

AppSentinels API Security Platform

IBM Datapower Gateway Integration

Revision	Date Modified	Author	Comments
1.0	19-Sep-24	Arun	Initial spec for IBM Datapower Gateway Integration
1.1	17-Dec-24	Arun	Update covering unified GatewayScripts for inline and OOB modes
1.2	12-Mar-24	Arun	Update controller health check and message queue support in OOB mode
1.3	10-Apr-25	Arun	Add API Connect policy integration reference

Contents

AppSentinels sensor for IBM Datapower Gateway	4
Policy modes	4
Transparent or Out of Band (OOB) mode	4
Auth mode	4
Log forwarding to AppSentinels Edge Controller in OOB mode	4
AppSentinels controller health check	5
IBM Message Queue (IBM MQ)	5
GatewayScript integration in IBM API Connect	6
TLS Client profile	6
Datapower API Gateway	7
GatewayScripts	7
Edit configuration in GatewayScripts	8
Checkpoint existing configuration	11
Upload GatewayScripts to Datapower Gateway	12
Define Assembly rule	15
Configure API Gateway policy	17
Configure health check	19
Configure message queue	23
Datapower Multi-Protocol Gateway (MPGW)	27
GatewayScripts	27
Edit configuration in GatewayScripts	28
Policy configuration	29
XML Manager scheduled policy rules for IBM MQ consumer and health check	32
Troubleshooting	32

AppSentinels sensor for IBM Datapower Gateway

This document describes the steps to deploy AppSentinels policy in IBM Datapower Gateway. AppSentinels supports Datapower Gateway in API Gateway mode as well as Multi-Protocol Gateway mode. This document covers AppSentinels policy deployment for both Datapower API Gateway and Multi-Protocol Gateway.

AppSentinels provides the Datapower Gateway policies in the form of JavaScript code, called GatewayScript in Datapower Gateway. GatewayScript defines the action in Datapower assembly rules. AppSentinels inbound GatewayScript serves the purpose of defining the *pre-processing* assembly rule in Datapower API Gateway and *client to server* rule in Multi-Protocol Gateway. This GatewayScript executes on the API request. Similarly, the outbound GatewayScript, which executes on the API response, serves the purpose of defining *post-processing* assembly rule in the Datapower API Gateway and *server to client* rule in Multi-Protocol Gateway.

In Multi-Protocol Gateway, AppSentinels GatewayScript manages the errors in Auth mode to send appropriate responses to the client in case AppSentinels policy blocks the request.

Policy modes

AppSentinels sensor policy supports in following modes:

Transparent or Out of Band (OOB) mode

AppSentinels sensor captures the request and response headers and body and forwards the captured data to AppSentinels Edge Controller asynchronously. It does not enforce any blocking policy.

Auth mode

AppSentinels sensor can enforce threat actor policy actions in auth mode. It captures the request and forwards the request data to AppSentinels Edge Controller, which responds with the policy action on the API request. Depending on the action received from Controller, the sensor allows or blocks the request. If AppSentinels policy allows the request, Controller forwards the response data to the Controller.

It is important to note that the JavaScript code that constitutes the policy is implemented in the same files for auth mode and transparent mode and the policy mode is defined using a configuration variable. The method to deploy the policy is also identical for the two modes. The policy deployment steps are described in subsequent sections.

Log forwarding to AppSentinels Edge Controller in OOB mode

By default, AppSentinels GatewayScripts forward logs to AppSentinels controller directly using HTTPS or HTTP protocol. The logs are not buffered or batched and are forwarded immediately to AppSentinels controller. The GatewayScripts invoke IBM Datapower *urlopen.open()* method to send logs to AppSentinels controller. The downside of this mode is

that `urlopen.open()` method is synchronous and it blocks the Datapower Gateway while sending the logs. This impacts the latency of the requests, specifically if the AppSentinels controller is not reachable from the Datapower Gateway, then the GatewayScripts introduces a latency of one second, which is the minimum time to wait for completion of send operation.

To minimize the impact of log forwarding in transparent mode, the following mechanisms are supported for production environment to avoid latency issues.

AppSentinels controller health check

AppSentinels health check GatewayScript is invoked periodically every second to probe the reachability of the AppSentinels controller. If the AppSentinels controller is not reachable, then AppSentinels Controller is marked down, and the policy GatewayScripts do not attempt to send logs to AppSentinels controller. The health check GatewayScript is invoked periodically using the Datapower XML Manager periodic schedule policy rule.

The health check GatewayScript invokes `/health` endpoint of the AppSentinels controller to check if it is reachable. If the AppSentinels controller responds (even with a failure response), the AppSentinels controller is considered reachable and the policy GatewayScripts attempt to send logs to AppSentinels controller.

By default, AppSentinels policy GatewayScripts do not send the log to AppSentinels controller if the AppSentinels controller did not respond to health check for two seconds. This duration is configurable, and it is also possible to configure the periodicity of the XML Manager policy rule, but the granularity is limited to seconds.

