are blocked, or whose access is being throttled.
- IDP Config.

# **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 API Security Gateway is referred to as the 'device', 'product' or 'system'.

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

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

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

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

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

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

are not shown. For more information, refer to the Common Operations section of the Forum Systems Sentry Version 9.1 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.

# **IDP RULES**

# **IDP Rules Overview**

IDP Rules use IDP Actions to indicate what to do when the IDP Rule is triggered. The IDP Schedule is used to indicate when it is valid to trigger the IDP Rule. An IDP Group is a collection of IDP Rules.

Intrusion Detection and Prevention (IDP) Rules allow users to customize filtering and exception handling of network and data processing. In the event of an exception, the corresponding IDP Rule determines the correct course of action (e.g. log to an external quarantine database and send an email alert).

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

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

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

# **IDP Rules and Definitions**

The following table displays the IDP Rules and their definitions, with references to which IDP Rules are defaults on the system, and which have applicable Value and Period properties:

RULE	DEFINITION	VALUE	PERIOD
Attempted XML External URI Reference	The product does not allow external URI references in incoming XML documents. Any requests containing an external reference will always cause a failure.	Ν	Ν
Authentication failed #	Used for managing invalid credentials provided on a request.	Ν	Ν
Document does not match any message type filter #	Used when the request does not match any of the request filters configured for the Virtual Directory.	Ν	Ν
Document does not match any WSDL message #	Used when the message of the incoming SOAP request cannot be determined. This can be caused because the request is not a valid SOAP or it contains a message not defined in the WSDL file for the WSDL policy.	Ν	Ν

RULE	DEFINITION	VALUE	PERIOD
Document does not match any document identification task #	Used for requests which do not match any of the document identification tasks.	Ν	Ν
Document processing error #	Used for any type of error during the transaction.	N	N
Firewall rule violation	Used for WAF rule policy violation	Ν	Ν
Maximum attachment count	Used for maximum number of attachments allowed.	Y Max number of attachments	Ν
Maximum byte count (in bytes, KB, MB or GB)	Used for maximum byte count allowed for the SOAP messages or XML documents. The system cumulatively adds the byte count of processed requests and when reaching the value set, triggers the rule. The rule continues to be triggered as more requests are processed through the system until the specified period of time expires, or the rule is disabled.	Y Max cumulative byte count in selected unit	Y Rule is triggered for this period of time
Maximum document count	Used for maximum number of documents allowed.	Y Max number of documents	Y Rule is triggered for this period of time
Maximum element children	Used for maximum number of children per node in an XML document allowed.	Y Max number of children	N
Maximum element count	Used for maximum number of elements per XML document allowed.	Y Max number of elements	Ν
Maximum element depth	Used for maximum depth of elements allowed in an XML document.	Y Max depth of document	Ν
Maximum failed user login attempts	Used for maximum login attempts.	Y Max number of attempts	Y Rule is triggered for this period of time
Maximum internal reference expansion	Used to limit the number of XML entity references an XML document can have.	Ν	Ν

Maximum payload size (in bytes, KB,MG or GB)	Used for maximum request or response payload size, including XML document and all attachments.	Y Max size of payload in selected unit	Ν
Maximum response time	Used for maximum time to wait on a response from the remote server.	Y Max number in milliseconds	Ν
Maximum Scanning Depth	Used for maximum zip levels. How many times a document/documents in question have been zipped not the number of zip files in each zip	Y Max number of elements	Ν
Maximum XML document size (in bytes, KB, MB or GB) #	Used for maximum XML document size (including SOAP requests) allowed. This also applies to all documents including non-XML.	Y Max size of XML document in selected unit	Ν
Maximum zip payload size (in bytes, KB, MB or GB)	Used for maximum ZIP document size	Y Max size of ZIP document in selected unit	Ν
Minimum document size (in bytes, KB, MB or GB)	Used for minimum document size allowed.	Y Min size of document in selected unit	Ν
New operation	Used for tracking first time usage of WSDL operations.	Ν	Ν
New client IP address	Used for tracking the first time a request comes from a specific IP address.	Ν	Ν
New user	Used for tracking the first time a user accesses the system.	Ν	Ν
Pattern Match Policy Violation	Used to detect when a Pattern Policy is associated with a Pattern Match task, and the Policy has ALLOW/DENY configuration setting enabled.	Ν	Ν
SOAP Fault does not match any WSDL message	Used for detecting SOAP faults received that are not recognized in a WSDL.	Ν	Ν
SOAP Fault received from remote	Used for detecting any SOAP fault received in a response.	Ν	Ν
Unauthorized user	Used for detecting a user whose credentials are valid but lacks necessary permissions. The permissions are granted by an authorization call	Ν	Ν

	to an external ide Execute permission	ntity server and by the ACL on.		
Virus found	Used for detecting available only with	g a virus in a document, n licensed anti-virus plug-in.	Ν	Ν
Y = Applicable	N = Not Applicable	# = Default IDP Rule		

# **IDP Rule Screen Terms**

The following table describes each term and definition for the IDP Rule screen.

