



CHAPTER 20

Configuring Reactor Processing

This chapter describes the internal message processing engine in the ACE XML Gateway, the Reactor. It covers these topics:

- [About the Reactor, page 20-199](#)
- [Using Flex Path Reporting, page 20-201](#)
- [Enabling or Disabling Reactor on a Port or Server, page 20-202](#)
- [Configuring Reactor Message Format Defense, page 20-203](#)

About the Reactor

At the core of the ACE XML Gateway system is a high-performance, stream-oriented message processing engine called the Reactor. The Reactor helps to alleviate the performance costs of XML processing.

The Reactor supports a subset of the features that can be enabled in a policy. Specifically, the Reactor provides SSL processing, XML well-formedness checking, XML schema validation, and certain WS-Security features. For service definitions with features enabled that are not supported by the Reactor, messages are handled by the standard HTTP processing path in the ACE XML Gateway, the Flex Path.

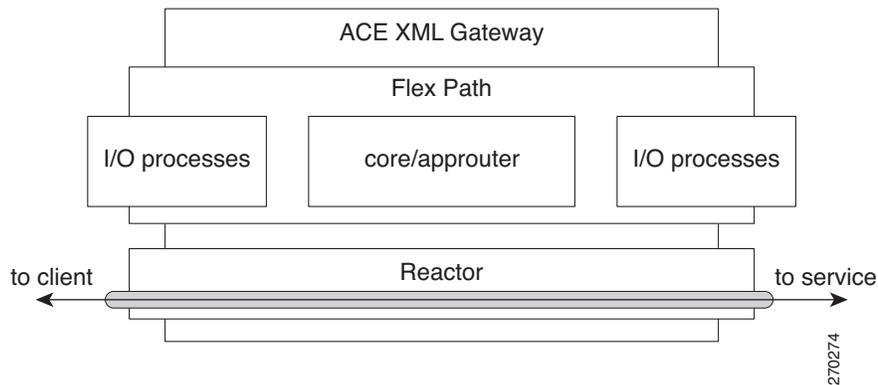
While it doesn't support global content screening or denial-of-service rules, the Reactor does support message format defense. In format defense, the Reactor screens messages that could over-burden an XML processor, including possible XML denial-of-service type attacks. Format defense blocks messages by properties such as maximum size, number of elements, entity size, or several other configurable properties.



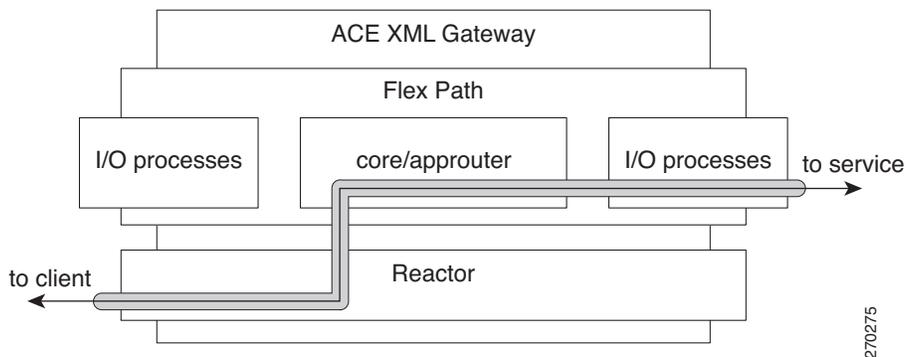
Note

If you enable Flex Path reporting in the Manager web console, you can view which policy objects are supported by the Reactor, and for those that aren't, the specific settings blocking its use.

Messages handled by the Reactor are passed through the ACE XML Gateway with the Reactor handling I/O processing on both sides of the transmission to the network.