It should also be noted that with default configuration, AppSentinels policy GatewayScripts continue to send logs to AppSentinels controller for two seconds after AppSentinels controller becomes unreachable, so the clients observe a latency of one second during this time window of two seconds.

IBM Message Queue (IBM MQ)

AppSentinels GatewayScripts send logs to AppSentinels controller via IBM message queue. A separate message queue consumer GatewayScript is invoked periodically every second to consume the logs from IBM message queue and send those to AppSentinels controller. This GatewayScript is invoked periodically using the Datapower XML Manager periodic schedule policy rule. In case the AppSentinels controller is not reachable, then the logs are buffered in the queue and sent to AppSentinels controller once the AppSentinels controller becomes reachable. Thus, there is no impact on the latency of the client requests.

Even when the controller remains unreachable for longer duration, the message queue becomes full, and the logs are not appended to the queue. the logs are dropped, but there is no impact on the latency of the client requests.

The message queue consumer GatewayScript is invoked every second and in each iteration, it picks up to 500 logs from the queue and sends them to AppSentinels controller. In case if it fails to send the logs to AppSentinels controller, it stops immediately, thus if AppSentinels

controller is not reachable, the consumer GatewayScript picks up one log from the queue and drops it due to failure to send the log to AppSentinels controller. Please note that the maximum number of logs to be picked up in each iteration is configurable and the default value is 500.

GatewayScript integration with IBM API Connect

This document mainly focuses on GatewayScript deployment in IBM Datapower in API Gateway and Multi-Protocol Gateway configuration. IBM Datapower gateway is commonly used as API Gateway in IBM API Connect. AppSentinels GatewayScripts can be integrated with API Connect (if it is using IBM Datapower as API Gateway). Please refer to ***IBM-API-Connect-Policy-Integration.pdf*** for integration with IBM API Connect.

To configure AppSentinels GatewayScript policies in IBM API Connect, please refer to the following sections in this document:

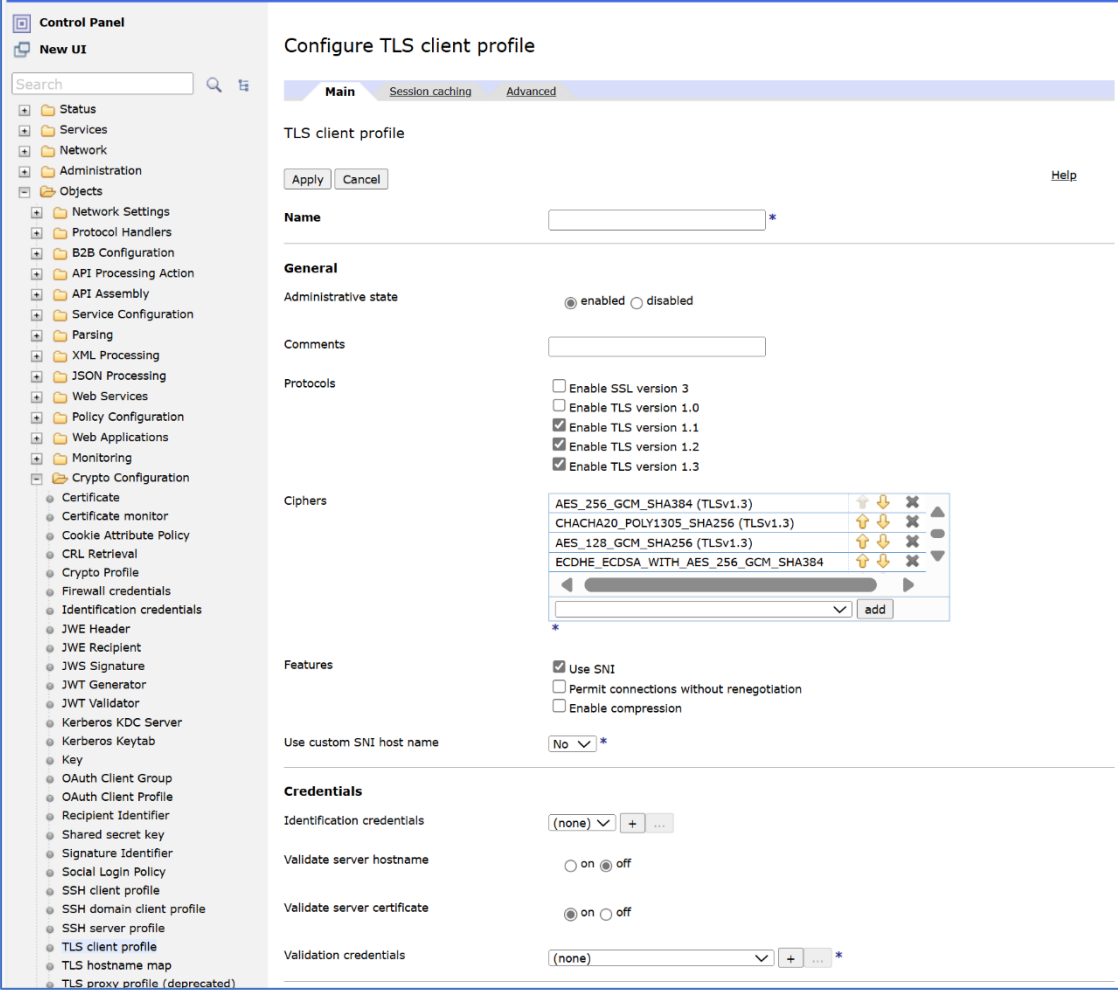
- TLS client profile creation
- AppSentinels GatewayScript configuration variable settings in this document

The other configuration covered in the document is not relevant from API Connect perspective.

