FORUM **S**YSTEMS **S**ENTRY **V**ERSION **9.1**
IDP RULES **G**UIDE

Table of Contents

List of Figures

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.	N	N
Authentication failed #	Used for managing invalid credentials provided on a request.	N	N
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.	N	N
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.	N	N

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.	N	N
Document processing error #	Used for any type of error during the transaction.	N	N
Firewall rule violation	Used for WAF rule policy violation	N	N
Maximum attachment count	Used for maximum number of attachments allowed.	Y Max number of attachments	N
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	N
Maximum element depth	Used for maximum depth of elements allowed in an XML document.	Y Max depth of document	N
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.	N	N

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	N
Maximum response time	Used for maximum time to wait on a response from the remote server.	Y Max number in milliseconds	N
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	N
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	N
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	N
Minimum document size (in bytes, KB, MB or GB)	Used for minimum document size allowed.	Y Min size of document in selected unit	N
New operation	Used for tracking first time usage of WSDL operations.	N	N
New client IP address	Used for tracking the first time a request comes from a specific IP address.	N	N
New user	Used for tracking the first time a user accesses the system.	N	N
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.	N	N
SOAP Fault does not match any WSDL message	Used for detecting SOAP faults received that are not recognized in a WSDL.	N	N
SOAP Fault received from remote	Used for detecting any SOAP fault received in a response.	N	N
Unauthorized user	Used for detecting a user whose credentials are valid but lacks necessary permissions. The permissions are granted by an authorization call	N	N

	to an external identity server and by the ACL Execute permission.		
Virus found	Used for detecting a virus in a document, available only with licensed anti-virus plug-in.	N	N

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.

TERM	DEFINITION
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	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	
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	
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	
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.

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 Policy (Block-NoLifting) Associated with the IDP Rule Policy (MaxDoccount_NoEnforce)

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

MaxDoccount_NoEnforce IDP Rule Policy

IDP RULE POLICIES > IDP RULE DETAIL

DETECTION SETTINGS

IDP Rule Name*: MaxDoccount_NoEnforce

Description:

Criterion: Maximum document count

When document #25 comes into the system from any group, IP or user within a 1 hour period, the MaxDoccount_NoEnforce rule will be triggered, and the Block-Lift_After1Hour action will be active.

THRESHOLD

Value: 24 KB

Period: Hour

ENFORCEMENT SETTINGS

☐ Enforce only on User Group:

SNMPMonitor

☐ Enforce By IP

☐ Enforce By User

With No Enforcement Settings options checked, the counter is incremented for requests from any IP and any User.

IDP ACTION

IDP Action: BlockLiftAfter1Hour

Abort Message:

Subsequent documents will be blocked, but 120 minutes later, the blocking will be removed and the 1 hour timer will be restarted for this rule.

IDP SCHEDULE

IDP Schedule: Anytime

When the blocking restriction is lifted after 120 minutes, the IDP Rule is re-actived. The first document that comes in after the 2 hours have expired is considered Document #1.

IDP Action Policy associated with IDP Rule

IDP ACTION POLICIES > IDP ACTION DET

IDP ACTION

Name*: BlockLiftAfter1Hour

Description:

Processing document #25 (and all subsequent documents starting from the time Document #25 was received) for the next 2 hours will be aborted.

PREVENTION SETTINGS

☑ Abort processing of the document

☐ Stealth Mode (do not send a response)

Future Access Restrictions:

○ None

○ Throttle at 50 %

⊙ Block

☑ Lift restriction after 120 minutes

A log of this event is written to the System Logs.

ALERTS

☑ Log an alert

Wait 0 minutes before logging another alert

☑ Send an alert

User: klittle

Wait 0 minutes before sending another alert

☐ SNMP trap alert

Wait 0 minutes before issuing another SNMP trap alert

Karen Little will receive an email Alert when the IDP Rule triggers this IDP Action.

AUDITING

Quarantine the document:

☑ Database

☐ Soap Logging   Remote Policy: BostonEast-R

Remote Path:

Remote URI:

☑ Database Auditing

Document #25 and subsequent documents for the next 120 minutes are quarantined.