DETECTION SETTINGS           IDP Rule Name         The name for this IDP Rule policy.           Description         Description of this IDP Rule.           Criterion         The IDP metric used to track and enforce the IDP Rule.           THRESHOLD         Value           Value         Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.           Period         Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.           ENFORCEMENT SETTINGS         The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.           Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identify servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Group should not be confused with IDP Groups.           Enforce By IP         When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.           Enforce By User         When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IVsr.           IDP Action         The sel	TERM	DEFINITION
IDP Rule Name         The name for this IDP Rule policy.           Description         Description of this IDP Rule.           Criterion         The IDP metric used to track and enforce the IDP Rule. <b>THRESHOLD</b> Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.           Period         Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Veriod. <b>ENFORCEMENT SETTINGS</b> Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list. <b>INSET Note:</b> The User Group referenced by the Enforce only User Group poption is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SMMPMonitor and SMMPTech groups are the only exception. User Groups should not be confused with IDP Groups.           Enforce By IP         When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP. <b>IDP ACTION</b> The selected IDP Action policy used by this IDP Rule.           Abort Message         Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal erro	DETECTION SETTI	NGS
Description         Description of this IDP Rule.           Criterion         The IDP metric used to track and enforce the IDP Rule. <b>THRESHOLD</b> Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.           Period         Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period. <b>ENFORCEMENT SETTINGS</b> Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list. <b>Note:</b> The User Group of the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.           Enforce By IP         When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.           Enforce By User         When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending User.           IDP ACTION         IDP Action are applied only to the offending User.           IDP ACtion         The selected IDP Action policy used by this IDP Rule.           Abort Message         Used to add a custom error message when the %abortmsg% fi	IDP Rule Name	The name for this IDP Rule policy.
Criterion       The IDP metric used to track and enforce the IDP Rule.         THRESHOLD         Value       Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.         Period       Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.         ENFORCEMENT SETTINGS       The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.         Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups.         Enforce By IP       When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.         Enforce By User       When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.         IDP Action       The selected IDP Action policy used by this IDP Rule.         Abort Message       Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message	Description	Description of this IDP Rule.
THRESHOLD         Value       Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.         Period       Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.         ENFORCEMENT SETTINGS       The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.         Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.         Enforce By IP       When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.         Enforce By User       When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.         IDP ACtion       The selected IDP Action policy used by this IDP Rule.         Abort Message       Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.	Criterion	The IDP metric used to track and enforce the IDP Rule.
Value       Where applicable, this field contains the limit for the selected criteria. Not all IDP         Rules require a Value.       Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.         ENFORCEMENT SETTINGS       Enforce only on         The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.         Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups.         Enforce By IP       When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.         Enforce By User       When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.         IDP ACTION       IDP Action The selected IDP Action policy used by this IDP Rule.         Abort Message       Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.         IDP Schedule       The selecte	THRESHOLD	
Period       Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.         ENFORCEMENT SETTINGS       The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.         Note: The User Group referenced by the Enforce only user Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.         Enforce By IP       When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.         Enforce By User       When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.         Enforce By User       When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.         IDP Action       The selected IDP Action policy used by this IDP Rule.         Abort Message       Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the	Value	Where applicable, this field contains the limit for the selected criteria. Not all IDP Rules require a Value.
ENFORCEMENT SETTINGS           Enforce only on User Group         The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.           Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.           Enforce By IP         When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.           Enforce By User         When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.           IDP ACTION         The selected IDP Action policy used by this IDP Rule.           Abort Message         Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.           IDP Schedule         The selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	Period	Where applicable, this field specifies the period over which the value statistics are accumulated. The period may be a second, a minute, an hour or a day. Not all IDP Rules require a Period.
Enforce only on User GroupThe Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.Note: The User Group referenced by the Enforce only User Group option is any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.Enforce By IPWhen checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.Enforce By UserWhen checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.IDP ACTIONThe selected IDP Action policy used by this IDP Rule.Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP ScheduleThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	ENFORCEMENT SE	ETTINGS
any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.Enforce By IPWhen checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.Enforce By UserWhen checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.IDP ACTIONIDP Actions are applied only to the offending User.IDP ActionThe selected IDP Action policy used by this IDP Rule.Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP ScheduleThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	Enforce only on User Group	The Enforce only on User Group option is a filtering mechanism. When checked, it restricts enforcement of this IDP Rule only to the User Group selected from the drop down list.  Note: The User Group referenced by the Enforce only User Group option is
Enforce By IPWhen checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.Enforce By UserWhen checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. 		any user group on the system. This includes groups created for identity servers such as LDAP and SiteMinder. The SNMPMonitor and SNMPTech groups are the only exception. User Groups should not be confused with IDP Groups.
Enforce By UserWhen checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.IDP ACTIONThe selected IDP Action policy used by this IDP Rule.Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP SCHEDULEThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	Enforce By IP	When checked, restricts enforcement of this IDP Rule to the unique IP address which triggered the IDP Rule. The rate criteria are tracked on a per IP basis. IDP Actions are applied only to the offending IP.
IDP ACTIONIDP ActionThe selected IDP Action policy used by this IDP Rule.Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP SCHEDULEIDP ScheduleIDP ScheduleThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	Enforce By User	When checked, restricts enforcement of this IDP Rule only to the unique User who triggered the IDP Rule. The rate criteria are tracked on a per User basis. IDP Actions are applied only to the offending User.
IDP ActionThe selected IDP Action policy used by this IDP Rule.Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP SCHEDULEThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	IDP ACTION	
Abort MessageUsed to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.IDP SCHEDULEThe selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	IDP Action	The selected IDP Action policy used by this IDP Rule.
IDP Schedule       The selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	Abort Message	Used to add a custom error message when the %abortmsg% field is set in an Error Template, this text field provides a custom IDP error message sent in the SOAP response to the client. When no text is entered in the Abort Message field, the normal error message is sent to the Administrator.
IDP Schedule The selected IDP Schedule is used to indicate when the IDP Rule can be triggered.	IDP SCHEDULE	
	IDP Schedule	The selected IDP Schedule is used to indicate when the IDP Rule can be triggered.

# Value-based IDP Rules

The IDP Rules which include value-based data are:

- Maximum attachment count
- Maximum byte count
- Maximum document count
- Maximum payload size
- Maximum XML document size
- Maximum element children
- Maximum element count
- Maximum element depth
- Maximum scanning depth
- Minimum document size

These IDP Rules are managed according to the value(s) indicated in the Value field. All specified data in the value field are integers. When throttling is activated, the resultant throttle threshold value is also an integer (rounded down if necessary).

**Note:** The size rate rules (Maximum payload size, Maximum XML document size, and Minimum document size) convert all values to bytes internally, so a maximum byte count specified as 1 MB would throttle to 512 KB when throttling is set at 50%.

# **Rate-based IDP Rules**

The IDP Rules which include rate-based data (both maximum value, also referred to as threshold value, and time period settings) are:

- Maximum byte count
- Maximum document count

These IDP Rules are managed according to the rate indicated in the Value and Period fields.

### How Rate-based IDP Rules Work

All rate-based IDP Rules (i.e. maximum value and time period) are implemented by maintaining a running counter, comparing it to the maximum value, and then resetting it at the end of the specified time period.

### **Throttling Behavior with Rate-based IDP Rules**

With rate-based IDP Rules, throttling is implemented by multiplying the specified maximum value by the throttle percent and using that as the new, effective maximum value to compare against. Since the maximum value is an integer value, integer math is used in calculating the throttle value (which truncates by default), so:

1 Document / hour throttled at 50% = 0 Documents / hour

This setting would, therefore, have the effect of blocking. If you selected 2 documents per hour, as Figure 1 displays, the throttling allows 1 document per hour to be processed through the system.

# How Sentry Associates Rate-based IDP Rules with Throttling

The following graphic displays an example of rate-based IDP Rules associated with throttling set and its processing consequences. Note in each of the cases below, that throttle values are rounded down to the nearest integer.