TLS Client profile

AppSentinels Controller supports HTTPS based communication with sensor. The default mode of communication is *http*, it can be changed to *https* in the GatewayScripts configuration (as described in subsequent sections). Please configure TLS client profile in **Objects > Crypto Configuration > TLS client profile** for enabling HTTPS between Datapower Gateway and AppSentinels Controller in API Gateway as well as Multi-Protocol Gateway.

The TLS client profile can be created by clicking on **Add** button in **Configure TLS client profile** dialog, this opens the TLS client profile configuration dialog as shown below.



Control Panel
New UI

Search

- Status
- Services
- Network
- Administration
- Objects
 - Network Settings
 - Protocol Handlers
 - B2B Configuration
 - API Processing Action
 - API Assembly
 - Service Configuration
 - Parsing
 - XML Processing
 - JSON Processing
 - Web Services
 - Policy Configuration
 - Web Applications
 - Monitoring
 - Crypto Configuration
 - Certificate
 - Certificate monitor
 - Cookie Attribute Policy
 - CRL Retrieval
 - Crypto Profile
 - Firewall credentials
 - Identification credentials
 - JWE Header
 - JWE Recipient
 - JWS Signature
 - JWT Generator
 - JWT Validator
 - Kerberos KDC Server
 - Kerberos Keytab
 - Key
 - OAuth Client Group
 - OAuth Client Profile
 - Recipient Identifier
 - Shared secret key
 - Signature Identifier
 - Social Login Policy
 - SSH client profile
 - SSH domain client profile
 - SSH server profile
 - TLS client profile
 - TLS hostname map
 - TLS proxy profile (deprecated)

Configure TLS client profile

Main Session caching Advanced

TLS client profile

Apply Cancel Help

Name *

General

Administrative state ☒ enabled ☐ disabled

Comments

Protocols

- ☐ Enable SSL version 3
- ☐ Enable TLS version 1.0
- ☒ Enable TLS version 1.1
- ☒ Enable TLS version 1.2
- ☒ Enable TLS version 1.3

Ciphers

AES_256_GCM_SHA384 (TLSv1.3)	↑	↓	×
CHACHA20_POLY1305_SHA256 (TLSv1.3)	↑	↓	×
AES_128_GCM_SHA256 (TLSv1.3)	↑	↓	×
ECDSA_WITH_AES_256_GCM_SHA384	↑	↓	×

Features

- ☒ Use SNI
- ☐ Permit connections without renegotiation
- ☐ Enable compression

Use custom SNI host name No *

Credentials

Identification credentials (none) + ...

Validate server hostname ☐ on ☒ off

Validate server certificate ☒ on ☐ off

Validation credentials (none) + ... *

- Please specify the **Name** of the TLS client profile.
- Enable the **Use SNI** checkbox in **Features** configuration.
- Turn on **Validate server certificate** under **Credentials** and configure the CA certificate in **Validation credentials** configuration.
- If AppSentinels Controller presents a self-signed certificate (which is possible in test and PoC environments), turn off server certificate validation by selecting the **off** button in **Validate server certificate** configuration.
- Click on **Apply** and **Save** buttons.

Datapower API Gateway

GatewayScripts

Following table lists the AppSentinels GatewayScripts for inline and OOB deployment modes.

GatewayScript name	API Gateway policy rule
appsentinels-pre-proc.js	Preprocessing rule
appsentinels-post-proc.js	Postprocessing rule

appsentinels health check.js	Health check (XML Manager periodic schedule rule)
appsentinels mq.js	Message queue consumer (XML Manager periodic schedule rule)

It should be noted that the same GatewayScripts are used for inline (or auth) mode and OOB (or transparent) mode. The policy mode (auth or transparent) is defined using a configuration variable defined in the GatewayScripts. In subsequent sections, the terms *request policy GatewayScript* and *response policy GatewayScript* refer to request and response GatewayScripts, respectively. please select the appropriate files depending on the policy mode.

