



FORUM SENTRY™ VERSION 9 HTML POLICIES GUIDE



Legal Marks

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

FORUMOS™ Firmware, Forum Systems HTMLSec™ WebAdmin, Forum Systems HTML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ API Security Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

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

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

Forum Sentry™ Version 9 HTML Policies Guide, published May 2024.

D-ASF-SE-019006

Table of Contents

INTRODUCTION TO THE HTML POLICIES GUIDE	4
Audience for the HTML Policies Guide.....	4
Conventions Used in the HTML Policies Guide.....	4
HTML POLICIES	6
HTML Features.....	7
HTML Policy Examples.....	7
VIRTUAL DIRECTORIES	9
Virtual Directories Tab Screen Terms for HTML Policies	10
Virtual Directory Detail Terms for HTML Policies	10
Operations on Virtual Directories for HTML Policies	13
Processing in Proxy and Service Modes	13
Protocol Mixing with HTML Policies.....	14
Default Filter Expression in a Virtual Directory	15
TASK LISTS AND TASK LIST GROUPS FOR HTML POLICIES	17
Task Lists Groups or Task Lists at the Virtual Directory Level	17
Task Lists Groups or Task Lists at the HTML Policy Level	18
SETTINGS FOR HTML POLICIES	19
IDP RULES FOR HTML POLICIES	19
IDP Rule Tab Screen Terms for HTML Policy	20
LOGGING SETTINGS FOR HTML POLICIES	20
Logging Tab Screen Terms for HTML Policy	20
TRANSFERRING EXPORTING AND IMPORTING HTML POLICIES.....	21
REQUEST FILTERS FOR HTML POLICIES.....	23
Request Filters Available to All HTML Policies.....	24
Request Filters Available to Each Virtual Directory	24
Common Default Request Filters with HTML Policies	26
Request Filter Syntax	26
View or HTML Common Default Request Filters for HTML Documents.....	27
Delete a Request Filter	28
APPENDIX	29
Appendix A - How Request Filters Work	29
Appendix B - Constraints in HTML Policies Guide	30
Appendix C - Specifications in HTML Policies Guide	30
Appendix D - Virtual Directory Reference Chart in HTML Policies Guide	31
INDEX	32

List of Figures

Figure 1: Proxy and Service Modes.....	14
Figure 2: Protocol Mixing on HTML Policies.....	14
Figure 3: Request Filters Identify and Convert HTML Documents	29
Figure 4: The Virtual Directories Screen and Associated Options with HTML Policies.....	31

INTRODUCTION TO THE HTML POLICIES GUIDE

Audience for the HTML Policies Guide

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

- Create or import HTML policies.
- Manage Virtual Directories on an HTML policy.
- Manage settings on an HTML policy.
- Associate IDP Groups to HTML policies.
- Apply a Task List Group to an HTML policy.
- Apply a Pattern Match policy to HTML requests/responses.
- Apply Request Filter Templates on an HTML policy.

Assumptions

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

For information on Task Lists and performing Tasks on an HTML policy, refer to the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.

Screen Element on Legacy Systems

For customers upgrading from earlier versions of Forum Systems software to V9, the DOCUMENTS tab will not be visible on HTML policies.

However, for customers running legacy versions, the DOCUMENTS tab will be visible. The Documents listed in the DOCUMENTS tab will not appear in the Documents screen (on the Navigator), but remain in the HTML policies to be available for those customers who have run previous versions of the software.

Conventions Used in the HTML Policies Guide

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

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

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

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

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

Throughout this and other documents in the Documentation Set, repetitive actions such as the following are not shown:



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

(For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.)







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

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

For the focus of this document, the STATUS column is displayed on HTML policies, and Virtual Directories.

Virtual Directories Task Lists Settings		
<input type="checkbox"/>	VIRTUAL DIRECTORY	STATUS
<input type="checkbox"/>	New Virtual Directory	
<input type="checkbox"/>	New Virtual Directory2	

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

REQUEST FILTER POLICIES > REQUEST FILTER POLICY					
REQUEST FILTER POLICY					
Policy Name*:		Default_HTML			
<input type="checkbox"/>	#	MESSAGE TYPE FILTER	FORMAT	DESCRIPTION	STATUS
<input type="checkbox"/>	1	 HTTP GET	Simple	HTTP GET	
<input type="checkbox"/>	2	  HTTP POST	Simple	HTTP POST	
<input type="checkbox"/>	3	  Web Form	Web Form	Posted form (URL Encoded)	
<input type="checkbox"/>	4	 Web Form Data	Web Form Data	Posted form (Mime Encoded)	
Enable Disable New Delete Update Save Restore Defaults					

HTML POLICIES

An HTML policy is a set of rules that provide a policy for processing of HTML flowing through the system.

HTML policies include the following accessible properties and actions; each of which manages a portion of the HTML policy and is detailed later:

The screenshot shows the 'Virtual Directories' tab of an HTML policy configuration. The interface includes several sections: 'Virtual Path' with a text field containing '/testtesttest' and a checkbox for 'Enable Virtual Path Case Insensitivity'; 'Filter Expression' with a text field containing '(/.*)?'; 'Replace Expression' with a text field containing '\$0'; 'Request Filter Policy' with a dropdown menu set to 'Default_HTML' and an 'Edit' link; 'Error Template' with a dropdown menu set to '[From Listener Policy]'; 'Google Analytics' with a dropdown menu set to '[None]'; 'ACCESS CONTROL' section with 'IP ACL Policy' set to 'Unrestricted', 'Host ACL Policy' set to '[None]', 'ACL Policy' set to '[Allow All]', 'Password Authentication' set to '[From Listener Policy]', and 'Redirect Policy' set to '[None]'; 'VIRTUAL DIRECTORY TASKS' section with 'Request Processing' and 'Response Processing' both set to 'Task List Groups'; 'REMOTE SETTINGS' section with 'Send to remote server' checked, 'Remote Policy' set to 'api-openweathermap-org', 'Remote Path' set to '/testtesttest', 'Host Header' empty, 'Process Response' set to 'On', and a checkbox for 'Discard response from server'.

- **Virtual Directories:** Manage the services of the HTML policy and Request Filters.
- **Task Lists:** Manage Task Lists Groups. (For more information on the Task Lists or performing Tasks, refer to the *Forum Systems Sentry™ Version 9 Tasks Management Guide*).
- **Settings:** Manage HTML policy general settings.
- **IDP Rules:** Manage IDP Groups which represent a collection of Intrusion Detection and Prevention Rules. (For more information on IDP Rules, refer to the *Forum Systems Sentry™ Version 9 IDP Rules Guide*.)
- **Logging:** Manage policy level logging settings.

The screenshot shows the 'Virtual Directories' tab of an HTML policy configuration. It displays a table with the following data:

<input type="checkbox"/>	VIRTUAL DIRECTORY	STATUS	VIRTUAL URI	REMOTE URI
<input type="checkbox"/>	New Virtual Directory	●	http://192.168.1.35:80/html	http://10.5.1.17:80/html
<input type="checkbox"/>	New Virtual Directory2	●	http://10.5.1.35:80	http://10.5.1.17:80

At the bottom right of the table, there are four buttons: **Enable**, **Disable**, **Delete**, and **New**.