Figure 20-1 Reactor processing path

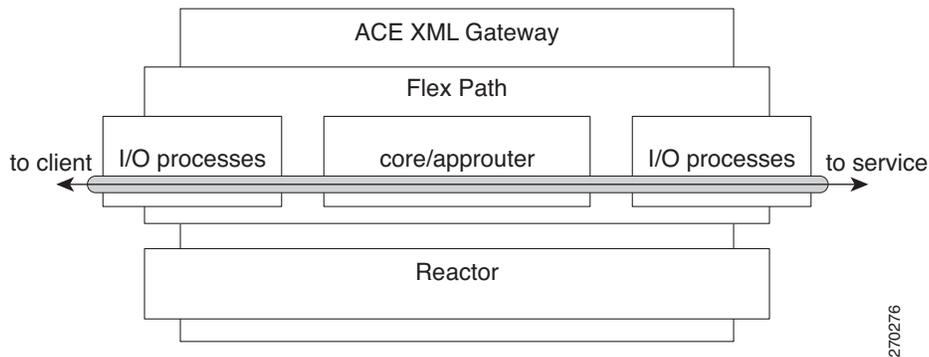
When it receives a message it can't handle, the Reactor hands off the message to other processors in the ACE XML Gateway (exactly which one varies by message type). This non-Reactor message path is called the *Flex Path*. When the response has been received and processed by the ACE XML Gateway, the Flex Path passes it back to the Reactor for delivery to the client, as shown in [Figure 20-2](#).

Figure 20-2 Reactor hand-off to Flex Path

A port object defines a client-side listening port on the ACE XML Gateway. The port object can be configured to bypass Reactor handling for all messages on the port. Individual virtual services can be configured to perform Flex Path processing only as well.

In this case, the usual HTTP listener process receives and sends messages on the network.

Figure 20-3 Flex Path mode



For systems upgraded to 5.0, the existing port objects in the policy are set to bypass Reactor by default. This helps to prevent possible compatibility issues in previously tested and deployed systems. Server objects in the policy can similarly be configured to bypass Reactor handling.

In general, the Reactor should be used for a service only after careful interoperability testing with the backend service and client.

Authentication is supported by the Reactor, but primarily in the form of an authentication cache. The first time a message is received with a given set of credentials, it is processed on the Flex Path. If accepted, its credentials are cached. Subsequent requests with the same credentials are supported by the Reactor. This can improve performance particularly for web-based applications, which usually submit credentials at every request.

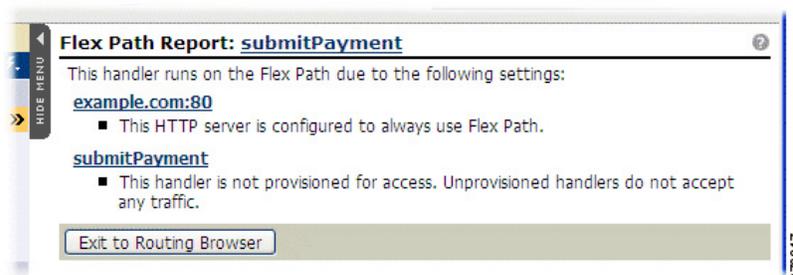
Using Flex Path Reporting

As mentioned, not all policy features are supported by the Reactor. Messages that are subject to protocol mediation or transformation by XSLT, for example, need to be processed on the ACE XML Gateway Flex Path instead of the Reactor.

At policy development time, you can view whether a virtual service defines a message path that can be processed by the Reactor.

When Flex Path reporting is enabled, a report icon appears next to service objects in the **Virtual Services** browser that are not handled by the Reactor (🔍). Clicking the icon opens a page that reports the policy settings that prevent Reactor processing.

Figure 20-4 Flex Path Reporting



The report icons only appear when Flex Path reporting is enabled, as described in the following steps:

-
- Step 1** In the ACE XML Manager console, click the **System Management** link on the navigation menu.
- Step 2** Click **Manager Settings** link on the right side of the ACE XML Manager information area.
In the Workflow area, enable the **Show Flex Path Reports** item to make compatibility reports accessible from the **Virtual Services** browser.
- Step 3** Click **Save Changes** to have the change take effect.
-

This change takes effect immediately. When you go to the **Virtual Services** browser, Flex Path report icons now appear next to applicable service objects in the browser.