Edit configuration in GatewayScripts

Each of the GatewayScripts has a configuration section containing definitions of the attributes used by the GatewayScripts. The following picture displays configuration parameters for the `appsentinels_apigw_response_policy.js` GatewayScript. Other GatewayScripts have similar configuration parameter definitions.

```
// Configuration
const config = {
  // Deployment mode - 'auth' or 'transparent'
  deploymentMode: 'transparent',

  // Appsentinels controller configuration
  controllerHost: '<controller-url>',
  controllerPort: '9004',
  scheme: 'http', // or 'https'

  // TLS client profile name - needed for HTTPS communication
  tlsClientProfileName: 'client:<TLS client profile name>',

  // Payload configuration
  maxSupportedPayload: 131072,
  supportedContentTypes: ["json", "xml", "graphql", "form"],

  // Sensor visibility configuration
  pluginVersion: '1.0.0',
  sensorHostname: 'datapower-gateway',
  sensorInstanceName: 'datapower-apigw',

  // Health check enabled or not
  healthCheckDisabled: true,
  // Don't send log if health check response not received within this threshold
  healthCheckThreshold: 2000, // in milliseconds

  // Configuration for IBM message queue
  mqPostLogToQueue: false,
  mqQueueManager: '<queue-manager-name>',
  mqQueueName: '<queue-name>',
  mqScheme: 'idgmq'
}
```

Following points summarize steps to update configuration parameter

- Change the *deploymentMode* to 'auth' if inline (or auth) mode policy needs to be deployed.
- Controller URL is the only mandatory configuration parameter. So, find out AppSentinels Edge Controller DNS name or IP address.
- Open the request policy GatewayScript file.
- Search for <controller-url> in the file and replace it with AppSentinels Edge Controller DNS name or IP address.
- If Datapower Gateway communicates with AppSentinels Controller over HTTPS, then update the *scheme* and *tlsClientProfileName*. Please configure a TLS client profile in **Objects > Crypto Configuration > TLS client profile** in Datapower Gateway configuration.

- The parameters *sensorHostName* and *sensorInstanceName* are used for sensor visibility. Please modify the default values of these parameters appropriately depending on sensor visibility requirement.
- To enable AppSentinels controller health check –
 - Set *healthCheckDisabled* flag to *false*.
 - The parameter *healthCheckThreshold* defines the maximum time to wait for AppSentinels Controller to respond to health check request. Modify this if the default configuration is not suitable.
 - Configure the configuration parameters in *appsentinels_health_check.js* GatewayScript, as shown below.

```
// Configuration
const config = {
  // Health check enabled
  enabled: true,

  // Appsentinels controller configuration
  controllerHost: '<controller-url>',
  controllerPort: '9004',
  scheme: 'http', // or 'https'

  // TLS client profile name - needed for HTTPS communication
  tlsClientProfileName: '<TLS client profile name>',
}
```

- The configuration of *controllerHost*, *controllerPort*, *scheme* and *tlsClientProfileName* is same as that in the response policy GatewayScript. Keep the *enabled* flag *true* to enable health check.
- To enable log forwarding via IBM MQ –
 - Set *mqPostLogToQueue* to *true*.
 - Set *mqQueueManager* to IBM MQ Manager name, which is same as the IBM MQ v9+ queue manager created in IBM Datapower to communicate with IBM MQ.
 - Set *mqQueueName* to the name of the queue in IBM MQ to receive AppSentinels logs.
 - The parameter *mqScheme* defines the scheme used to communicate with IBM MQ, the default value is *idgmq*.
 - Configure the parameters in the *appsentinels_mq.js* GatewayScript, as shown below.

```
// Configuration
const config = {
  // Message queue enabled
  enabled: true,

  // Appsentinels controller configuration
  controllerHost: '<controller-url>',
  controllerPort: '9004',
  scheme: 'http', // or 'https'

  // TLS client profile name - needed for HTTPS communication
  tlsClientProfileName: 'client:<TLS client profile name>',

  // Configuration for IBM message queue
  mqQueueManager: '<queue-manager-name>',
  mqQueueName: '<queue-name>',
  mqScheme: 'idgmq',
  mqMaxMessagesInEachIteration: 500, // Number of messages to process in each iteration
  mqBatchSize: 8 // Number of messages to process in each batch
}
```

- The configuration of *controllerHost*, *controllerPort*, *scheme* and *tlsClientProfileName* is same as that in the response policy GatewayScript. Keep the *enabled* flag *true* to enable AppSentinels logs via IBM message queue.
- The parameters *mqQueueManager*, *mqQueueName* and *mqScheme* are same as the ones defined in the response policy GatewayScript and are needed to consume the messages from IBM MQ.
- Parameter *mqMaxMessagesInEachIteration* defines the maximum number of messages to process in each periodic iteration.
- The parameter *mqBatchSize* defines the number of AppSentinels API log messages to be sent in one message to AppSentinels Controller.
- The configuration in the request policy GatewayScript is a subset of the configuration described above in the response policy GatewayScript.

Checkpoint existing configuration

Create a checkpoint of the existing working configuration in **Administration > Configuration > Configuration Checkpoints**.