#### Throttling 2 documents per Hour at 50% would result in 1 document per hour being processed.

DPFECTION SETTINGS         IDP Rule Name":       MadDocCount         Description:       Criterion:         Criterion:       Maximum document count         THRESHOLD       Period:         Value:       2         Period:       Hour         Period:       Hour         Enforce only on User Oroup:       Steath Mode (do not send a response)         Puture Access Restrictions:       None         Throttling 1 Ouser Oroup:       Steath Mode (do not send a response)         Puture Access Restrictions:       None         Throttling 1 document per       Maximum         DP Action:       Abort         Abort Message:       Walt         DP Schedule:       Anytime         Throttling 1 document per Hour at 50% would result in 0       Value:         Period:       Hour         In reality, all documents per hour at 55% would result       Period:         Hour at 55% would result       Throttlie at 65         Period:       Hour         Period:       Hour         Period:       Hour         Throttling 400 documents per hour at 65% would result 65       %         Period:       Hour         Period:       Hour         Period:<	IDP RULE P	OLICIES > IDP F	
IDP Rule Name*:       MaxDocCount         Description:	DETECTION SETT	INGS	Name*: HayDocCountErrolling0 [7]
Description: Criterion: Maximum document count HRESHOLD Value: 2 KS W Period: Hour w ENFORCEMENT SETTINGS ENFORCEMENT SETTINGS LUT restriction after 50 % Do a naiert Wait © minutes before logging another alert User: Wittle wEdit Wait © minutes before logging another alert User: Wittle wEdit Wait © minutes before issuing another alert DP Schedule: Aunt a 50% would result in 0 documents being processed. Throttling 10 documents per Hour at 55% would result 6 documents per hour being processed. Throttling 400 documents per Hour at 55% would result 200 documents per Hour at 50% would result 200 documents Period: Hour w Hour	IDP Rule Name*:	MaxDocCount	Description:
Criterion:       Maximum document count         THRESHOLD         Value:       2         Period:       Hour         Hour       Image: Strait Mode (do not send a response)         Future Access Restrictions:       None         Period:       Hour         ENFORCEMENT SETTINGS       Image: Throtte at 50 %         Enforce only on User Group:       SNMPMontor         DP Action:       Abort         IDP Action:       Abort         Abort       Massage:         IDP Action:       Abort         Abort       SNUP trap alert         Watt © minutes before issuing another alert       SNUP trap alert         Watt © minutes before issuing another SNMP trap alert         IDP Schedule:       Arytime         IDP Schedule:       Arytime         IDP Schedule:       Arytime         IDP Schedule:       Arytime         IDP Schedule:       Immutes before issuing another SNMP trap alert         Watte:       Immutes before issuing another SNMP trap alert         Watte:       Immutes before issuing another SNMP trap alert         IDP Schedule:       Arytime         IDP conting 10 documents       Immutes before issuing another SNMP trap alert         Walue: <t< th=""><th>Description:</th><th></th><th></th></t<>	Description:		
Image: Interesting 1 documents per Hour at 50% would result in 0 documents per hour at 55% would result 200 documents per hour at 55% would result 200 documents per hour at 50% would result 200 documents per h	Criterion:	Maximum desument	PREVENTION SETTINGS
THRESHOLD         Value:         2         Period:         Hour         Period:         Hour         ENFORCEMENT SETTINOS         Enforce only on User Oroup:         SNMPMontor         Enforce By IP         Enforce By User         IDP Action:         Abort         Abort         Abort         Message:         IDP Schedule:         Arytime         In reality, all document per Hour at 50% would behave as if blocked.         Value:       1         Value:       1         Period:       Hour         In reality, all documents per Hour at 55% would result 6 documents per hour being processed.       Throttle at 65         Throttling 400 documents per Hour at 55% would result 200 documents per hour being processed.       Value:         Yalue:       400	Cinterion.	Maximum document coun	t Abort processing of the document
Value:       2       None         Period:       Hour       Image: The state of t	THRESHOLD		Future Access Restrictions:
Period: Hour   Hour Hour   ENFORCEMENT SETTINGS Block   Enforce only on User Group: SNMPMonitor   Enforce By IP Enforce By User   DP Action: Abort   Mathematical Software Watt © minutes before logging another alert   Watt © minutes before sending another alert Send an alert   User: Kittle with   Mathematical Watt Immates before issuing another alert   Watt © minutes before issuing another SNMP trap alert   Mathematical Watt Mathemati	Value:	2 KB V	O None
ENFORCEMENT SETTINGS   Enforce only on User Group: SNMPMonitor   Enforce By IP   Enforce By User   IDP ACTION   IDP Action:   Abort   Abort Message:   IDP Schedule:   Arytime ♥    Throttling 1 document per Hour at 50% would result in 0 documents per hour at 55% would result at 655 %   Throttling 10 documents per hour being processed.  Value:  Period:  Hour I 100 %   Hour I 100 %   Throttling 10 documents per hour at 50% would result at 50 %   Throttling 10 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %   Throttling 400 documents per hour at 50% would result at 50 %	Period:	Hour	Throttle at 50 %
ENFORCEMENT SETTINGS   □ Enforce only on User Group: SNMPMonitor   □ Enforce By IP   □ Enforce By User   IDP ACTION   IDP ACTION   IDP Action:   Abort   Abort Message:   IDP Schedule:   Arrytime ✓   Throttling 1 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 10 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttling 400 documents per Hour at 50% would result in 0 for biog processed. Throttle at 50 %		Hou	OBlock
Enforce only on User Group: SNMPMonitor Enforce By IP Enforce By User IDP Action: Abort Abort Abort Abort Abort Abort Abort Abort Abort Comments per Hour at 50% would result in 0 Gocuments per Hour at 65% would behave as if blocked. Value: 10 / Value:	ENFORCEMENT S	ETTINGS	Lift restriction after 60 minutes
Enforce By IP Enforce By User IDP ACTION IDP ACTION IDP ACTION IDP Action: Abort Abort Message: User IDP Schedule: Anytime w IDP Schedule: Anytime w IDP Schedule: Anytime w In reality, all document per processed. In reality, all documents being processed. In reality, all documents per hour at 55% would result 6 documents per hour at 50% would result 6 documents per hour at 55% would result 6 documents per hour at 50% would result 6 documents per hour at 50% would result 6 documents per hour at 50% would result 200 documents per hour being processed.	Enforce only (	on User Group: SNMPMo	nitor ALERTS
□ Enforce By User   □ DP ACTION   IDP Action:   Abort   Abort Message:   □ DP Schedule:   Anytime v    Throttling 1 document per Hour at 50% would result in 0 documents being processed.    In reality, all document processing would behave as if blocked.     Value:   100 Frottle at 50     Value:   100 Frottling 10 documents per Hour at 65% would result 6 documents per hour being processed.      Value:   100 Frottle at 65     Value:   100 Frottle at 50   100 Throttling 400 documents per Hour at 50% would result 200 documents per H	Enforce By IP		☑ Log an alert
Interest of over   IDP Action   IDP Action:   Abort   Abort Message:     IDP Schedule:   IDP Schedule:     Anytime     Value:   IDP Schedule:     IDP Schedule:     IDP Schedule:     IDP Schedule:     Anytime     Value:     IDP Schedule:     In reality, all documents   per Hour at 65% would   result 6 documents   per Hour at 50% would   result 200 documents   per Hour at 50% would </th <th></th> <th>-</th> <th>Wait 0 minutes before logging another alert</th>		-	Wait 0 minutes before logging another alert
IDP Action       User: kittle ♥ Edit         IDP Action:       Abort         Abort Message:       SNMP trap alert         IDP Schedule:       Anytime ♥         In reality, all document per Hour at 50% would result in 0 ♥       ♥         In reality, all documents per Hour at 65% would result 6 documents per hour being processed.       ●         In reality, all documents per hour at 65% would result 20 documents per Hour at 50% would result 200 documents per Hour at 50% would result 200 documents per Hour baing norcessed       ●         In rottling 400 documents per hour baing norcessed       ●       ●         In rottling 40	Emorce By Us	201	Send an alert
IDP Action: Abort   Abort Message:     Wait: 0 minutes before sending another alert     SNMP trap alert     Wait: 0 minutes before issuing another SNMP trap alert     IDP SCHEDULE   IDP Schedule: Anytime v     Throttling 1 document per   Hour at 50% would result in 0   documents being processed.   In reality, all document   processing would behave as   if blocked.     Value:   10   Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     minutes before issuing another SNMP trap alert     Wait: 0     Throttling 1 documents   per Hour at 65% would   result 6 documents   per Hour at 50% would   result 200 documents pe	IDP ACTION		User: klittle v <u>Edit</u>
Abort Message: Wait O minutes before issuing another SNMP trap alert Wait O minutes before issuing another SNMP trap alert Nor Streeoute IDP Schedule: Anytime V Throttling 1 document per Hour at 50% would result in 0 documents being processed. In reality, all document processing would behave as if blocked. Throttling 10 documents per Hour at 65% would result 6 documents per hour being processed. Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed. Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed. Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed. Throttle at 50 %	IDP Action:	Abort	Wait: 0 minutes before sending another alert
IDP Schedule:       Anytime v         Throttling 1 document per Hour at 50% would result in 0 documents being processed.       Value: 1	Abort Message:		Wait 0 minutes before issuing another SNMP tran alert
IDP Schedule:       Anytime ✓         Throttling 1 document per Hour at 50% would result in 0 documents being processed.       Value:       1         In reality, all document processing would behave as if blocked.       ✓alue:       1         Throttling 10 documents per Hour at 65% would result 6 documents per hour being processed.       Image:       10         ✓alue:       10       ✓e         ✓alue:       10       ✓e         ✓eriod:       Hour       ✓e         ✓alue:       400       ✓e         ✓eriod:       Hour       ✓e         ✓alue:       400       ✓e         ✓eriod:       Hour       ✓e         ✓alue:       400       ✓e         ✓eriod:       Hour       ✓e         ✓eriod:       Hour       ✓e         ✓eriod:       Hour       ✓         ✓eriod:       Hour       ✓         ✓eriod:       Hour       ✓ <th>-</th> <th></th> <th>there is a second to be any under the map alert</th>	-		there is a second to be any under the map alert
IDP Schedule:       Anytime •         Throttling 1 document per       Yalue:       1         Hour at 50% would result in 0       •       1         documents being processed.       Image: Period:       Hour •         In reality, all document       •       Throttle at 50       %         processing would behave as       •       Throttle at 50       %         Throttling 10 documents       •       Throttle at 50       %         Period:       Hour •       •       Throttle at 65       %         Throttling 10 documents       •       Throttle at 65       %         Throttling 400 documents       •       Throttle at 65       %         Throttling 400 documents       •       Throttle at 65       %         Throttling 400 documents       •       Throttle at 65       %	IDP SCHEDULE		
Throttling 1 document per         Hour at 50% would result in 0         documents being processed.         In reality, all document         processing would behave as         if blocked.             Throttling 10 documents         period:         Hour         Main             In reality, all document         processing would behave as         if blocked.             In reality, all documents         period:       Hour         In rottle at 65       %	IDP Schedule:	Anytime	×
Throttling 10 documents per Hour at 65% would result 6 documents per hour being processed. Throttle at 65 Walue: 10 Period: Hour S Throttle at 65 Walue: 400 Value: 400 Value	Throttling Hour at 5 documen In reality processin if blocked	g 1 document per i0% would result in 0 its being processed. , all document ng would behave as d.	Value: 1 KB Period: Hour Throttle at 50 %
Throttling 10 documents per Hour at 65% would result 6 documents per hour being processed. Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed			Value:
Throttling 400 documents per hour being processed. Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed Value: 400 KB Period: Hour Sol %	Throttling	10 documents	Period: Hour W
result 6 documents per hour being processed.       Image: Throttle at 65 %         Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed       Value: 400 KB Value: 400	per Hour a	at 65% would	HOUT M
Throttling 400 documents per Hour at 50% would result 200 documents per bour being processed.	result 6 de	ocuments per	Throttle at 65 %
Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed	hour bein	g processed.	
Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed			
Throttling 400 documents per Hour at 50% would result 200 documents per hour being processed S Throttle at 50 %			Value: 400 KB 🗸
per Hour at 50% would result 200 documents per hour being processed	Throttlin	g 400 documents	Period: Hour 🐋
result 200 documents per <ul> <li>Throttle at 50 %</li> </ul>	per Hour	at 50% would	
	result 20	0 documents per	Throttle at 50 %