From an open HTML policy, users may select:

- **Enable / Disable** to enable or disable the Virtual Directory.
- **Delete** to delete a Virtual Directory.
- **New** to create a new Virtual Directory.

HTML Features

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

- Add an HTML policy.
- Create new or associate existing listener and/or remote network policy.
- Add, view or edit virtual directories.
- Apply access control to virtual directories.
- Associate Task List Groups in the HTML policy.
- Transfer, import or export HTML policies. (For more information, refer to the *Forum Systems Sentry™ Version 9 System Management Guide*.)
- Edit the default HTTP Request Filter settings.

HTML Policy Examples

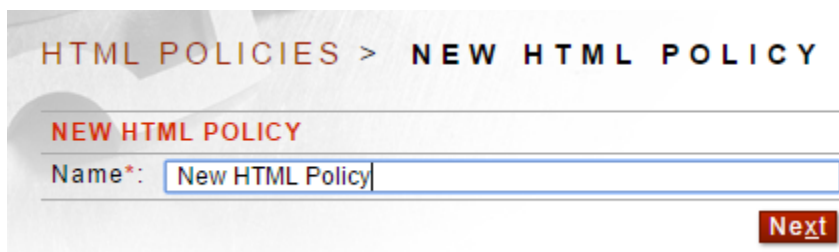
Examples for a HTML policy include:

- Add an HTML Policy.
- Create New Network Policies for HTML Policy.
- Use Existing Network Policy for HTML Policy.
- View Virtual Directories of an HTML Policy.

Add an HTML Policy

When adding an HTML policy, you may associate any existing Listener policy (HTTP, HTTPS, FTP, Tibco RV, Tibco EMS, IBM MQ, or Group Remote policy). Follow these steps to add an HTML policy and associate an existing Listener policy:

Adding an HTML Policy



- Navigate to the **HTML Policies** screen and select **New**.
- In the Name field, enter the **Name** for this HTML policy.

Note: At this point, you could associate any existing listener policy or create a new listener policy. This instruction uses the **Select from an existing listener policies** option.

Create New or Use Existing Network Policy for the HTML Policy
 You may create a new Listener Policy when creating an HTML Policy:

HTML POLICIES > NEW HTML POLICY

SET LISTENER POLICY

Please specify a listener policy for virtual directory: New Virtual Directory

☒ Select from existing listener policies
 HttpListenerPolicy (10.5.1.35:80) [Edit](#)

☐ Create a new HTTP listener policy

Listener Policy Name*: NewHTMLPolicy2-Listener

Use Device IP: ☐

Listener IP*: 192.168.1.35

Listener Port*: 80

SET VIRTUAL DIRECTORY PATH

Virtual Directory Path:

SET REMOTE POLICY

Please specify a remote network policy

☐ Do not send to remote server

☒ Select from existing remote policies
 NewXMLPolicy-Remote (10.5.1.17:80) [Edit](#)

☐ Create a new HTTP remote policy for this remote server

Remote Policy Name*: NewHTMLPolicy2-Remote

Remote Policy Host*:

Remote Policy Port*: 80

Finish

- From the SET LISTENER POLICY section, select the **Create a new HTTP listener policy** radio button.

NOTE: CHECKING THE USE DEVICE IP CHECKBOX MEANS THAT THE IP FROM WHICH THIS LISTENER POLICY LISTENS WILL BE THE SAME AS THE SYSTEM'S DEVICE IP.

- Enter the **Listener IP** address in the Listener IP field or check the **Use Device IP** checkbox to use the assigned device IP of the system.
- Enter the **Listener Port** in the Listener Port field.
- Enter the **Virtual Directory URI** path for accessing this policy (here users can “cloak” the back-end URI by entering a value different from the actual physical URI of the back-end server).
- From the SET REMOTE POLICIES section, select the **Create a new HTTP remote policy for this remote server** radio button.

Note: The Virtual URI is a read-only field because the system determines this value from the Network policy, virtual path, Filter and Replace Expression settings. The Physical Path and Physical URI fields are

read-only because the system uses the values from the HTML document.

If Administrators need to allow arbitrary subdirectories or URL parameters, the Filter Expression can be changed from the default `"/?"` to `"/.*?"`.

- Enter the **Remote IP** in the Remote policy Host field.
- Enter the **Remote Port** in the Remote policy Port field.
- Click **Finish**.

You may also use an existing Network Listener policy or Remote policy.

VIRTUAL DIRECTORIES

The Virtual Directories tab displays a summary of all the Virtual URIs in this HTML policy, as well as the Virtual URI and the Remote URI. HTML policies can have multiple Virtual Directories, but each must either have a unique Virtual URI or specify a unique Virtual Host.

Clicking on the **Virtual Directory name** link reveals the Virtual Directory settings for this HTML policy. Each virtual directory is used to map a virtual URI (local) to the physical path and URI (remote, as defined in the HTML document).

NOTE: WHERE HTTP POLICIES ARE DISCUSSED, ALL OTHER NETWORK POLICIES ARE VALID, EXCEPT WHEN USING AN FTP POLICY AS A REMOTE POLICY.

A Virtual Directory is a pattern which matches an incoming HTTP request URI. A Virtual Directory is defined on the port node in an HTML policy. Because the physical endpoint defined in the HTML policy is static, virtual directories can be used to:

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

Virtual Directories Tab Screen Terms for HTML Policies

The following table describes each term and definition on the Virtual Directories tab in HTML policies.

TERM	DEFINITION
Virtual Directory	Local URIs used to access the HTML policy.
Status	<ul style="list-style-type: none">• Green status light = enabled policy.• Yellow status light = a required functional element of this policy is disabled; i.e. the listener is disabled or the remote network policy is disabled.• Red status light = disabled policy.
Virtual URI	The Unique Resource Indicator (URI) path used by clients to access this policy.
Remote URI	Actual URI back-end server.

Virtual Directory Detail Terms for HTML Policies

The following table describes each term and definition found on the Virtual Directory of an HTML policy.

TERM	DEFINITION
Name	The identifier of this Virtual Directory.
Description	An optional description of this Virtual Directory.
Listener Policy	The Listener Policy on the system to associate with this Virtual Directory.
User Virtual Host as a Regular Expression	Using regular expressions within the virtual host definitions allow the HOST header to be matched based on the defined regular expression pattern. Enable this checkbox if the value entered in the virtual host field is to be interpreted as a regular expression rather than a string match for comparing to the inbound HOST header.
Virtual Host	<p>The Virtual Host option allows the IP:Port combination to have a 3rd parameter which uses the HOST header of the inbound request to determine which virtual directory policy matches. With no virtual host defined, the virtual directory is matched simply based on IP, Port and URI. With virtual host defined, the virtual directory is matched based on IP, Port, HOST Header, and URI.</p> <p>i.e.</p> <p>http://10.5.1.1:80/test/policy HOST: prod.company.com</p> <p>http://10.5.1.1:80/test/policy HOST: dev.company.com</p>
Virtual Path	The Virtual Path field allows users to customize this HTML's virtual path.
Virtual URI	The Unique Resource Indicator (URI) path used by clients to access this policy. This is where the system receives a request.