DataPower Gateway admin @ ecf77b4f4a20 9/19/2024, 9:21:42 AM (EDT) WebGUI deprecated, use new UI

Control Panel
New UI

Search

- Status
- Services
- Network
- Administration
 - Main
 - Configuration
 - Application domain
 - Export Configuration
 - Import Configuration
 - Compare Configuration
 - Configuration Checkpoints
 - Access

Configuration Checkpoints

[Refresh List](#)

Name	Time	Actions		
working_apigw	September 6, 2024 12:48:39 AM EDT	Rollback	Remove	Compare
apigw_with_appsentinels_policies	September 9, 2024 8:44:08 AM EDT	Rollback	Remove	Compare

Create a new Configuration Checkpoint

Checkpoint Name: Save Checkpoint

Upload GatewayScripts to Datapower Gateway

Before configuring AppSentinels policy, upload both request policy GatewayScript and response policy GatewayScript to the Datapower Gateway. Please follow the below steps to upload the files.

- Open Datapower UI portal and go to **Administration > Main > File Management**.

DataPower Gateway admin @ ecf77b4f4a20 9/19/2024, 5:51:50 AM (EDT) WebGUI deprecated, use new UI

Control Panel
New UI

Search

- Status
- Services
- Network
- Administration
 - Main
 - File Management
 - System Control
 - Configuration
 - Access
 - Device
 - Storage Devices
 - Debug
 - Miscellaneous
 - Objects

Firmware: IDG.10.6.0.0
 Build: 365335
 Delivery type: Long-term support
 IBM DataPower Gateway
 Copyright IBM Corporation 1999-2024
[View License Agreement](#)

File Management

[Refresh Page](#) [Help](#)

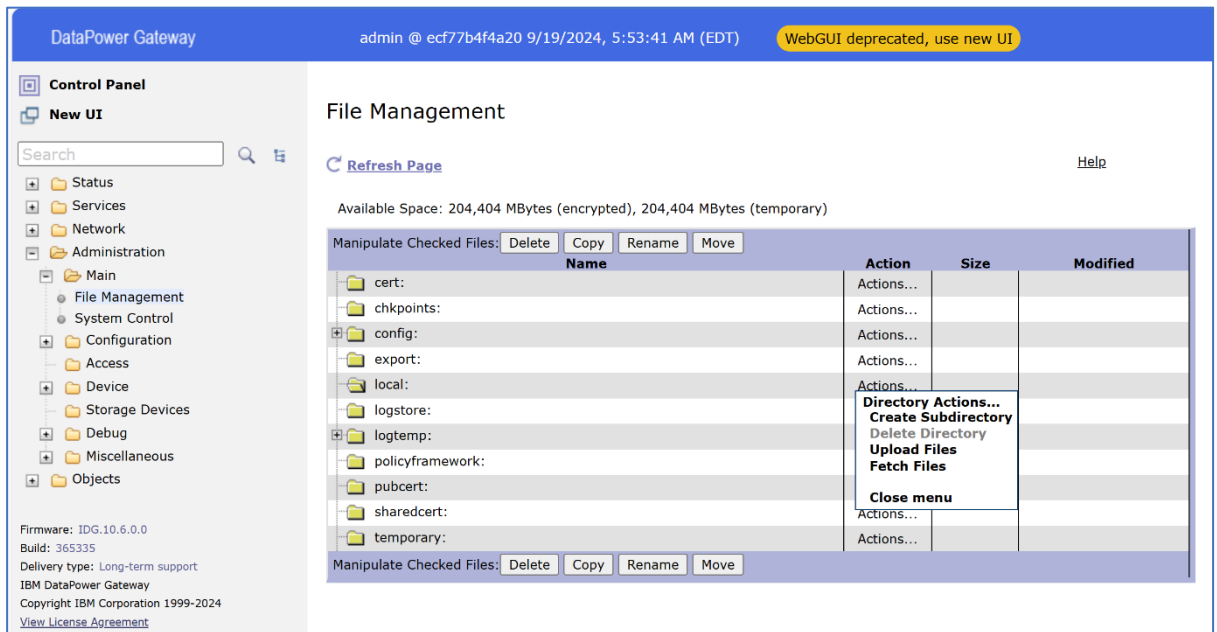
Available Space: 204,404 MBytes (encrypted), 204,404 MBytes (temporary)

Manipulate Checked Files:

