SWIFTNet HTTP Server Adapter

The following table provides an overview of the SWIFTNet HTTP Server adapter:

System name	SWIFTNetHTTPServerAdapter
Graphical Process Modeler (GPM) category	None
Description	Processes HTTP requests from trading partners using a Perimeter server.
Business usage	Use this adapter to communicate with MEFG SWIFTNet Server using HTTP protocol, to receive request/send response from/to the SWIFTNet network. **Note:** You will also need to configure this adapter if you are receiving Inbound CHIPS messages (if you are using the SWIFT transport mode) only when an SSL connection between Application and the SWIFTNet MEFG Server is required.
Usage example	All the URLs in this adapter have been preconfigured to receive all types of requests from the SWIFTNet MEFG Server. Each URL will initiate a specific business process to process the request and will return the response accordingly to the SWIFTNet MEFG Server.
Preconfigured?	This instance is preconfigured and installed with Application. By default this instance uses a local-mode Perimeter server.
Requires third party files?	No
Platform availability	All supported Application platforms
Related services	This adapter must be used in conjunction with the HTTP Respond service (which is the only way to return an HTTP response to a request waiting at a particular adapter instance).
Application requirements	When this adapter is configured with a non-local-mode Perimeter server, the Perimeter server must be installed and running. This Perimeter server is typically installed in a DMZ environment, separated from Application by a firewall. SSL is not supported on the AIX 5.2 or 5.3 operating systems for the connection between the SWIFTNet MEFG Server and the following service or adapters: SWIFTNet Client service, SWIFTNet HTTP Server adapter, and SWIFTNet Server adapter. Please note that this does not impact outbound or inbound SSL connectivity between the SWIFTAlliance Gateway (SAG) and SWIFTNet, because secure transmissions to the host are supported.
Initiates business processes?	This adapter can find the name of a business process that is configured for a particular URL, initiate that business process, and wait for the response.
Invocation	Is not invoked by a business process. To return a response, use the HTTP Respond service.
Business process context considerations	When a business process is initiated as a result of an HTTP request, the initial context process data contains the transport-instance-id and transport-session-id, information necessary for the HTTP Respond service to return the HTTP response. Process data also contains any query parameters in the URL.
Returned status values	None

Restrictions	WAR file deployment functionality does not work on WebSphere.
Persistence level	None
Testing considerations	Debug information related to this adapter can be found in http.log.

How the SWIFTNet HTTP Server Adapter Works

The SWIFTNet HTTP Server adapter receives data from a SWIFTNet trading partner through the SWIFTNet MEFG Server using HTTP. This adapter initiates a preconfigured SWIFTNet business process after receiving a request from the SWIFTNet MEFG Server. The preconfigured business process processes the request accordingly and it invokes the HTTP Respond Service, which sends the response to the SWIFTNet MEFG Server, to be forwarded to the respective SWIFTNet trading partner.

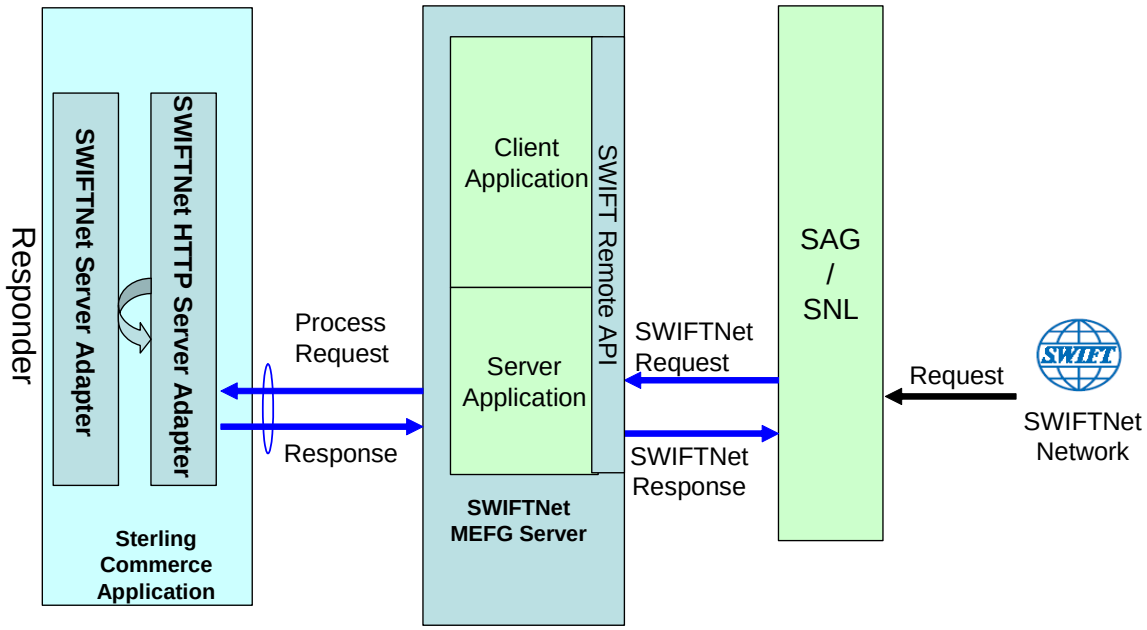
Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications on the Internet for activities such as Web browsing, e-mail, Internet faxing, instant messaging, and other data transfers.