Figure 1: IDP Rules and Consequences to Document Processing

How Sentry Manages Enforcement Settings on IDP Rules - Example 1 The following two graphics display enforcement settings on an IDP Rule:

IDP	Action P	olicy (B	Block-NoLifting)	Associated with
the	IDP Rule	Policy	(MaxDoccount_	NoEnforce)

IDP ACTION		
Name*:	Block-NoLifting	
Description:		
PREVENTION	SETTINGS	Blocking can only be
Abort pro	cessing of the document	or by a WebAdmin
Steal	th Mode (do not send a response)	assigned to a Domain
Future Ac	cess Restrictions:	that grants access to IDP Blocking) from the IDP
	e	Blocking screen.
○ Thro	ttle at 50 %	
Bloc	k	Notice that Lifting this Blocking action is not
🗆 Lift r	estriction after 60 minutes	selected since the Lift restriction after <i>nn</i>
ALERTS		minutes is unchecked,
🗹 Log an al	ert	and no value is entered.
Wait 0	minutes before logging another alert	
🗹 Send an :	alert	
User: m	arysmith 🗸 Edit	
Wait: 0	minutes before sending another alert	
SNMP tra	p alert	
Wait 0	minutes before issuing another SNMP tra	p alert
Wait 0	minutes before issuing another SNMP trap al	ert

Figure 2: Example 1 of Enforcement Settings between an IDP Rule and an IDP Action.

# How Sentry Manages Enforcement Settings on IDP Rules - Example 2



Figure 3: Example 2 of Enforcement Settings Betwen an IDP Rule and an IDP Action.

# **Restrictive Configurations for Enforcement Settings**

The following hypothetical scenarios describe examples of enforcement settings for an IDP Rule:

# Scenario 1 - Less Restrictive Configuration for Enforcement Settings

A less restrictive configuration for enforcement settings on an IDP Rule would be:

- MaxDocCount is 100 an Hour
- Enforce by IP is checked
- Enforce by User is checked
- IDP Action is Abort
- Schedule is Anytime

Requests are received by the system from:

- 15 unique IPs
- 50 unique Users

The actual policy request (or policy response) associated with this IDP Rule allows:

- Every IP (15) X 100 docs per hour = 1500 requests could be processed before the IDP Rule is triggered.
- Each User (50) X 100 docs per hour = 5000 requests could be processed before the IDP Rule is triggered.

**Caution:** In the case where both the Enforce by IP and Enforce by User checkboxes are checked, it is the combination of both unique IPs and unique users that is tracked.

In all probability, the restriction on the Enforce by IP will be hit before the restriction on the Enforce by users because it is a combination of IPs and users that is being restricted.

When a document comes into the system within an hour that exceeds the quota allowed for either an authenticated IP or authenticated User, then this IDP Rule is triggered, and all further document processing received from this unique IP (or unique User) is aborted. No further requests from this unique IP or unique user will be processed until the IDP Action is lifted.

# Scenario 2 - More Restrictive Configuration for Enforcement Settings

A more restrictive configuration for enforcement settings on an IDP Rule would be:

- MaxDocCount is 100 an Hour
- Enforce only on Group is unchecked
- Enforce by User is unchecked
- Enforce by IP is unchecked
- IDP Action is Abort
- Schedule is Anytime

When the 101<sup>st</sup> document comes into the system within an hour from any IP and any User, the Rule is triggered. Processing of the 101<sup>st</sup> document and all subsequent documents received within this hour is aborted.

# **Scenario 3 - Selective Restrictive Configuration for Enforcement Settings**

IDP Rules can be selectively enforced by checking the "Enforce only on Group" option and selecting an appropriate Group on which to enforce the IDP Rule. A selective restrictive configuration for enforcement settings on an IDP Rule would be:

- MaxDocCount is 100 an Hour
- Enforce only on Group is checked
- A user Group is selected from the drop down list
- IDP Action is Abort
- Schedule is Anytime

Because the Enforce only on user group option is a filtering mechanism, only traffic from the group is analyzed by this IDP Rule. When the 101st document comes into the system within an hour (all 100 previous documents originated from members of the selected group), the Rule is triggered and processing is aborted. Documents coming into the system from any other users not in the specified group are not affected.

# **IDP Rule Policies Examples**

### The IDP Rule Policies Examples

Examples for IDP Rule policies include:

- Add an IDP Rule policy.
- Add an IDP Rule policy with a Custom Error Message.

# Add an IDP Rule Policy

Follow these steps to add an IDP Rule policy:

DETECTION SETTI	NGS
IDP Rule Name*:	DocProcessError_reqRule
Description:	
Criterion:	Document processing error
THRESHOLD	
Value: 0	КВ 🗸
Period: S	econd v
ENFORCEMENT SE	TTINGS
Enforce only o	n user group: Vendors 🗸 Edit
Enforce by IP	
Enforce by use	er
IDP ACTION	
IDP Action:	MalformedDocReceived 👽 Edit
Abort Message:	
IDP SCHEDULE	

- From the Navigator, select the **Rules** screen. In the IDP Rule Name field, enter a **name** for this IDP Rule.
- In the Description field, enter a **description** for this IDP Rule (optional).
- In the Criterion drop down list, select the **criteria** for this IDP Rule.
- Skip the Value and Period fields. These settings are not appropriate for this rule.
- From the ENFORCEMENT SETTINGS section, check the **Enforce only on User Group** checkbox. From the drop-down list, select a **Group name**.
- Skip the Enforce By IP and Enforce By User checkboxes.
- From the IDP ACTION section, aligned with IDP Action, select an action that should occur if this IDP Rule is triggered.
- Skip the Abort Message field.
- From the IDP SCHEDULE section, aligned with IDP Schedule, select the schedule that this action will follow if this IDP Rule is triggered.
- Click Create.