Filter Expression	The default "/" value represents an extended regular expression on which exists a trailing portion that must match a defined pattern before a request is accepted for processing.
Replace Expression	The "\$0" value represents the entire trailing portion of the request URI.
Send to remote server	<ul style="list-style-type: none"> When checked, the Remote Policies drop down list is enabled. Now, all requests and responses will be processed by the system in Proxy mode and sent to the selected Remote Policy. When unchecked, all requests and responses will be processed by the system in Service mode, with the processed request being returned to the client, and access to the Remote policy is disabled. <p>For more on Proxy versus Service mode see the chapter below titled: Processing in Proxy and Service Modes</p>
Discard response from server	When checked, responses from the back-end server are discarded.
Remote Policy	The Remote Policy associated with this Virtual Directory.
Remote Path	The back-end server IP / Port which identifies the Remote Policy.
Remote URI	Actual URI back-end server.
Host Header	The Host header set by Sentry when communicating with the remote server.
Process Response	When set to ON, the response from the back-end server undergoes pre-processing before being sent to the client.
IP ACL	The IP Access Control List that will be enforced on this Virtual Directory. With UnHTMLricted selected, there is no access control by IP enforced.
ACL	The User Access Control List that will be enforced on this Virtual Directory. With the Allow All ACL selected, there is no access control enforced. The selected User ACL grants access of this HTML policy to any member of the User ACL.

Password Authentication	<p>When set to From Listener Policy, the password authentication credentials captured at the Listener Policy level will be used for enforcement.</p> <p>When set to Specify, the administrator can choose to enforce any of the following Password Authentication options:</p> <ul style="list-style-type: none"> • Use basic authentication • Use digest authentication • Use cookie authentication • Use form post authentication • Username and Password Parameters are used with the form post authentication • Require password authentication (any): to enforce a successful authentication not just capture the credentials. <p>For more information on Password Authentication please refer to the Forum Sentry v9 Access Control Guide.</p>
Redirect Policy	The Redirect Policy that is associated to this Virtual Directory. Redirect Policies allow redirection to a different URL based on four events: Authentication Success, Authentication Failure, No Credentials and On Error. A valid Redirect Policy will need to be configured on the Resources>>Redirect Policies page in order to associate a Redirect Policy to the Virtual Directory.
Error Template	Associate an Error Template to this Virtual Directory or reference the Error Template in a selected Listener Policy that is associated with this Virtual Directory.
Request Task List Group	The Task List Group selected to process the request messages for this Virtual Directory.
Response Task List Group	The Task List Group selected to process the response message for this Virtual Directory.

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

Operations on Virtual Directories for HTML Policies

HTML policies may have one or more Virtual Directories. Operations on Virtual Directories include:

- Add, edit or associate another Listener and/or Remote policy to the Virtual Directory.
- Configure Additional Virtual Directories on an HTML policy.
- View / reconfigure a Virtual Directory.
- Enable / disable the Virtual Directory.
- Associate an ACL policy to the Virtual Directory.
- Associate an Error Template to this Virtual Directory or reference the Error Template in the Listener Policy.
- Edit the Remote Path of this Virtual Directory.
- Edit the Filter Expression used.
- Change the Replace Expression used.
- Add, edit, enable/disable, remove, promote or demote the request filter associated with the Virtual Directory.
- Select a Redirect Policy for the Virtual Directory.
- Select a Request Filter Policy

Virtual Directories in HTML policies may be set to process traffic in proxy mode or service mode.

Processing in Proxy and Service Modes

The following graphic displays processing in Proxy or Service modes:

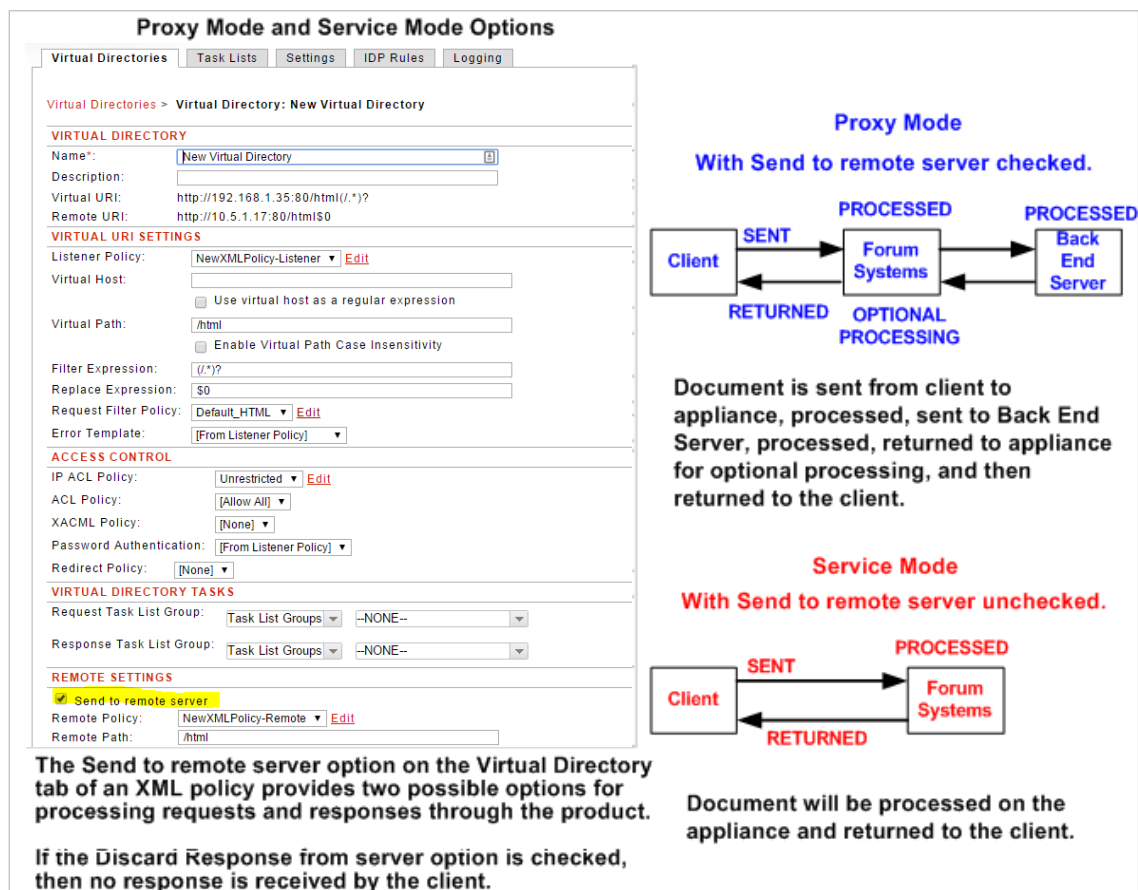


Figure 1: Proxy and Service Modes.

Proxy Mode

In Proxy mode, a document is sent from the client to the appliance, processed, sent to the back end server, processed, returned to the appliance for optional processing, and then returned to the client. Proxy mode is set when:

- the **Sent to Remote Server** checkbox in the Virtual Directory is checked.
- a **Remote policy name** is selected in the Remote policy field in the Virtual Directory.