SSL provides endpoint authentication and communications privacy over the Internet using cryptography. When you use SSL, usually only the server is authenticated (the client is not authenticated). The authentication of the server ensures that the end user (which may be a person or an application such as a Web browser) knows exactly with whom he or she is communicating. Once the server is authenticated, all the data communicated is encrypted and secured between the client and server only.

Application provides you with the ability to set up SSL in a loopback between the SWIFTNet HTTP Server and the SWIFTNet MEFG Server, so both ends of the communication are secure. You can also initiate or receive an InterAct or FileAct request using SSL (another form of loopback).

If you use the SWIFTNet HTTP Server adapter in conjunction with the SWIFTNet Server adapter to use Secure Sockets Layer (SSL), the SWIFTNet HTTP Server adapter accepts the forwarded request from the SWIFTNet MEFG Server, and provides secure authentication.

This diagram illustrates the process flow between Application and the SWIFTNet network through the SWIFTNet MEFG Server (using the SWIFTNet HTTP Server adapter for SSL):



Example

Your trading partner sends a SWIFTNet message to your company, through the SWIFTNet network. It is received by the SWIFTNet MEFG Server, which forwards the request to SWIFTNet HTTP Server adapter.

Depending on the type of request, the SWIFTNet MEFG Server sends the data to the specific URI using an HTTP request. When the request is received and passed to the SWIFTNet HTTP Server adapter, it invokes the preconfigured SWIFTNet business process. The adapter collects the transport-instance-id and transport-session-id from the initial request, and places the information into process data.

The adapter then initiates the business process, and the HTTP request connection is put into a wait state while the business process completes. Once complete, the HTTP Respond service is called and uses the transport-instance-id and transport-session-id that were stored in process data to send a reply on the same connection that the request came in on.

Implementing the SWIFTNet HTTP Server Adapter

To implement the SWIFTNet HTTP Server adapter, complete the following tasks:

1. Create a SWIFTNet HTTP Server adapter configuration. For information, see *Managing Services and Adapters*.
2. Configure the SWIFTNet HTTP Server adapter. For information, see *Configuring the SWIFTNet HTTP Server Adapter*.

Note: This adapter instance is preconfigured. You only need to configure this adapter when you want to set up SSL communication between this adapter and the SWIFTNet MEFG Server.

Configuring the SWIFTNet HTTP Server Adapter

To configure the SWIFTNet HTTP Server adapter, you must specify field settings in Application:

Field	Description
Name	Unique and meaningful name for the adapter configuration. Required.
Description	Meaningful description for the adapter configuration, for reference purposes. Required.
Select a Group	Leave this set to: ◆ None – You do not want to include this configuration in a group at this time. **Note:** Do not use the SWIFTNet HTTP Server adapter in groups.
HTTP Listen Port	The port number on which the Perimeter server process listens for connections from external trading partner HTTP clients. If a local-mode Perimeter server is chosen, this listen port is bound on the local computer. Valid values are 1 through 65536. On many operating systems, only the root user can bind on ports 1 through 1024. Required.
Perimeter Server Name	List of available Perimeter servers, including local-mode Perimeter servers. Required. Default is **node 1 & local** Perimeter server.
Total Business Process queue depth threshold	Specify the maximum number of HTTP connections that can be waiting for a business process to complete. Exceeding this value will result in an HTTP 503 response. Required. **Note:** If too many business processes are allowed at any one time, you may experience performance issues. Therefore, you should not input too high a value for this parameter.
Document Storage	Where to store the body of the request document. Valid values are: ◆ System Default ◆ Database (this is the default) ◆ File System Required. **Note:** For more information about document storage types, see *Managing Services and Adapters*.
User Authentication Required	Whether to enable HTTP basic authentication. Valid values are: ◆ Yes – A connection must pass HTTP basic authentication to be serviced. ◆ No – HTTP basic authentication is not to be used. **Caution:** Always select **No**. Default is No. Required.