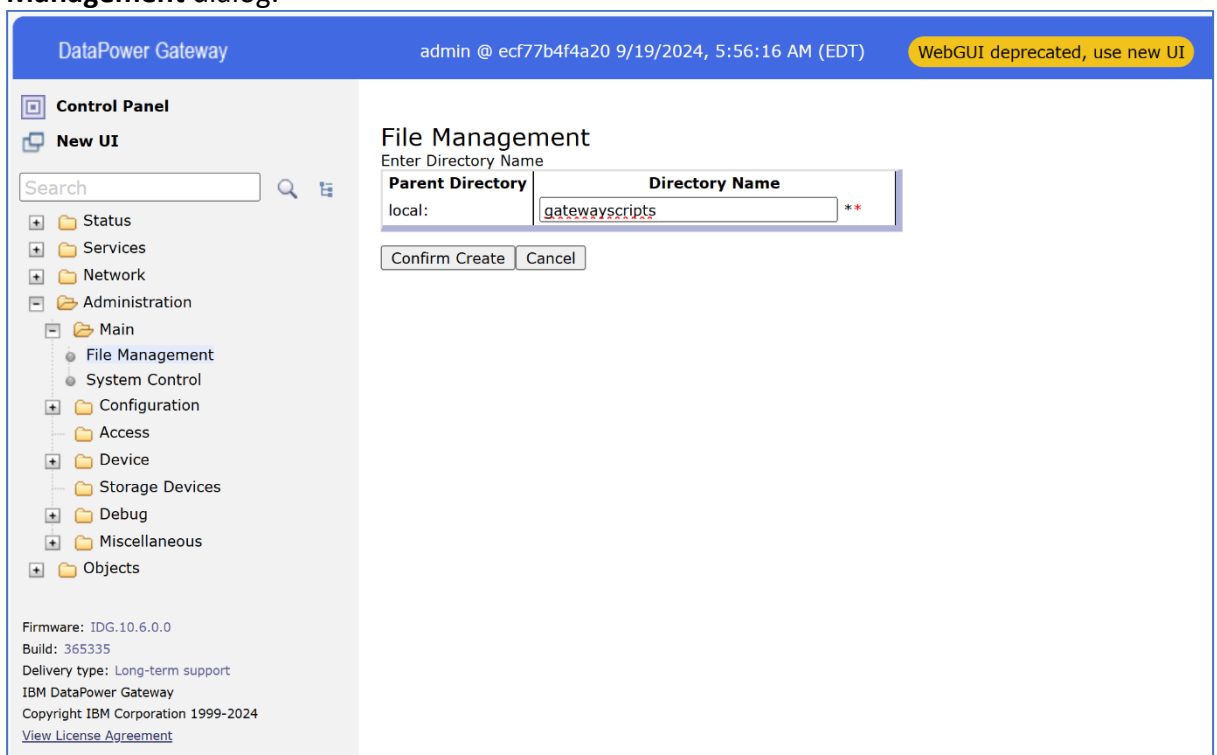
Name	Action	Size	Modified
cert:	Actions...		
chkpoints:	Actions...		
config:	Actions...		
export:	Actions...		
local:	Actions...		
logstore:	Actions...		
logtemp:	Actions...		
policyframework:	Actions...		
pubcert:	Actions...		
sharedcert:	Actions...		
temporary:	Actions...		

Manipulate Checked Files:

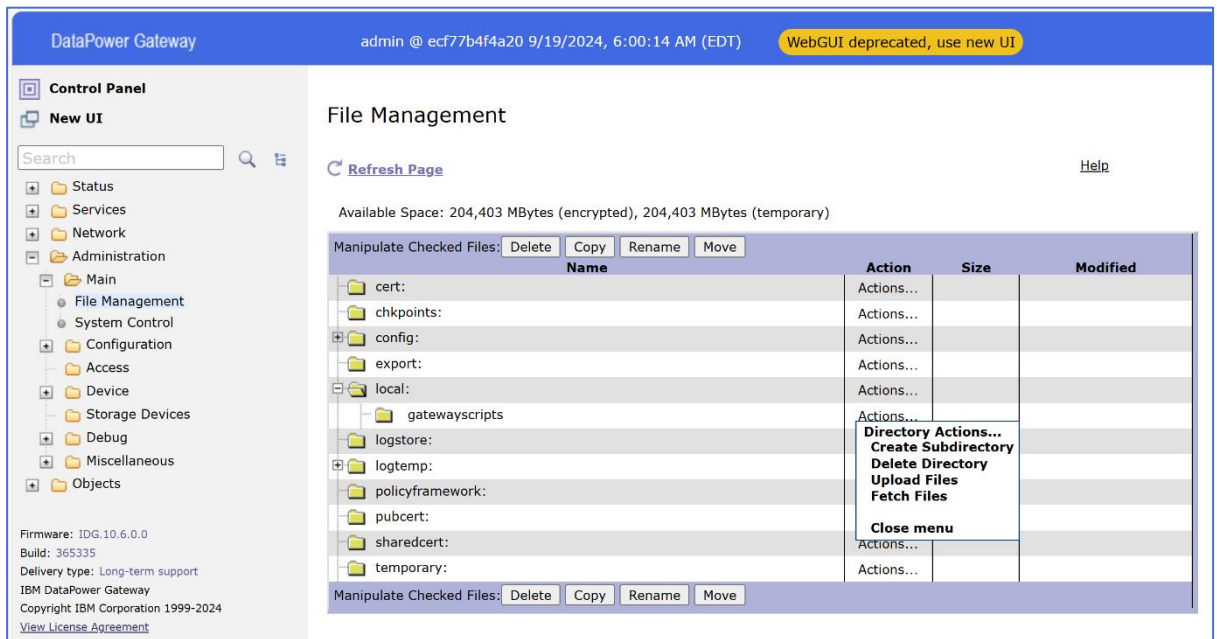
- Select **local:** directory and click on **Actions** corresponding to it, then select **Create Subdirectory** option.