Service Mode

Service mode allows the product to run as a service provider. A client request is processed by the product as an HTML document and then sent back to the client in the HTTP response. Service mode is set when:

- the **Sent to Remote Server** checkbox in the Virtual Directory is unchecked.
- access to the Remote policy field is blocked in the Virtual Directory.

Protocol Mixing with HTML Policies

Protocol mixing with HTML policies provides a method of mixing protocols between incoming request and outgoing responses on the system. Protocol mixing is allowed on the following example network policies, from Incoming Request to Outgoing Response on the system:

- from HTTP/S listener to Tibco-Rv remote.
- from HTTP/S listener to Tibco-EMS remote.
- from HTTP/S listener to IBM MQ remote.
- from HTTP/S listener to SMTP remote.
- from Tibco-Rv listener to HTTP/S remote.
- from Tibco-EMS listener to HTTP/S remote.
- from IBM MQ listener to HTTP/S remote.
- from SMTP listener to HTTP/S remote.

NOTE: THE BULLETED LIST ABOVE DOES NOT CONTAIN **EVERY** PERMUTATION POSSIBLE WITH PROTOCOL MIXING, BUT IS A SMALL REPRESENTATIVE SUMMARY OF SOME PROTOCOLS THAT MAY BE MIXED WITH OTHERS.

How the System Manages Protocol Mixing on HTML Policies

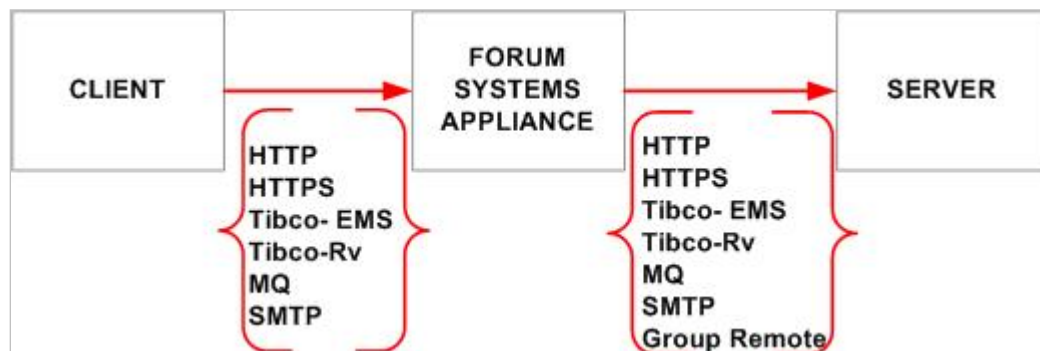


Figure 2: Protocol Mixing on HTML Policies.

NOTE: FOR MORE INFORMATION, REFER TO THE MIX PROTOCOLS ON AN HTML POLICY INSTRUCTION.

Asynchronous Protocols Supported with HTML Policies

The system also supports protocol mixing between the following asynchronous protocols:

- from Tibco-EMS to Tibco-Rv.
- from Tibco-EMS to IBM MQ.
- from Tibco-RV to Tibco-EMS.
- from Tibco-Rv to IBM MQ.
- from IBM MQ to Tibco-EMS.
- from IBM MQ to Tibco-Rv.

Asynchronous protocols, such as IBM MQ, need to be used in the “synchronous” mode in order to be compatible with HTTP. For example, if an IBM MQ policy has the Synchronous policy option turned off, protocol matching cannot occur with HTTP because they are incompatible paradigms.

Authentication with IBM MQ Policies

When authenticating a message in an IBM MQ policy or Tibco-EMS policy during run-time, the system searches each message for the **fs_user** and **fs_password** property, and uses this information to authenticate each message and establish identity.

For the JMS-based messaging protocols that support SSL (Tibco EMS, IBM MQ) we have added our own basic authentication capability to allow each message to be authenticated and an identity established. The identity can then be used for access control, obtaining a signing key or even generating and propagating an identity token such as a SAML token. The sender simply has to add two fields to the message headers that contain the user and password to use. For protocols that support SSL, it is recommended that SSL is used when sending the password along with a message. The password will not be propagated after it is consumed by the system. The properties **fs_user** and **fs_password** should be used in the JMS headers to add the appropriate credentials.

HTTP Headers

When HTTP is the inbound protocol, all headers allowed by RFC 2616 may be propagated to the remote protocol. The converse is also true, if the listener protocol is a JMS protocol (Tibco EMS or IBM MQ) any http headers that are specified (escaped with underscores rather than dashes) and the remote protocol is HTTP the headers will be placed into the HTTP protocol and propagated. This allows cookies such as authentication tokens from Tivoli Access Manager to be propagated and also content-type and any other stateful headers to be passed.

When mixing protocols on an IBM MQ policy, for example, the system manages authentication by converting all dashes to underscores in HTTP headers. This allows for the case of | HTTP | ----- | IBM MQ | ----- |HTTP| and all of the inbound headers (and cookies) will be propagated.

Default Filter Expression in a Virtual Directory

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

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

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

NOTE: THE DEFAULT FILTER EXPRESSION `"/?"` IS MORE HTMLRICTIVE THAN IN SOME PREVIOUS VERSIONS OF THE PRODUCT. IF YOU NEED TO ALLOW SUBDIRECTORIES OR URI PARAMETERS (A QUERY STRING), YOU CAN CHANGE THE FILTER EXPRESSION TO THE ALL-INCLUSIVE `".*"`.

Replace Expression in a Virtual Directory

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

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

Client requests are mapped to a Virtual Directory at run-time as follows:

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

Example:

WSDL port Virtual Directory is configured with:

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

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

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

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

TASK LISTS AND TASK LIST GROUPS FOR HTML POLICIES

The Task List tab allows users to view all Tasks and Task Lists associated with an HTML policy through Task List Groups or Task Lists.

Note: With Forum Systems Sentry v9, Task List Groups or Task List can now be set to process request or response documents individually per Virtual Directory, or per HTML Policy. In previous releases, a single Task List Group was set for all messages (request and response) for the Virtual Directory.

Task Lists Groups or Task Lists at the Virtual Directory Level

Task List Groups set at the Virtual Directory level are applicable only the Request or Response Messages for that Virtual Directory. Different Task List Groups can be selected for the request or response messages.

The screenshot displays the 'HTML POLICIES > HTML POLICY' configuration page. The 'Task Lists' tab is selected, showing settings for a 'New HTML Policy'. The 'Virtual Directories' section includes fields for Name, Description, Virtual URI, and Remote URI. Below this, the 'OPENAPI SETTINGS' section has a checkbox for 'Publish a different location in exported OpenAPI' and fields for 'Published Protocol', 'Published Host', and 'Published Port'. The 'VIRTUAL URI SETTINGS' section includes a 'Listener Policy' dropdown, 'Virtual Host' and 'Virtual Path' fields, checkboxes for 'Use virtual host as a regular expression' and 'Enable Virtual Path Case Insensitivity', and fields for 'Filter Expression', 'Replace Expression', 'Request Filter Policy', 'Error Template', and 'Google Analytics'. The 'ACCESS CONTROL' section includes dropdowns for 'IP ACL Policy', 'Host ACL Policy', 'ACL Policy', 'Password Authentication', and 'Redirect Policy'. The 'VIRTUAL DIRECTORY TASKS' section has dropdowns for 'Request Processing' and 'Response Processing', each with a 'Task List Groups' dropdown and a 'Type or select label name' field. The 'REMOTE SETTINGS' section has a checkbox for 'Send to remote server' and fields for 'Remote Policy', 'Remote Path', 'Host Header', and 'Process Response'.