Enabling or Disabling Reactor on a Port or Server

If a service object applies a processing task or validation step to messages that is not supported by the Reactor, the Reactor hands off the message to the Flex Path automatically. In some cases, however, you may want to bypass Reactor handling entirely. In production systems, Reactor should not be used without first performing careful interoperability testing with the external client and service.

Disabling Reactor handling at the port ensures that the Flex Path rather than Reactor listens for requests and passes responses back to the client on the port. Similarly, disabling the Reactor handling on the server object ensure that outgoing requests and incoming responses are handled by Flex Path listeners rather than the Reactor.

Enabling Reactor Handling on a Port

A port object can be configured so that Reactor handling is bypassed for all messages on the port. In this configuration, the standard HTTP listener, http-server, receives incoming requests and sends response messages to the client.

To enable or disable Reactor listening on a port:

-
- Step 1** In the ACE XML Manager console, click **HTTP Ports & Hostnames** on the navigation menu.
In the port list, the Flex Path column indicates whether the Reactor is currently active for the port:
- A dash means that the Reactor is enabled.
 - A checkmark indicates that the Reactor is disabled.
- Step 2** To change the setting, click the **edit** link next to the port object.
- Step 3** Use the **Always Use Flex Path** option to control Reactor listening for this port. If selected, the Reactor is disabled on the port.
- Step 4** Click **Save Changes** to commit your change to the working policy.
-

Once deployed, requests for services that use the port object are handled by either by the Flex Path rather than the Reactor.

Enabling Reactor Handling on a Server

Like a port object, a server definition in the policy can be configured so that the Reactor is either enabled or disabled for communication with the server. If Reactor is disabled, the usual HTTP handler process, `http-server`, exchanges messages with the backend server.

You can also enable or disable Reactor handling on the consumer side (that is, at the port), however, specifying the option on the server allows you individualize this behavior by server.

To enable or disable the use of Reactor on a server:

-
- Step 1** In the ACE XML Manager, click **HTTP Servers** in the navigation menu.
 - Step 2** Click the **view** link next to the server object.
If Flex Path handling is already enabled, **always use Flex Path** appears in the general settings.
 - Step 3** To change the setting, click the **Edit** link on the **General** header.
 - Step 4** Use the **Always Use Flex Path** option to control Reactor listening for this port. If enabled, the compatibility mode is on, meaning that the Reactor is disabled on the server. If not selected, the Reactor sends requests to the server and listens for the responses.
 - Step 5** Click **Save Changes** to commit your change to the working policy.
-

Configuring Reactor Message Format Defense

While the Reactor does not enforce the standard Gateway content screening or denial-of-service rules, it does support format defense. Format defense is a set of configurable rules applicable to message structure that the Reactor can apply to message traffic.

These rules cover, for example, settings maximums on the size of the message, the number of elements, the size of attributes, and so on. These can be used to prevent the types of attacks for which XML processors may be vulnerable.

To be able to apply format defenses to message traffic for an HTTP Get or Post Body service definition, the message specification for those services must indicate that the content is to be treated as XML. Also, well-formedness checking must be enabled on the service definition.

To configure Reactor message screening:

-
- Step 1** In the ACE XML Manager console, click the **System Management** link on the navigation menu.
 - Step 2** Under the ACE XML Gateway header portion of the page, click the **I/O process settings** link.
 - Step 3** Scroll down, if necessary, until the **Reactor** settings are visible.
 - Step 4** Use the Reactor settings to define rules to be enforced on the traffic handled by the Reactor.
For details on these settings, open the online help from the **I/O process settings** page.
 - Step 5** Click **Save Changes** to have your changes saved to the working policy.
-

Once the policy is deployed, incoming requests that do not meet the requirements you have configured are blocked by the Reactor.