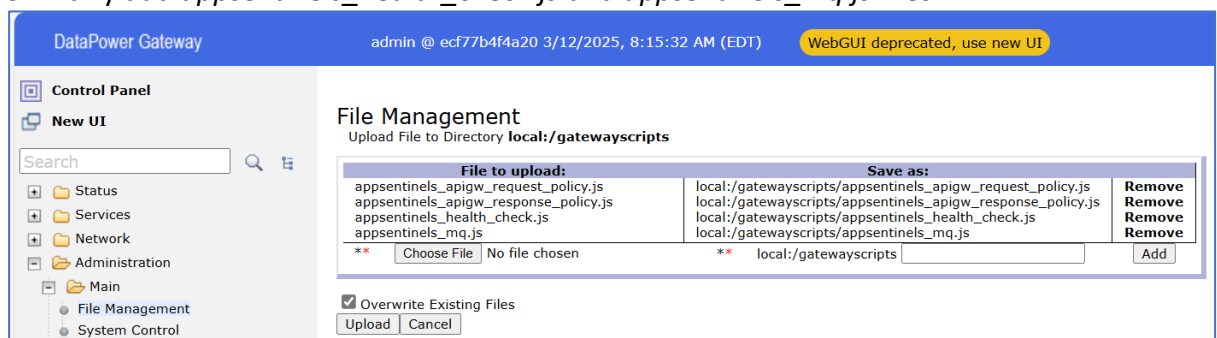
- Create the sub-directory with name **gatewayscripts** and click **Confirm Create**. Check the status of the sub-directory creation operation and press **Continue** to the **File Management** dialog.



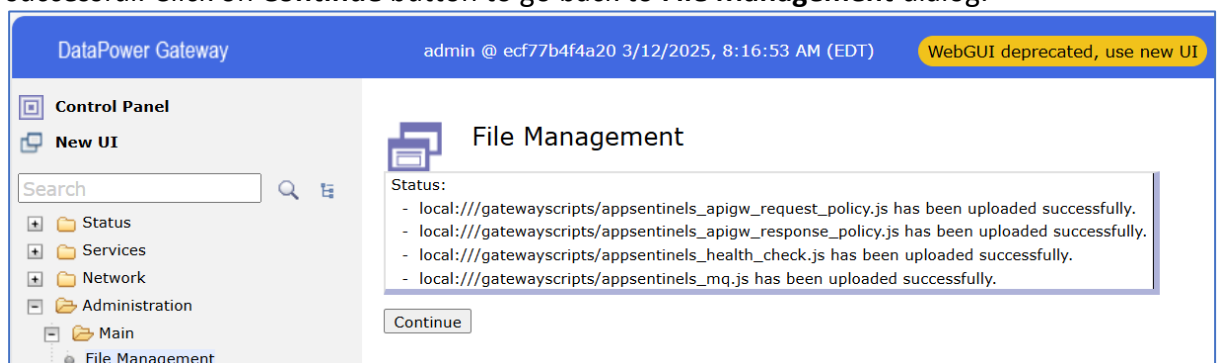
- Expand **local:** and click on **Actions** corresponding to **gatewayscript** sub-directory, select **Upload Files**.



- Click on **Choose File**, select the *appsentinels_apigw_request_policy.js* file (double-click the file name or click **Open** after selecting the file), and click **Add** button.
- Click on **Choose File** again, select the *appsentinels_apigw_response_policy.js* file, and click **Add** button.
- Similarly add *appsentinels_health_check.js* and *appsentinels_mq.js* files.



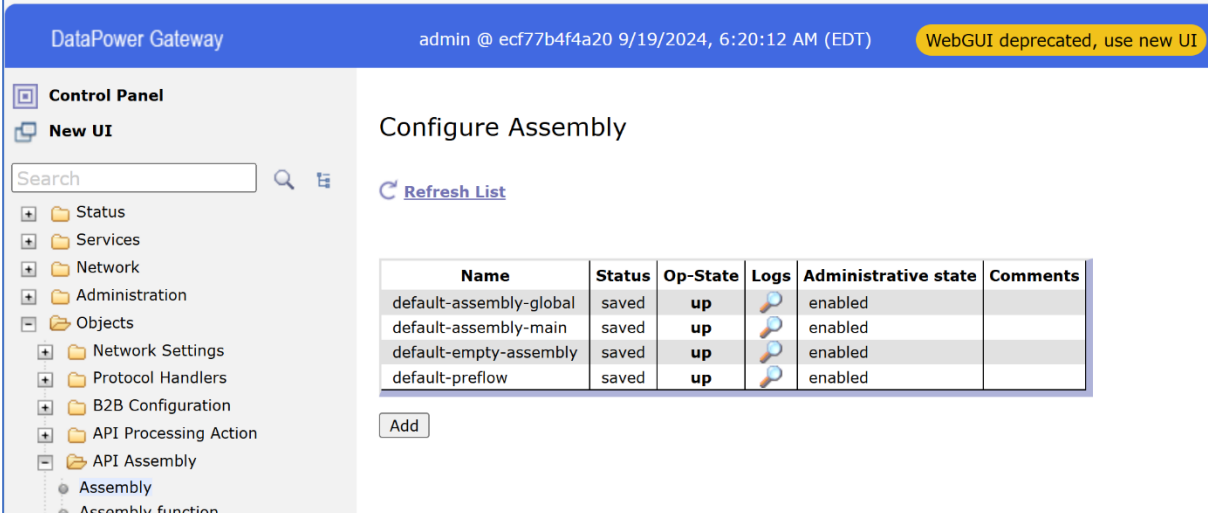
- Select **Overwrite Existing Files** checkbox and click **Upload**. Files upload should be successful. Click on **Continue** button to go back to **File Management** dialog.