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: New HTML Policy

Virtual Directories Task Lists Settings IDP Rules Logging Documents

Virtual Directories > Virtual Directory: New Virtual Directory

VIRTUAL DIRECTORY

Name: New Virtual Directory

Description:

Virtual URI: http://10.10.20.10:8181/testtesttest/.*?

Remote URI: http://api.openweathermap.org/testtesttest150

OPENAPI SETTINGS

☐ Publish a different location in exported OpenAPI

Published Protocol: http

Published Host:

Published Port:

VIRTUAL URI SETTINGS

Listener Policy: DEX-0181 Edit

Virtual Host:

☐ Use virtual host as a regular expression

Virtual Path: /testtesttest

☐ Enable Virtual Path Case Insensitivity

Filter Expression: /.*?/

Replace Expression: \$0

Request Filter Policy: Default HTML Edit

Error Template: [From Listener Policy]

Google Analytics: [None]

ACCESS CONTROL

IP ACL Policy: Unrestricted Edit

Host ACL Policy: [None]

ACL Policy: [Allow All]

Password Authentication: [From Listener Policy]

Redirect Policy: [None]

VIRTUAL DIRECTORY TASKS

Request Processing: Task List Groups Type or select label name [None]

Response Processing: Task List Groups Type or select label name [None]

REMOTE SETTINGS

☒ Send to remote server

Remote Policy: api-openweathermap-org Edit

Remote Path: /testtesttest

Host Header:

Process Response: On

☐ Discard response from server

Apply Save

Task Lists Groups or Task Lists at the HTML Policy Level

Task List Groups or Task Lists set at the HTML Policy level are applicable for all Virtual Directories of the HTML Policy. The Task List Groups or Task Lists can be associated with the Request Messages for all Virtual Directories.

HTML POLICIES > HTML POLICY

HTML POLICY

Policy Name: New HTML Policy

Virtual Directories

Task Lists

Settings

IDP Rules

Logging

TASK LIST GROUPS

Request Task List Group

Task List Groups

--NONE--

Response Task List Group

Task List Groups

--NONE--

Create

Save

NOTE: FOR FULL DOCUMENTATION ON TASKS, TASK LISTS AND TASK LIST GROUPS, REFER TO THE *FORUM SYSTEMS SENTRY™ VERSION 9 TASKS MANAGEMENT GUIDE*.
FOR INFORMATION ON EDITING / VIEWING A TASK LIST, REFER TO THE *COMMON OPERATIONS OF THE FORUM SYSTEMS SENTRY™ VERSION 9 WEB-BASED ADMINISTRATION GUIDE*.

SETTINGS FOR HTML POLICIES

The Settings tab includes name and description for this HTML policy. The Settings tab also includes the “Protect virtual resource option” and the “Enable session cookies option.”

TERM	DEFINITION
Policy Name	The identifier of this HTML Policy.
Policy Description	An optional description of this HTML Policy.
Protect Virtual Resource	<p>When Protect virtual resource is checked, the system uses the Sentry Virtual Directory when authenticating and authorizing against the back end server.</p> <p>When Protect virtual resource is unchecked, the system uses the Sentry physical URI when authenticating and authorizing against the back end server.</p>
Enable Session Cookies	<p>When the Enable session cookies option is checked, Sentry will automatically set a cookie (often the FSESSION cookie) for authentication and cache it for the duration noted. The cookie can be used in a Single Sign On paradigm.</p> <p>When the Enable session cookies option is unchecked, cookie is set.</p> <p>Cookie Parameters include:</p> <ul style="list-style-type: none">• Cookie Name• Cookie Path• Cookie Domain• Session Timeout (mins)• Session Idle Timeout (mins)
Enable Persistent Sessions	When the Enable Persistent Sessions option is checked, Sentry will store the cookie information in a database, using the selected Data Source. This allows for persistent sessions across multiple Sentry instances that all use the same database.
Use Secure cookies	A cookie with the Secure attribute is sent to the server only with an encrypted request over the HTTPS protocol, never with unsecured HTTP, and therefore can't easily be accessed by a man-in-the-middle attacker.
Use HTTP Only cookies	HttpOnly is an additional flag included in a Set-Cookie HTTP response header. Using the HttpOnly flag when generating a cookie helps mitigate the risk of client side script accessing the protected cookie (if the browser supports it)
WAF Policy	Associate a Web Application Firewall (WAF) policy from Resources->WAF Policies
Exclude from Monitoring	Do not include statistics from this policy in the Monitoring and performance statistics
Enable Response Caching	Enable a response caching policy (when licensed for this feature) to apply to responses for this policy
Enable Google Analytics	Enable statistics from this policy to be written to a Google Analytics policy (when licensed for this feature)

IDP RULES FOR HTML POLICIES

Intrusion Detection and Prevention (IDP) Rules define a set of criteria which can be associated with an HTML policy. IDP Groups represent a reusable collection of IDP Rules that may be applied to this HTML

policy. Under the IDP Group drop down list is a listing of all the IDP Rules included in the selected IDP Group.

NOTE: FOR FULL DOCUMENTATION THAT THE PRODUCT PROVIDES ON IDP RULES, REFER TO THE *FORUM SYSTEMS SENTRY™ VERSION 9 IDP RULES GUIDE*.

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

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

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

IDP Rule Tab Screen Terms for HTML Policy

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

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

LOGGING SETTINGS FOR HTML POLICIES

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

Logging Tab Screen Terms for HTML Policy

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

TERM	DEFINITION
------	------------

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

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

TRANSFERRING EXPORTING AND IMPORTING HTML POLICIES

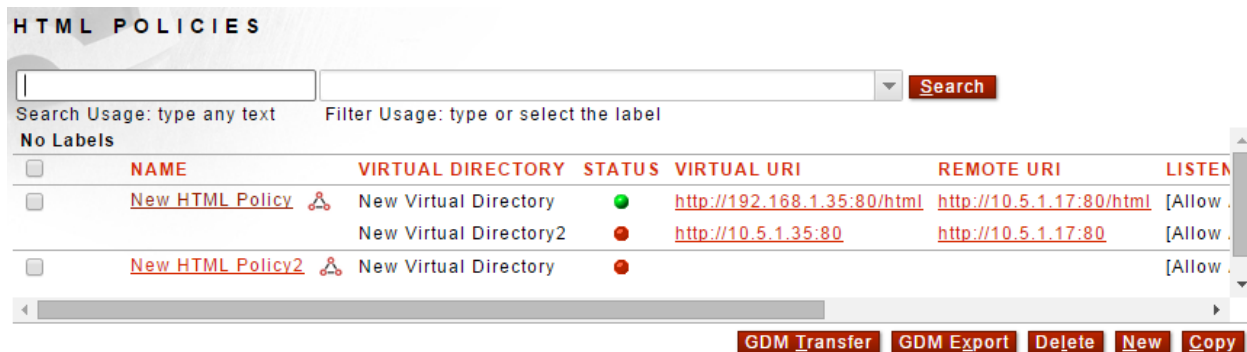
Users may transfer one or more HTML policies (and all its dependencies) from one Agent machine to another Agent machine with the **GDM Transfer** command visible on the HTML Policies screen. This type of transfer is referred to as a GDM partial configuration transfer.