The Document that triggered the IDP Rule is sent to an auditing database.

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 101st document comes into the system within an hour from any IP and any User, the Rule is triggered. Processing of the 101st 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:

- 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_SENSOR			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 pre-loaded 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 pre-loaded 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 pre-loaded 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 pre-loaded 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:

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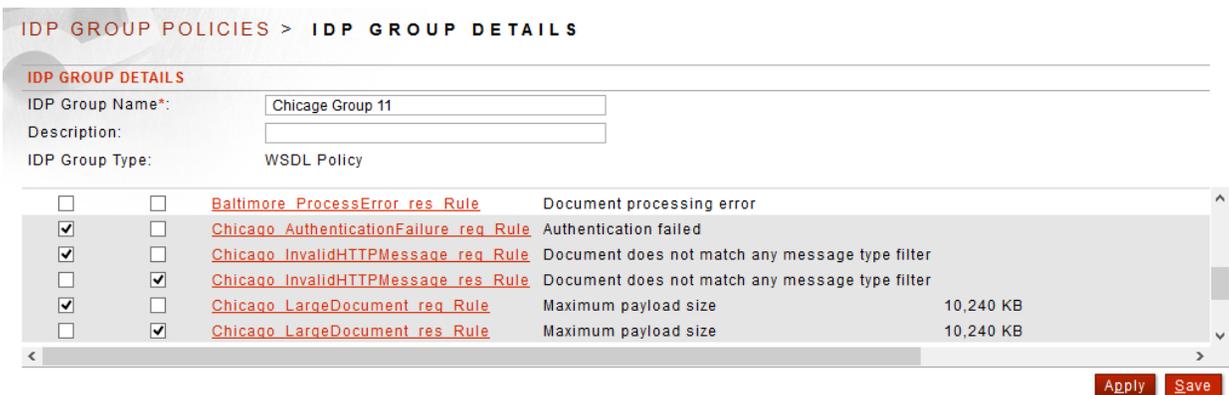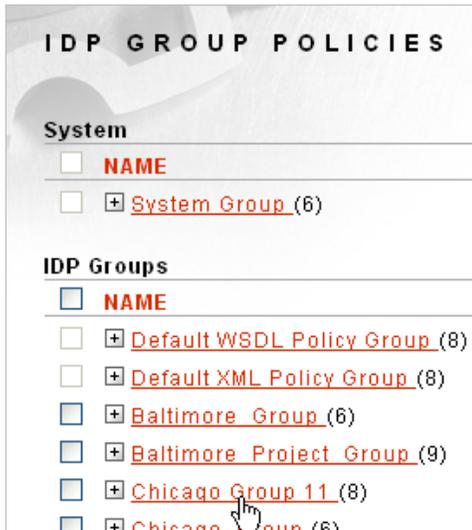
- From the Navigator, select the **Groups** screen. Select an **IDP Group name** link.
- On the IDP GROUP DETAILS screen, scroll down to view all IDP Rules currently on the system.
- Check the **checkbox** prefacing each IDP Rule that should be associated with the IDP Group.
- Click **Save**.

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
Id	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 SETTINGS	
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. **Note:** 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 RESTRICTIONS	
None	When selected, results in no access restrictions on the associated IDP Rule.
Throttle at *nn* %	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 *nn*% 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.
Block	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.
Lift restriction after *nn* minutes	• When checked, results in lifting the IDP Action restriction after the *nn* duration entered. • When unchecked (blocking is not restricted), then an Administrator is required to remove the blocking restriction from the IDP Blocking screen.

TERM	DEFINITION
ALERTS	
Log the alert	When checked, adds this request event to the System Logs.
Wait *nn* 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 *nn* 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. **Note:** For more information on Archiving policies, refer to the *Forum Systems 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

- 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:

- 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.
- 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:

- 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	The system mode of operation: 1. Standalone: Normal mode of operation. 2. Agent: In this mode of operation the system stores IDP information on a central location, the system selected as the Policy Server. 3. 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.
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 whther 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