# Add an IDP Rule Policy with a Custom Error Message

This instruction assumes you have created an Error Template and defined a custom Error Message using the **%abortmsg%** replacement value. For more information, refer to the Error Handling Templates section of the *Forum Systems Sentry Version 9.1 Network Policies Guide.* 

Add an IDP Rule policy with a custom Error Message in the same manner shown in Add an IDP Rule Policy with these additional steps:

- In the Abort Message field, enter the **text** of the custom message.
- From the IDP SCHEDULE section, aligned with IDP Schedule, select the schedule that this action will follow if this IDP Rule is triggered.
- Click Create.

**Note:** Now that you have created an IDP Rule policy that includes a custom error message, you must also associate it with a WSDL policy to be active.

# **Constraints of IDP Rule Policies**

ELEMENT	CONSTRAINTS	CHARACTER COUNT
IDP Rule name	Unique and case sensitive. Accepts equal signs, the "@" character, dashes, underscores and spaces.	1-80
Abort Message	Must be alphanumeric characters and may include equal signs, the "@" character, dashes, underscores and spaces.	0-80

# **Specifications of IDP Rule Policies**

ELEMENT SUPPORTED	SPECIFICATIONS
IDP Rule policies	Unlimited

**Database Dictionary for Quarantine Tables** The following tables list common database terms, definitions and conventions used in the Quarantine database.

TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
QRTN_DOC			Quarantine documents
	ID	NUMBER(16)	Record key (sequence)
	CLIENTIP	VARCHAR2(16)	Client IP address
	CLIENTPORT	NUMBER(10)	Client port number
	CLIENTUSERNAME	VARCHAR2(32)	Client user name
	DOCUMENT	BLOB	XML message
	RESPONSE	BLOB	Web Server Response
	PROJECT	VARCHAR2(80)	Name of WSDL or XML Policy on device
TABLE NAME	FIELD NAME	DATA TYPE	DESCRIPTION
QRTN_SENSC	R		Quarantine document IDP fault information
	ID	NUMBER(16)	Record Key (sequence)
	IDPCRITERION	VARCHAR2(80)	Intrusion Detection & Prevention (IDP) rule that was triggered
	LOGTS	DATE	Device system date
	IDPLIMIT	VARCHAR2(16)	Threshold set in the IDP rule
	IDPPERIOD	VARCHAR2(100)	Duration set in the IDP rule
	RESPONSE	VARCHAR(1)	Indicates whether the information belongs to a request or a response. If it is a request it is "N" and "Y" for responses

# **IDP GROUPS**

# **IDP Groups Overview**

An IDP Group is a collection of individual IDP Rules providing a global method of applying and reusing IDP Rules.

# **Group Types**

The types of IDP Groups available are:

- WSDL Policy
- WSDL Operation
- XML Policy
- JSON Policy
- REST Policy
- HTML Policy

# **Default IDP Groups**

Default IDP Groups on the system apply IDP Rules on the following levels:

- System Group (global-level group rules are global across all policies).
- Default WSDL Policy Group (mid-level group rules are set at the WSDL Policy level and apply to all the operations in that WSDL Policy).
- Default Operation Group (most granular-level group rules are set at the individual operation level for a specified WSDL Policy).
- Default XML Policy Group (mid-level group rules are set at the XML Policy Level and apply to all request in that XML Policy)
- Default JSON Policy Group (mid-level group rules are set at the JSON Policy Level and apply to all request in that JSON Policy)
- Default REST Policy Group (mid-level group rules are set at the REST Policy Level and apply to all request in that REST Policy)
- Default HTML Policy Group (mid-level group rules are set at the HTML Policy Level and apply to all request in that HTML Policy)

Each applicable group acts on every request and response that comes into the system.

### **Reset the Default IDP Groups**

Superusers may reset any of the default IDP to its default factory state by selecting the **default IDP Group name link** from the IDP GROUP POLICIES screen. On the IDP GROUP DETAILS screen, select **Reset**.

# The System Group

The System Group may reference any IDP Rule and acts on every request and response that is processed by the system. The System Group is not explicitly associated with any policy. It is applied globally to all transactions.

There is only one System Group. It comes pre-loaded on the system, cannot be deleted, and is editable only to superusers of the system.

### The Default WSDL Policy Group

The Default WSDL Policy Group may reference any IDP Rule and acts on every WSDL policy that is processed by the system. There is only one Default WSDL Policy Group. It comes pre-loaded on the

system, and cannot be deleted. However, the IDP Rules associated with the Default WSDL Policy Group can be edited.

When you create a new WSDL policy, the IDP Rules tab will, by default, associate this policy with the Default WSDL Policy Group in the IDP Group field. Administrators may associate another IDP Group to this WSDL policy at any time.

# IDP Groups of the Type WSDL Policy

An IDP Group of the type WSDL Policy may be created to apply to all operations defined in a WSDL policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to WSDL message requests, responses or both.

# The Default Operation Group

The Default Operation Group may reference any IDP Rule and acts on every WSDL operation request and response that is processed by the system. There is only one Default Operation Group. It comes preloaded on the system, and cannot be deleted. However, the IDP Rules associated with the Default Operation Group can be edited.

Every operation in the new WSDL policy is also associated, by default, with the Default WSDL Operation Group. The Default WSDL Operation Group does not contain any IDP Rules. Administrators may add IDP Rules to this group whenever appropriate.

### IDP Groups of the Type WSDL Operation

An IDP Group of the type WSDL Operation may be created to apply to specific operations defined in a WSDL policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to the request message, the response message or both.

### The Default XML Policy Group

The Default XML Policy group may reference any IDP Rule and act on every XML request and response that is processed by the system. There is only one Default XML Policy Group. It comes pre-loaded on the system, and cannot be deleted. However, the IDP Rules associated with the Default XML Policy group can be edited.

### IDP Group of the Type XML Policy

An IDP Group of the type XML Policy may be created to apply to all operations defined in an XML Policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to all XML requests, responses, or both.

When you create a new XML policy, the IDP Rules tab will, by default, associate this policy with the Default XML Policy Group in the IDP Group field. Administrators may associate another IDP Group to this XML policy at any time.

### The Default JSON Policy Group

The Default JSON Policy group may reference any IDP Rule and act on every JSON request and response that is processed by the system. There is only one Default JSON Policy Group. It comes preloaded on the system, and cannot be deleted. However, the IDP Rules associated with the Default JSON Policy group can be edited.

# IDP Group of the Type JSON Policy

An IDP Group of the type JSON Policy may be created to apply to all operations defined in an JSON Policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to all JSON requests, responses, or both.

When you create a new JSON policy, the IDP Rules tab will, by default, associate this policy with the Default JSON Policy Group in the IDP Group field. Administrators may associate another IDP Group to this JSON policy at any time.

# The Default REST Policy Group

The Default REST Policy group may reference any IDP Rule and act on every REST request and response that is processed by the system. There is only one Default REST Policy Group. It comes preloaded on the system, and cannot be deleted. However, the IDP Rules associated with the Default REST Policy group can be edited.

### IDP Group of the Type REST Policy

An IDP Group of the type REST Policy may be created to apply to all operations defined in an REST Policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to all REST requests, responses, or both.

When you create a new REST policy, the IDP Rules tab will, by default, associate this policy with the Default REST Policy Group in the IDP Group field. Administrators may associate another IDP Group to this REST policy at any time.

### The Default HTML Policy Group

The Default HTML Policy group may reference any IDP Rule and act on every HTML request and response that is processed by the system. There is only one Default HTML Policy Group. It comes preloaded on the system, and cannot be deleted. However, the IDP Rules associated with the Default HTML Policy group can be edited.

# IDP Group of the Type HTML Policy

An IDP Group of the type HTML Policy may be created to apply to all operations defined in an HTML Policy. IDP Rules referenced by an IDP Group of this type may be configured to apply to all HTML requests, responses, or both.