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

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

For information on the following features, refer to the following sections of these volumes:

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



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

GDM IMPORT

Password*:

☒ From file (.fsg)*:

Choose File

No file chosen

☐ From database

Configuration Name:

Browse

Import

REQUEST FILTERS FOR HTML POLICIES

A Request filter allows the system to select those HTTP requests that match selection criteria based on the HTTP headers and decode the request appropriately. Most request filters will only need to examine the content-type header, but any header may be used.

Request filters can be used to manage sets of standard, emerging and future content types, along with associated rules. Administrators may add, configure, edit and remove request filters, as well as HTMLore default request filters that have been deleted. You may enable or disable request filters, and re-prioritize the list of request filters. Request filters include a name, format, description, identifying expression and parameter.

There are two sets of default Request Filters. One is pre-configured; the other one is not.

One set of Request Filters is common; that is, these are a collection of Request Filters which are available to all HTML policies.

The other set of Request Filters is local; that is, these are a collection of Request Filters which are available to any subsequently created Virtual Directory on an individual HTML policy.

Both sets of Request Filters include:

- HTTP GET*
- HTML POST*
- Web Form*
- Web Form Data

Requests not matching a defined Request Filter policy will not be processed and will throw a process error triggering the IDP Process Error rule.

Request Filter Properties

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

TERM	DEFINITION
Name	The name given to the Request Filter.
Format	<p>The following formats are available for Request Filters:</p> <ul style="list-style-type: none">• Simple• Web Form• Multipart• DIME (Direct Internet Message Encapsulation)• Web Form Data• Streaming• HTML• MTOM
Note: for JSON use Simple or use the default JSON Request Filter.	
Description	A description for the Request Filter.
Identification	An expression using “request filter” syntax, used to match HTTP request to process with

Expression	this filter.
Parameter	For “Web Form” and “Web Form Data” request filters, the name of the HTML form parameter which contains the data to process.
Convert Content-encoding	<ul style="list-style-type: none"> • The No conversion option means that whatever compression (i.e. HTTP Transfer-encoding) was received from the client (compress, gzip, deflate, or none) will be retained and used for forwarding the HTML message to the back end server. • The identity (uncompressed) option means that any compression used by the originating client will be removed before forwarding the uncompressed HTML message to the back end server. • The gzip option means that whatever compression was received from the client (compress, gzip, deflate, or none) will be replaced with gzip compression before forwarding the HTML message to the back end server. • The deflate option means that whatever compression was received from the client (compress, gzip, deflate, or none) will be replaced with deflate compression before forwarding the HTML message to the back end server.

Request Filters Available to All HTML Policies

The collection of common default request filters on the system is accessed from the **REQUEST FILTER POLICIES**. These request filters affect and apply only to newly created HTML policies and represent the collection of all Request Filters available to any newly created Virtual Directory.

REQUEST FILTER POLICIES

8 items found. Search , max results [Show](#)

☐ **REQUEST FILTER POLICY**

☐ [Default](#)

☐ [Default HTML](#)

☐ [Default JSON](#)

☐ [Default OAuth](#)

☐ [Default REST](#)

☐ [Default STS](#)

☐ [Default WSDL SOAP 1 1](#)

☐ [Default WSDL SOAP 1 2](#)

[Restore Defaults](#) [Delete](#) [Copy](#) [New](#)

Request Filters Available to Each Virtual Directory

Local default request filters on the system are accessed from the **HTML Policies** screen, after selecting an **individual HTML Policy name link**. On the Virtual Directory tab, select a **Virtual Directory link**. On the Virtual Directory Details screen, scroll to the bottom of the screen. These request filters apply only to an individual Virtual Directory on an HTML policy and represent the collection of all local Request Filters available to this specific Virtual Directory. The Request Filters area of the screen displays the three enabled request filters.

Virtual Directories

Task Lists

Settings

☐ VIRTUAL DIRECTORY

☐ [New Virtual Directory](#)

☐ [New Virtual Directory2](#)

Apply

Save

<input type="checkbox"/>	#	MESSAGE TYPE FILTER	FORMAT	DESCRIPTION	STATUS
<input type="checkbox"/>	1	⬇ HTTP GET	Simple	HTTP GET	●
<input type="checkbox"/>	2	⬇⬆ Web Form	Web Form	Posted form (URL Encoded)	●
<input type="checkbox"/>	3	⬇⬆ Web Form Data	Web Form Data	Posted form (Mime Encoded)	●
<input type="checkbox"/>	4	⬆ HTTP POST	Simple	HTTP POST	●
<div> <div>Restore Defaults</div> <div>Enable</div> <div>Disable</div> <div>Delete</div> <div>New</div> </div>					

Common Default Request Filters with HTML Policies

A summary of the common default Request Filters that come pre-configured with HTML policies are:

REQUEST FILTER NAME	FORMAT	CONTENT TYPES
HTML Default	Simple	<ul style="list-style-type: none">• text/HTML• application/HTML
Web Form	Web Form	<ul style="list-style-type: none">• application/x-www-form-urlencoded
Web Form Data	Web Form Data	<ul style="list-style-type: none">• multipart/form-data
HTTP GET	Simple	<ul style="list-style-type: none">• text/HTML• application/HTML
Streaming	Streaming	<ul style="list-style-type: none">• (agnostic)
HTML	HTML	<ul style="list-style-type: none">• (agnostic)

Note: Add a new Request Filter by navigating to the **Virtual Directories** tab, and then click **New** from the HTTP REQUEST FILTER section of the screen. Enter **values**, and then click **Save**.

Request Filter Syntax

The following table displays literal Request Filter syntax conventions used when creating an identifying expression for a Request Filter:

LITERAL CONVENTION	DEFINITION
	Or
&&	And
()	Grouping
==	Exact match
==i	Case insensitive (Header field will be matched without regard to case.)
==~	Regular expression match (Header field will be matched to a regular expression or a wild card.)
" "	Quotes must surround the value to match.

Note: If your business processes use only the default Request Filters, then there is no need to create new Request Filters. Adding a new Request Filter is a global operation, and doing so makes all content types listed in the Request Filter screen available to all documents that are processed on the system.

For information on enabling / disabling or editing a Request Filters, refer to the Common Operations of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

View or HTML Common Default Request Filters for HTML Documents

Viewing Common Default Request Filters for HTML Documents

The common default Request Filters for HTML policies can be viewed by navigating to the **REQUEST FILTERS POLICY** and selecting the Default HTML request filter policy. If any of the common default request filters have been edited or removed, you may revert them back to their factory state by following these steps:

These common default Request Filters are available to all Virtual Directories of all HTML policies on the system.