Field	Description
Use SSL	Whether SSL Server authentication must be enabled. Valid values are: ◆ Must – SSL is enabled ◆ None – SSL is disabled Default is None. Required. **Note:** User Authentication without SSL results in a weak security configuration.
System Certificate	Select a system certificate from the list. This is the private key that the SSL server will use. Required if Use SSL is set to Must.
Cipher Strength	Specifies the strength of the algorithms (cipher suites) used to encrypt data. Valid values are: ◆ STRONG – Required if Use SSL is Must ◆ ALL – All cipher strengths are supported (default) ◆ WEAK – Often required for international trade, because government regulations prohibit STRONG encryption from being exported Default is ALL. Required if SSL is checked.
CA Certificate	Not supported by the SWIFTNet MEFG Server because it only supports server authentication.
URI (Add | Edit | Delete)	Click **Add** to add a new URI. Or, click **Edit** or **Delete** next to an existing URI to revise or remove it.
URI	Uniform Resource Indicator (URI) representing incoming requests. Add one or more URIs to represent incoming requests and the business process or Web application (represented as a WAR file) associated with each. Required. Only displayed if you click **Add** or **Edit** on the URI page.
Launch BP or WAR	Whether the URI launches a business process or WAR file. Default is Business Process. Required. Only displayed if you click **Add** or **Edit** on the URI page.
Business Process	Specifies business process to be launched by URI. Select from the list of available business processes. Required if BP is selected for Launch BP or WAR File field. Only displayed if you click **Add** or **Edit** on the URI page.
Send Raw Messages	Whether the raw message is presented to the business process. The term raw denotes that the primary document associated with the business process contains HTTP headers. Valid values are: ◆ Yes – Both the HTTP headers and the entity body are copied to the body of the business process document before the business process is started. This setting is required for EDIINT AS2, RosettaNet, and ebXML. ◆ No – Just the HTTP entity body is copied to the body buffer of the business process document. The headers are not available to the business process. Default is No. Required if BP is selected for Launch BP or WAR File field. Only displayed if you click **Add** or **Edit** on the URI page.

Field	Description
Run BP in sync mode	Whether to invoke Web services in synchronous mode. Valid values are: ◆ Yes – HTTP Server Adapter bootstraps the BP in synchronous mode. HTTP Server Adapter executes the BP in the same thread. ◆ No – HTTP Server Adapter bootstraps the BP asynchronous mode. Default is No. Required if BP is to be run in synchronous mode. Only displayed if you click **Add** or **Edit** on the URI page.
Enter WAR File Path	Specifies WAR file to be launched by URI. Valid value is any accessible path. Required if WAR File is selected for Launch BP or WAR File field. Or, you can Load a System Generated War File if at least one system-generated WAR file exists. Only displayed if you click **Add** or **Edit** on the URI page.

Output from Adapter to Business Process

The following table describes the output from the SWIFTNet HTTP Server adapter to the business process:

Field Name	Description
http-request-uri	Target URI as specified by the Trading Partner. Required for applications that need it. For example, SOAP.
transport-instance-id	Identifies the specific instance of the SWIFTNet HTTP Server adapter on which the request was received. Valid value is a non-empty string that should not be fabricated. Each value is created for an SWIFTNet HTTP Server adapter instance. Required.
transport-session-id	Transport Session ID. Identifies the specific inbound connection on the SWIFTNet HTTP Server adapter (identified by the transport instance id) on which the request was received and to which the response must be returned. Valid value is a non-empty string that should not be fabricated. Each value is created by an SWIFTNet HTTP Server adapter instance for an inbound HTTP session. Required.
b2b-protocol	Identifies the protocol type, with a value of **http**
SyncModeBP	Indicates whether the BP has been bootstrapped in synchronous mode or not. Valid values are true and false.

Initial Process Data XML Document Example

The following example shows how the initial process data XML document looks:

```
<?xml version="1.0" encoding="UTF-8"?>
<ProcessData>
  <PrimaryDocument SCIObjectID="server1:b1aebf:fa40ae79ca:-7209"/>
  <b2b-protocol>http</b2b-protocol>
  <transport-instance-id>TestHTTPServerAdapter-insecure_HttpAdapter_node1</transport
-instance-id>
  <transport-session-id>Thu Jan 22 22:04:16 EST 2004:5</transport-session-id>
```

```
  <http-request-uri>/reflect</http-request-uri>
</ProcessData>
```

Activity Types for This Adapter

This adapter reports the following activities to the Services Controller for Service/Adapter Monitoring:

- Get—retrieves whatever information is identified by the http-request-uri.
- Post—requests that the origin server accept the entity enclosed in the request as a new subordinate of the resource identified by the URI in the Request-Line.

Enhancing SWIFTNet HTTP Server Adapter Performance

To improve performance, the SWIFTNet HTTP Server adapter enables you to specify a range of threads for handling events. The range, which is specified in the http.properties file, includes a Min Thread value and Max Thread value. If the Max Thread value is reached, any additional connection requests fail. The http.properties file is located in the properties folder under your Application installation directory.