When you create a new HTML policy, the IDP Rules tab will, by default, associate this policy with the Default HTML Policy Group in the IDP Group field. Administrators may associate another IDP Group to this HTML policy at any time.

# Procedure for Enabling an IDP Group Policy

For an IDP Group policy to function properly, or be fully enabled, Administrators must:

- 1. Create the IDP Group policy.
- 2. Assign one or more IDP Rules to this IDP Group policy.

Associate the IDP Group policy to: a WSDL Policy, XML Policy or WSDL operation.

# **IDP Groups Examples**

# The IDP Groups Examples

Examples for IDP Groups include:

- Add an IDP Group Policy.
- Add / Remove IDP Rules in an IDP Group Policy.

# Add an IDP Group Policy

Follow these steps to add an IDP Group policy:

NEW IDP GROUP	
IDP Group Name:	Chicago Group 11
IDP Group Type:	WSDL Policy

#### IDP GROUP POLICIES > IDP GROUP DETAILS

IDP GROU	P DETAILS							
IDP Grou	Name*:	Chicag	e Group 11					
Descripti	on:							
IDP Grou	o Type:	WSDL	Policy					
REQUEST	RESPONSE	IDP RULE	CRITERION	THRESHOLD	USER GROUP	ENFORCE BY	IDP ACTION	IDP SCHEDULE
-	-	Invalid HTTP Message	Document does not match any message type filter				Abort	Anytime
-	~	Invalid WSDL Message	Document does not match any WSDL message				Abort	Anytime
•	<	Large Pavload	Maximum payload size	25 MB			Abort	<u>Anytime</u>
✓	<	Large XML	Maximum XML document size	10 MB			Abort	Anytime
-	<	Process Error	Document processing error				Abort	Anytime
✓	✓	Virus Detected	Virus found				Abort	<u>Anytime</u>
✓	✓	Authentication Failure	Authentication failed				Abort	Anytime
-	<	Authorization Failure	Unauthorized access				Abort	Anytime
		Max Archive Recursion	Maximum scanning depth	5 levels			Abort	Anytime
		Max Zip Payload	Maximum zip payload size	25 MB			Abort	Anytime
		No Matching XML	Document does not match any XML filter				Abort	Anytime
		WAF Rule Violation	Firewall rule violation				Abort	Anytime

- From the Navigator, select the Groups screen. Select New.
- On the NEW IDP GROUP screen, in the IDP Group Name field, enter a name.
- In the IDP Group Type field, select **WSDL Policy**, then click **Create**.
- Under the REQUEST and RESPONSE columns, check all the **checkboxes** aligned with the default IDP Rules which should apply to WSDL requests and responses, and then click **Save**.

# Add or Remove IDP Rules in an IDP Group Policy

After creating an IDP Group, Administrators must edit the group to add IDP request and / or response rules to the new group. Follow these steps to add an IDP Rule to an IDP Group:

	okeen retries
Syst	em
	NAME
	+ System Group (6)
IDP (	Groups
	Default WSDL Policy Group (8
	■ Default XML Policy Group (8)
	Baltimore Group (6)
	Baltimore Project Group (9)
	_
	🖽 <u>Chicago Group 11 (</u> 8)

IDP GROUP	DETAILS				
IDP Group	Name*:	Chicage Group 11			
Description	1:				
IDP Group	Type:	WSDL Policy			
		Baltimore ProcessError res Rule	Document processing error		
✓		Chicago AuthenticationFailure reg Rule	Authentication failed		
✓		Chicago InvalidHTTPMessage reg Rule	Document does not match any message type filter		
	✓	Chicago InvalidHTTPMessage res Rule	Document does not match any message type filter		
✓		Chicago LargeDocument reg Rule	Maximum payload size	10,240 KB	
	✓	Chicago LargeDocument res Rule	Maximum payload size	10,240 KB	
<					>

- From the Navigator, select the **Groups** screen. Select an **IDP Group name** link.
- On the IDP GROUP DETAILS screen, scroll down to view all IDP Rules currently on the system.
- Check the **checkbox** prefacing each IDP Rule that should be associated with the IDP Group.
- Click Save.

# **Constraints of IDP Group Policies**

ELEMENT	CONSTRAINTS	CHARACTER COUNT
IDP Group policy name	Unique and case sensitive. Accepts equal signs, the "@" character, dashes, underscores and spaces.	1-80

# **Specifications of IDP Group Policies**

ELEMENT SUPPORTED	SPECIFICATIONS
IDP Group policies	Unlimited

# **IDP ACTIONS**

# **IDP** Actions Overview

An IDP Action is a defined behavior that is executed when an IDP rule has been triggered. One IDP Action might be to notify Administrators. Each IDP Rule is associated with one IDP action policy. IDP Action policies also include IDP auditing functionality, which captures IDP data and sends it to a relational database. IDP auditing requires that an Archiving policy exists on the system and is enabled.

# The Default Abort IDP Action Policy

The default Abort IDP Action policy that is pre-loaded on the system aborts processing of the the document and logs and alert. This policy cannot be deleted; however, Administrators may edit it.

# **Alert Handling**

The system provides the following alert actions:

- Log an alert.
- Send an alert.
- SNMP trap alert.

These options are discussed in the IDP Action Detail Screen Terms table.

#### Alert Events

The following table displays the details of an IDP Action alert that are logged, and their descriptions:

LOGGED ITEMS	DESCRIPTION
ld	The sequence number of this IDP event record in the database.
Time of event	The timestamp when the IDP rule triggered.
Time zone of the event	The offset in hours from GMT of the time zone in which the IDP rule triggered.
Source	The WebAdmin IP address and port of the machine where the IDP rule triggered.
User at source of event	The user who triggered the IDP rule.
IP address of source	The source IP address of the user who triggered the IDP rule.
Port at source of event	The source port of the user who triggered the IDP rule.
Status code for event	The HTTP response code before the IDP rule triggered.
IDP Rule	The name of the IDP rule that triggered.
Network Policy	The network listener policy that received the document that triggered the IDP rule.
Criterion	The threshold value of the triggered IDP rule.
Period	The period of the triggered IDP rule.
Value	The value that triggered the IDP rule.
WSDL Port	The WSDL port that received the document that triggered the IDP rule.
WSDL Service	The WSDL service that received the document that triggered the IDP rule.
WSDL Operation	The WSDL operation that received the document that triggered the IDP rule.
WSDL Request	The input message name of the WSDL operation that triggered the IDP rule.
WSDL Response	The output message name of the WSDL operation that triggered the IDP rule.

# **IDP Action Details Screen Terms**

The following table describes each term and definition for the IDP Action details screen in WSDL policies. The Prevention Settings portion of IDP Action policies contains all settings that refer to Intrusion Prevention.

TERM	DEFINITION
IDP ACTION	
Name	The name for this IDP Action policy.
Description	Description of this Action rule.
PREVENTION SETT	INGS
Abort processing of the document	When checked, Abort processing of the document stops any further processing of this request or response.
Stealth mode	When checked, results in no response (silent abort) returned when the IDP rule is triggered.
	<b>Note:</b> Stealth mode is accomplished by closing the connection to the client without sending an error message. For HTTP, this action results in a 200 OK response code sent to the client with no data.
FUTURE ACCESS F	RESTRICTIONS
None	When selected, results in no access restrictions on the associated IDP Rule.
Throttle at <i>nn</i> %	When selected, if the corresponding IDP Rule is triggered by exceeding its specified threshold value, a new threshold value is set for that Rule at <i>nn</i> % of the specified value. For example, if the corresponding IDP Rule set a maximum document count at 4 documents per hour and throttle was set at 50% on a corresponding IDP Action, the IDP Rule is effectively changed to 2 documents/hour until the throttle restriction is lifted.
Throttle at <i>nn</i> % Block	<ul> <li>When selected, if the corresponding IDP Rule is triggered by exceeding its specified threshold value, a new threshold value is set for that Rule at <i>nn</i>% of the specified value. For example, if the corresponding IDP Rule set a maximum document count at 4 documents per hour and throttle was set at 50% on a corresponding IDP Action, the IDP Rule is effectively changed to 2 documents/hour until the throttle restriction is lifted.</li> <li>When selected, all future transaction which the corresponding IDP Rule applies to will trigger automatically until the block restriction is lifted. In the case where the corresponding IDP Rule has the "Enforce by IP" or "Enforce by User" box checked, only the offending IP/User's transactions are blocked.</li> </ul>