Note: When HTMLing default Request Filters, all previously created Request Filters will be deleted.

Add a Web Form Request Filter

To add a Web Form request filter:

REQUEST FILTER POLICIES > REQUEST FILTER POLICY > MESSAGE TYPE FILTER

HTTP REQUEST FILTER

Name*: InvoiceWebForm

Format: Web Form

Description:

Identification Expression*:
☒ Generate Expression

Methods:
☒ GET ☐ POST ☒ HEAD ☐ PUT ☐ DELETE
☐ OPTIONS ☐ TRACE ☐ CONNECT

Content Types:
☒ ANY ☐ XML ☐ SOAP 1.1 ☐ SOAP 1.2 ☐ SwA
☐ MIME ☐ MTOM ☐ DIME ☐ JSON
☐ URL Encoded ☐ Web Form

Parameter*: DOCUMENT

Remote Convert Content-Encoding: [No conversion]

Client Convert Content-Encoding: [No conversion]

Create

- From the Navigator, select an **HTML Policy** and then select a virtual directory.
- Select "Edit" next to the request filter policy and then select **New** on the following screen.
- On the REQUEST FILTER details screen, enter a **Request Filter** name in the Name field.
- From the Format drop down list, click **Web Form**.
- Enter a **Description** in the Description field (optional).

Note: Review the previous section entitled Request Filter Syntax or enter an identifying expression that parallels the examples below:

```
Example #1    Content-Type == "application/x-www-form-urlencoded" && method
== "POST"
```

```
Example #2    ( Host == "acme3.com" || Content Type ==~ "acme3/.*" ) &&
method == "POST"
```

You may type either expression into the Identification Expression field, or paste an expression into it.

- Enter an expression that tests HTTP header values in the Identification Expression field. Enter:

```
Content-Type == "application/x-www-form-urlencoded" && method == "POST"
```

- Enter **DOCUMENT** (the name of the text field from the posted form) in the Parameter field.
- Skip the Convert Content-Encoding drop down list.
- Click **Create**.

Promote or Demote a Request Filter Priority

Follow these steps to promote a Request Filter priority. This instruction promotes the Web Form Request Filter:

- From the Navigator, select an **HTML Policy** and then select a virtual directory.
- Select "Edit" next to the request filter policy and then select **New** on the following screen.
- With your mouse, select the **UP arrow** aligned with the Web Form Request Filter.
- The REQUEST FILTERS screen refreshes and the Web Form Request Filter has been promoted.

Delete a Request Filter

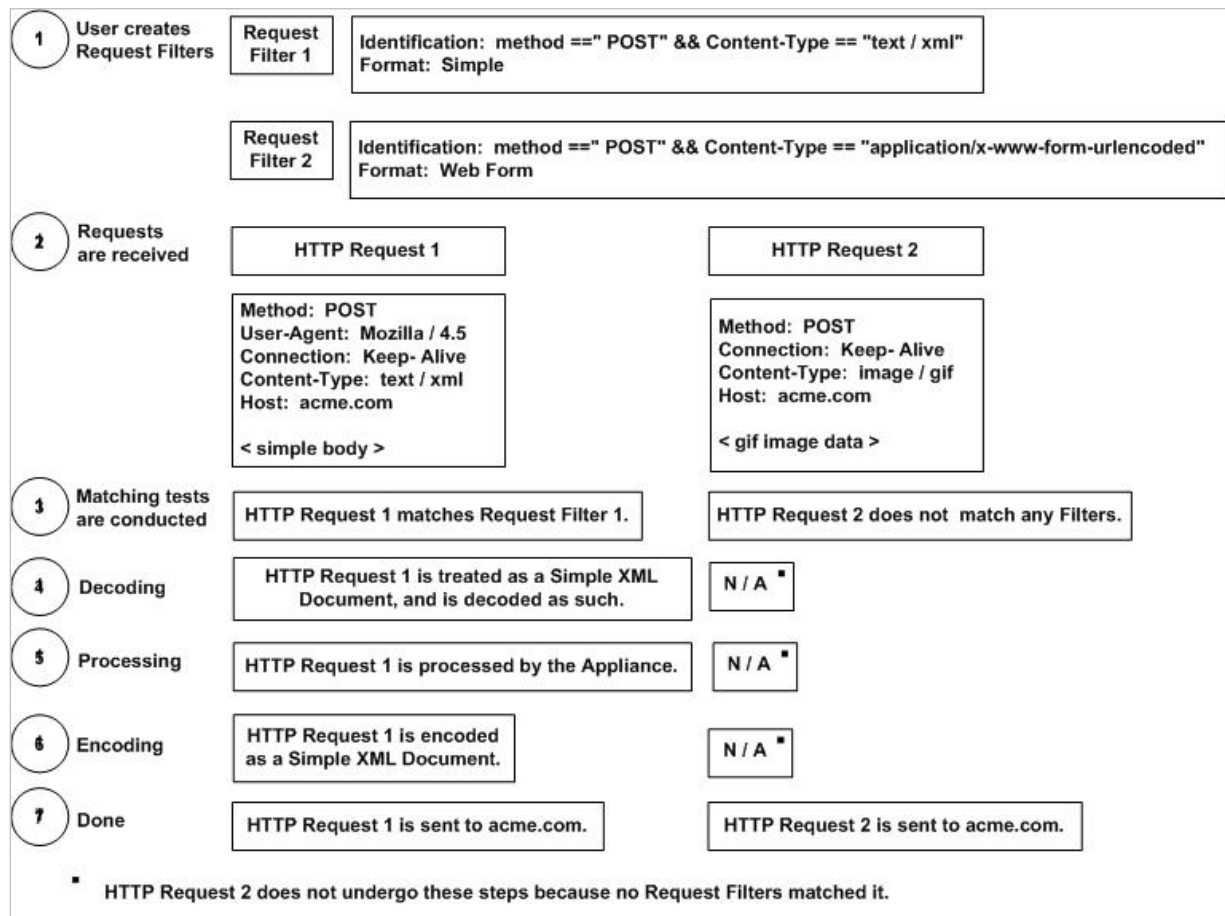
Follow these steps to delete a Request Filter:

- From the Navigator, select an **HTML Policy** and then select a virtual directory.
- Select "Edit" next to the request filter policy and then select **New** on the following screen.
- Check the **checkbox** aligned with a Request Filter, and then select **Delete**.
- The "Are you sure that you want to permanently delete all existing filters?" message appears. Click **OK**.

APPENDIX

Appendix A - How Request Filters Work

Request Filters identify and decode HTML documents of different types as they are prepared for processing in the system, before actual document manipulation. The graphic below displays the actions that occur as Request Filters are applied to a document:



NOTE: THIS GRAPHIC ASSUMES THAT THE NO MATCHING XML IDP RULE IS OFF.

Figure 3: Request Filters Identify and Convert HTML Documents

Appendix B - Constraints in HTML Policies Guide

ELEMENT	CONSTRAINTS	CHARACTER COUNT
HTML policy Names	Unique and case sensitive. Must start with an alpha character. Accepts underscores and dashes.	1-32
Virtual Directory name	Unique and case sensitive	1-256
Request Filter name	Unique and case sensitive	1-256

Appendix C - Specifications in HTML Policies Guide

ELEMENT SUPPORTED	SPECIFICATIONS
HTML policies	Unlimited *
Virtual Directories	With HTML policies, you may have an unlimited number of Virtual Directories per HTML policy.
Request Filters	100
Task Lists allowed per HTML policy	Unlimited * Task Lists are associated to Task List Groups, not directly to HTML Policies. Task List Groups can contain multiple Task List.
Task List Groups allowed per HTML policy	1 Task List Group can be set at the following levels: <ul style="list-style-type: none">• Virtual Directory for Requests• Virtual Directory for Responses• HTML Policy for Requests• HTML Policy for Responses

* Limited only by disk space.

Appendix D - Virtual Directory Reference Chart in HTML Policies Guide

Click on the Virtual Directory name link to view available options in a Virtual Directory.

The screenshot shows the 'Virtual Directories' tab in a web management interface. The main form is titled 'Virtual Directory: New Virtual Directory'. It contains several fields and checkboxes for configuring a new virtual directory. Red and blue arrows point from text explanations on the right to specific fields in the form.

Virtual Directories > Virtual Directory: New Virtual Directory

VIRTUAL DIRECTORY

Name*: New Virtual Directory

Description:

Listener Policy: Bayside_Listener

Virtual Path: /virtual/service

Virtual URI: https://10.5.6.92:8034/virtual/service/?

Filter Expression: /?

Replace Expression: \$0

☒ Send to remote server

☐ Discard response from server

Remote Policy: Bayside_Remote

Remote Path: /remote

Remote URI: http://www.server.com:8080/remote/\$0

Process Response: On

ACL: EastCoast_ACL

Error Template: [From Listener Policy]

From the Listener Policy drop down list, select a Listener Policy to associate with this XML Policy.

The Virtual Path field allows users to customize this XML policy's Virtual Path.

With **Send to remote server** checked, the Remote Policies drop down list becomes enabled.

With **Discard response from server** checked, any responses from the back end server are discarded.

From the Remote Policies drop down list, select a **Remote Policy** to associate with this XML Policy.

The Remote Path field allows users to customize this XML policy's Remote Path.

From the Access Control List drop down, select an **ACL Policy** to enforce on this XML policy. The "Allow All" ACL means there is no access control enforced.

From the Error Template drop down list, select the **Error Template Policy** referenced on the Listener policy, or select another one.

#	HTTP REQUEST FILTER	FORMAT	DESCRIPTION	STATUS
1	XML_Default	Simple	Plain XML	●
2	Web_Form	Web Form	Posted form (URL Encoded)	●
3	HTTP_GET	Simple	HTTP GET	●
4	Multipart	Multipart	SOAP with Attachments	●
5	DIME	DIME	WS-Attachments	●

Restore Defaults Enable Disable Delete New

Select a **Request Filter** link to view details, or select **New** to create a new HTTP Request Filter.

Figure 4: The Virtual Directories Screen and Associated Options with HTML Policies.

INDEX

- add a REST policy while creating a Listener policy, 8
- add a REST policy while creating a Remote policy, 8
- add REST policy and associate existing Listener, 7
- common default Request Filters, 26
 - restoring, 27
 - viewing, 27
- common Request Filter, 24
- communication mode
 - Proxy mode, 14
 - Service mode, 14
- content-encoding conversion options with request filters, 24
- conventions used, 4
- convert content-encoding options with request filters, 24
- default Filter Expression, 15
- deflate
 - content-encoding conversion option with request filters, 24
- delete Request Filter, 28
- description of Virtual Directory of an REST policy, 10, 19
- Discard response from server of Virtual Directory of an REST policy, 11
- Discard response from server on Virtual Directory, 31
- Error Template of Virtual Directory of an REST policy, 12
- examples for REST policy, 7
- export REST policies, 21
- expression that tests HTTP headers
 - Media Type, 28
- Filter Expression
 - default in WSDL policy, 15
- Filter Expression of Virtual Directory of an REST policy, 11
- fs_password, 15
- fs_user, 15
- gzip
 - content-encoding conversion option with request filters, 24
- identity (uncompressed)
 - content-encoding conversion option with request filters, 24
- IDP Rules tab terms, 20
- import REST policies, 21
- Listener Policy of Virtual Directory of an REST policy, 10
- local Request Filter, 24
- media type
 - expression that tests HTTP headers, 28
- mix protocols on an REST policy, 14
- name of Virtual Directory of an REST policy, 10, 19
- no conversion
 - content-encoding conversion option with request filters, 24
- parameter
 - for Web Form Request Filter format, 28
- Process Response of Virtual Directory of an REST policy, 11
- promote / demote Request Filter priority, 28
- Protect virtual resource
 - Settings tab, 19
- protocol mixing on an REST policy, 14
- Proxy mode
 - communication mode, 14
- Remote Path of Virtual Directory of an REST policy, 11
- Remote Policy of Virtual Directory of an REST policy, 11
- Remote URI of Virtual Directory of an REST policy, 11
- Replace Expression of Virtual Directory of an REST policy, 11
- Request Filter
 - common, 24
 - deleting, 28
 - format for Web Form, 27
 - local, 24
 - promoting/demoting priority, 28
 - syntax, 26
- Request Filters
 - common default, 26
 - how they work, 29
- REST policy, 6
 - adding and associate existing Listener, 7
 - adding while creating a Remote policy, 8
 - adding while creating Listener policy, 8
 - examples, 7
 - mixing protocols on an REST policy, 14
 - Proxy mode, 14
 - Service mode, 14
 - Settings tab, 19
 - using existing Listener policy, 9
 - Virtual Directories tab, 9

- REST Policy names, 7, 8
- restore common Default Request Filters, 27
- Send to remote server of Virtual Directory of an REST policy, 11
- Service mode
 - communication mode, 14
- Settings tab in REST policy, 19
- terms
 - in IDP Rules tab, 20
 - on Virtual Directories tab for REST policy, 10
 - on Virtual Directory of an REST policy, 10
- transfer REST policies, 21
- use existing Listener policy for REST policy, 9
- User ACL of Virtual Directory of an REST policy, 11
- view common Default Request Filters, 27
- Virtual Directories tab in REST policy, 9
- Virtual Directories tab screen terms, 10
- Virtual Directory
 - description, 10, 19
 - Discard response from server, 11, 31
 - Discard send to remote server, 11
 - Error Template, 12
 - Filter Expression, 11
 - Listener Policy, 10
 - name, 10, 19
 - Process Response, 11
 - Remote Path, 11
 - Remote Policy, 11
 - Remote URI, 11
 - Replace Expression, 11
 - User ACL, 11
 - Virtual Path, 10
 - Virtual URI, 10
- Virtual Directory terms, 10
- Virtual Path of Virtual Directory of an REST policy, 10
- Virtual URI of Virtual Directory of an REST policy, 10
- Web Form
 - Request Filter format, 27
- Web Form Request Filter format
 - parameter for, 28
- WSDL policy
 - default Filter Expression, 15