TERM	DEFINITION
ALERTS	
Log the alert	When checked, adds this request event to the System Logs.
Wait <i>nn</i> minutes	When checked, this option represents a time interval to wait before the next alert is logged into the system. A summary alert will be logged with information about the number of times the alert has triggered from the last logged alert.
Send an alert	When checked, an alert is sent to the user policy selected.
User	The email configured in the user policy is used to send the email.
Wait <i>nn</i> minutes	This field represents a time interval to wait before sending the next alert. A summary alert will be sent with information about the number of times the alert has triggered from the last sent alert.
SNMP trap alert	When checked, sends an SNMP IDP Rule violation trap to the Management Station.
Wait nn minutes	Time interval to wait before sending next SNMP trap alert.
Process alert	When checked, processes the Task List or Task List Group specified.
AUDITING	
Database	When checked, the system quarantines the document to a database when an enabled Archiving policy exists on the system.
SOAP Logging	When checked, the system sends the SOAP document to the Web Service running at the server specified by the remote policy.
Remote Policy	Defines the remote server used for SOAP logging.
Remote Path	The path used for SOAP logging.
Remote URI	The combination of the remote policy and the remote path.
Database Auditing	When checked, the system logs detailed information into an auditing database. Requires that an Archiving policy exists and is enabled on the WebAdmin. This option is unchecked by default.
	<b>Note:</b> For more information on Archiving policies, refer to the <i>Forum Systems</i> Sentry Version 9.1 Logging Guide.

# **IDP Action Policies Examples**

# The IDP Action Policies Examples

Examples for IDP Actions in a WSDL policy include:

• Add an IDP Action policy.

# Add an IDP Action Policy

Only after creating an IDP Action policy is it available to be bound to an IDP Rule. Email is assigned to a valid system User listed on the USER MANAGEMENT screen. This instruction assumes that your SMTP server is configured (from the System screen). Follow these steps to add an IDP Action policy, and sets quarantine a document to a database and sets quarantine a document to a remote server via SOAP.

# Adding an IDP Action Policy

IDP ACTION	N POLICIES > IDP ACTION DETAIL
IDP ACTION	
Name*:	QuarantineDocs
Description:	
PREVENTION SI	ETTINGS
🗹 Abort proce	ssing of the document
📃 Stealth	Mode (do not send a response)
Future Acce	ss Restrictions:
🔘 None	
💿 Throttle	e at 50 %
🔘 Block	
📃 Lift	restriction after 60 minutes
ALERTS	
📃 Log an aler	t
Wait 0	minutes before logging another alert
🗹 Send an ale	ert
User: jkanto	)S 💌
Wait: 1	_ minutes before sending another alert
🗹 SNMP trap a	alert
Wait 1	]minutes before issuing another SNMP trap alert

- From the Navigator, select the Actions screen. Select New.
- On the IDP ACTION POLICY screen, in the Name field, enter a **name** for this Action policy.
- In the Description field, enter a **description** for this Action policy (optional).
- Check the Abort processing of the document **checkbox**.
- Skip the Stealth mode (do not send a response) checkbox.
- Skip the None field.
- Select the **Throttle at** *nn* % radio button. Enter **50** as the value.
- Skip the Block and Lift restriction after *nn* minutes options.
- Skip the Log the alert and the Wait *nn* minutes before logging another alert options.
- Check the **Send an alert** checkbox.
- From the User drop down list, select a **user name** as the recipient of the alert email.
- In the Wait field, overwrite 0 minutes to **another value** minute before sending another alert.
- Check the **SNMP trap alert** checkbox.
- Enter 1 as the value in the Wait *nn* minutes before issuing another SNMP trap alert text field.

# **Constraints of IDP Action Policies**

ELEMENT	CONSTRAINTS	CHARACTER COUNT
IDP Action policy name	Unique and case sensitive. Accepts equal signs, the "@" character, dashes, underscores and spaces.	1-80

# **Specifications of IDP Action Policies**

ELEMENT SUPPORTED	SPECIFICATIONS
IDP Action policies	Unlimited

# **IDP SCHEDULES**

# **IDP Schedules Overview**

An IDP Schedule policy allows Administrators to schedule when an IDP Action policy is to be active. The IDP Schedule policy, associated with an IDP Action, provides a method of restricting a date/time during which requests being processed must meet the Request or Response criteria set in an IDP Rule policy.

# The Default Anytime Schedule

The Anytime IDP Schedule is pre-loaded on the system and is uneditable. Administrators are free to use the default Anytime IDP Schedule policy, or created custom schedules to meet their business requirements.

# **IDP Schedules Examples**

### The IDP Schedules Examples

The example for IDP Schedule policies is Add an IDP Schedule policy.

# Add an IDP Schedule Policy

Follow these steps to add an IDP Schedule policy:

IDP SCHEDULE	POLICIES > IDP SCHEDULE	DETAIL
IDP SCHEDULE DETAIL	S	
IDP Schedule Name*:	Chicago req Process Error Schedule	
Description:		
🗹 Sunday		
✓ Monday		
🗹 Tuesday		
🗹 Wednesday		
🗹 Thursday		
🗹 Friday		
🗹 Saturday		
Start time:	12:00 AM 🗸	
End time:	12:00 AM 👻	
🗌 Date Range:		
Start date:		
End date:		
	Create	

- From the Navigator, select the **Schedules** screen. Select New.
- On the IDP SCHEDULE POLICY screen, in the IDP Schedule name field, enter a **name** for this Schedule policy.

s

- In the Description field, enter a **description** for this Action policy (optional).
- For the days of the week, check the **checkbox** aligned with each day the schedule should run.
- Retain the default Start time values.
- Retain the default End time values.
- Click Create.

## **Constraints of IDP Schedule Policies**

ELEMENT	CONSTRAINTS	CHARACTER COUNT
IDP Schedule policy name	Unique and case sensitive. Accepts equal signs, the "@" character, dashes, underscores and spaces.	1-80

# **Specifications of IDP Schedule Policies**

ELEMENT SUPPORTED	SPECIFICATIONS
IDP Schedule policies	Unlimited

# **IDP BLOCKING**

# **IDP Blocking Overview**

The IDP Blocking screen provides a method of monitoring access restrictions placed on users or IPs because of IDP Rule violations. An IP or user can have its access restricted if it violates an IDP Rule which is associated with an IDP Action that has Blocking or Throttling set. Access to the IDP Blocking screen is available only to super users or a WebAdmin user with a Domain that grants access to IDP Blocking.

# **IDP Blocking Screen Terms**

The following table describes each term and definition for the IDP blocking screen:

TERM	DEFINITION
User / IP	The user or IP being tracked, and whose access is blocked or throttled.
Count	The number of transactions which have been restricted by throttling or blocking after the IDP Rules has been violated.
Trigger Value	The value which caused the IDP Rule to be violated.
	Example: If Max Document Size is set at 10 MG, and an 11 MG document is sent to the system, the Trigger Value would be displayed as 11.
IDP Rule	The name of the IDP Rule that was violated.
IDP Group	The name of the IDP Group which contains the IDP Rule.
Policy	The policy associated with the IDP Group that contains the IDP Rule that was triggered. This can be a WSDL policy or WSDL operation. If the IDP Rule belongs to the Default System Group, the policy is displayed as System.
Expires	Date on which restrictions will automatically be removed.

# Relationship between IDP Rules and IDP Actions and IDP Blocking

Historical data is tracked by both IP and user. Access restrictions are refused on IPs and users as applicable by the Enforce by IP and Enforce by User options set on an IDP Rule policy.

# **IDP Blocking Examples**

# The IDP Blocking Examples

Examples for IDP Blocking screen include:

- View IDP Blocking / Throttling Details.
- Remove IDP Blocking or Throttling Restriction.

# **View IDP Blocking or Throttling Details**

Follow these steps to view IDP Blocking / Throttling details:

Block	ked						
Г	U SER/IP	COUNT	TRIGGER VALUE	IDP RULE	IDP GROUP	POLICY	EXPIRES
Г	user1	0	10.07 KB / Minute	Max Bytes In A Minute	New XML IDP Group	New XML Policy	2005/05/25 13:47
	10.5.3.112	0	10.07 KB / Minute	Max Bytes In A Minute	New XML IDP Group	New XML Policy	2005/05/25 13:47
Throt	ttled						
	USER/IP	COUNT	TRIGGER VALUE	IDP RULE	IDP GROUP	POLICY	EXPIRES
No it	tems to display						

- From the Navigator, select the **IDP Blocking** screen.
- Review data on all violated IDP Rules associated with an IDP Action policy set to blocking or throttling.

# **Remove IDP Blocking or Throttling Restriction**

Follow these steps to remove IDP Blocking / Throttling restriction:

- From the Navigator, select the **IDP Blocking** screen.
- Check the **checkbox** aligned with the IDP Blocking policy to remove, and then click **Remove**.

# IDP Config – Aggregate IDP Across Multiple Sentry Instances

# **IDP Config Overview**

The IDP Config policy allows Administrators to enforce rate IDP Rules across different systems running behind a load balancer. Two or more systems are needed to use this feature. One of the systems in the cluster will behave as the Policy Server. All other systems will behave as agents. The Policy Server acts as a central location to keep track of the statistics for all the systems in the cluster. The agents update the Policy Server statistics, and receive information to handle the incoming requests.

# **IDP Config Screen Terms**

The following table describes each term and definition for the IDP config screen:

TERM	DEFINITION
Mode	<ol> <li>The system mode of operation:         <ol> <li>Standalone: Normal mode of operation.</li> <li>Agent: In this mode of operation the system stores IDP information on a central location, the system selected as the Policy Server.</li> <li>Policy Server: In this mode of operation the system behaves as Standalone. However, it also listens for IDP information from agents. This is the central location where all rate IDP information is aggregated.</li> </ol> </li> </ol>
Remote Policy	Used to indicate the location where the Agent should send request to update the IDP information. e.g. IP address and port of the Policy Server
Continue Processing if Policy Server Fails to Respond	If checked, when the Agent cannot contact the Policy Server it proceeds processing the requests. When unchecked, if the Agent cannot contact the Policy Server, the request is failed. By default this option is unselected.
Listener Policy	The IP address and port used by the Policy Server to listen for IDP information from the agents.

# **IDP Config Configuration**

As mentioned earlier at least two systems are required. One of the systems is going to be the Policy Server where the IDP values are stored. The other system will act as the agent that will ak the Policy Server whither it should allow the request through or not. Only the rate IDP rules, Maximum Document Count and Maximum Byte Count, are aggregated.

- On the System that will be the Policy Server, create a new HTTP Listener Policy that will listen for requests from the agent systems. Do not apply any authentication, just create a basic HTTP Listener.
- On the System that will be the Policy Server go to the IDP Config screen and set the Mode to Policy Server and select the new HTTP Listener Policy created in the step above.
- Create new IDP Rules for Maximum Document Count and/or Max Byte Count as needed. The IDP action used should have the blocking feature enabled if you want to be able to see what user or IP is being blocked on the IDP Blocking screen.
- Add the new IDP Rules to the IDP Group that is associated to the WSDL or XML policy.
- Transfer the WSDL or XML policy that you are working with to the agent system. This can be done via the Agent transfer or manually exporting the policy and importing it into the agent instance. This will also transfer the HTTP Listener policy, so be sure the listener policy has the use device IP option enabled to avoid an IP conflict with the listeners. The new IDP Rules will also be transferred.

- On the Agent system, create a new HTTP Remote policy that points to the HTTP Listener policy on the Policy Server system.
- On the Agent system, go to the IDP Config screen and set the mode to Agent. Select the new HTTP Remote policy created in the step above.

Requests sent to either system will increate the "count", once the limit is reach both instances will enforce the IDP Action configured in the new IDP Rules just created.

# INDEX

%abortmsg%	6
Abort IDP Action policy	23
add IDP Group policy	20
add IDP Rule policy	13
add IDP Rule policy with custom Error Mess	sage
	14
add IDP Schedule policy	31
alert actions	24
alert events	24
Anytime IDP Schedule policy	30
assign membership of IDP Rule to an IDP C	Group
· ·	2.1
conventions used	1
custom IDP error message	6
edit IDP Group policy membership	
example for IDP Blocking	33
examples for IDP Action policies	27
examples for IDP Groups	<u>2</u> 7 10
examples for IDP Pule policy	12
examples for IDP Schedule policies	 סג
how system associates rate-based rules with	00 ŀh
throttling	 o
IDP Action	ບ 
Abort processing of the document	23 25
Abort processing of the document	Z0
alert actions	24
BIOCK	25
	25
Lift restriction for <i>nn</i> minutes	25
Log the alert	26
no restriction on blocking	25
None	25
Send an alert	26
Send SNMP trap alert	26
silent mode	25
SNMP trap alert	26
Stealth mode	25
Wait <i>nn</i> minutes before issuing another	
SNMP trap alert	26
Wait nn minutes before logging another a	alert
	26
Wait nn minutes before sending another	alert
	26
IDP Action Details screen terms	25
IDP Action policies	6
examples	27
IDP Action policy	
options for obtaining a log	25
IDP Blocking	
Count	
examples	33
Expires	33
IDP Group which contains IDP Rule	33
IDP Rule that is violated	33
Policy	ວວ ຊຊ
1 Olloy	

trigger value	. 33
IDP Blocking and Throttling	.00
refreshing	31
IDP Blocking or Throttling	. 54
viewing details	24
IDD Blocking or Throttling rootriction	. 34
	24
	. 34
IDP Blocking screen terms	35
IDP Group policy	~~
adding	.20
assigning membership of IDP Rules in	.21
editing membership	.21
procedure for enabling	. 19
IDP Groups	. 16
default	. 16
examples	. 19
IDP Rule	
Abort Message	6
criterion	6
description	6
Enforce by IP	6
Enforce by User	6
Enforce only on User Group	6
how system associates rate-based rules wi	th
throttling	8
IDP Action policy selected	6
less restrictive enforcement settings	.11
more restrictive enforcement settings	.11
period	6
rate-based	7
selective enforcement settings	12
value	6
value-based	0
IDP Rule policy	
creating a global	13
creating with custom Error Template	11
	19
IDP Pulo scroop torms	בו. ה
IDP Schedule policies	0 6
overplan	0
IDD Sebedule policy 20	. 30 25
IDP Schedule policy	30
	.31
Anytime	.30
less restrictive enforcement of IDP Rule	.11
more restrictive enforcement of IDP Rule	.11
procedure for enabling an IDP Group policy	. 19
rate-based IDP Rules	1
retresh IDP Blocking and Throttling	.34
remove IDP Blocking or Throttling restriction .	.34
selective enforcement of IDP Rule	. 12
System	
IDP Group	. 16
terms	

in IDP Action Details screen	25
in IDP Blocking screen	.33, 35
in IDP Rule screen	6
trigger value	
IDP Blocking	33
value-based IDP Rules	7
view IDP Blocking or Throttling details	34
WSDL Operation	

16
20
17
16
20
17