Define Assembly rule

The Gateway script file uploaded above define action in the Datapower assembly rules. Please note that the request and response policy GatewayScripts require separate assembly rules, so please execute the steps listed below for both request policy GatewayScript and response policy GatewayScript.

- Go to **Objects > API Assembly > Assembly**.



DataPower Gateway admin @ ecf77b4f4a20 9/19/2024, 6:20:12 AM (EDT) WebGUI deprecated, use new UI

Control Panel
New UI

Search

- Status
- Services
- Network
- Administration
- Objects
 - Network Settings
 - Protocol Handlers
 - B2B Configuration
 - API Processing Action
 - API Assembly
 - Assembly
 - Assembly function

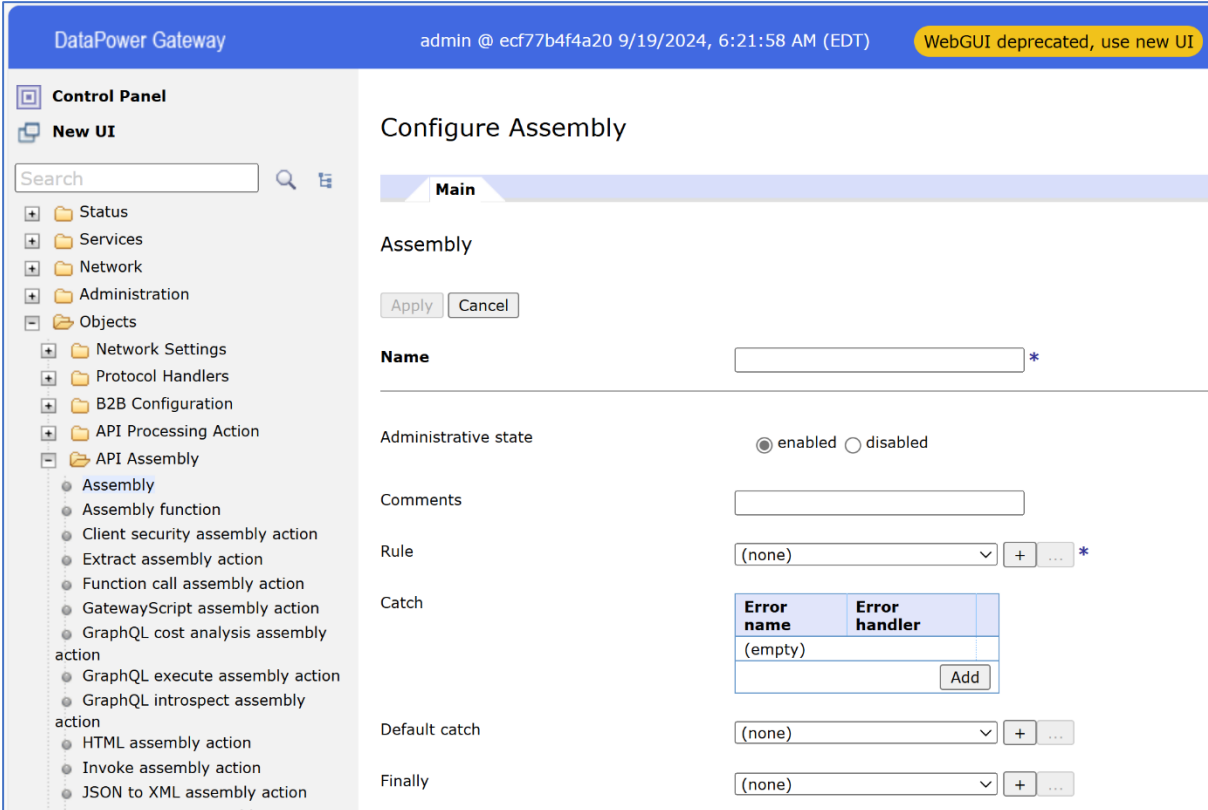
Configure Assembly

[Refresh List](#)

Name	Status	Op-State	Logs	Administrative state	Comments
default-assembly-global	saved	up		enabled	
default-assembly-main	saved	up		enabled	
default-empty-assembly	saved	up		enabled	
default-preflow	saved	up		enabled	

[Add](#)

- In the right pane, click on Add button to define new assembly.



DataPower Gateway admin @ ecf77b4f4a20 9/19/2024, 6:21:58 AM (EDT) WebGUI deprecated, use new UI

Control Panel
New UI

Search

- Status
- Services
- Network
- Administration
- Objects
 - Network Settings
 - Protocol Handlers
 - B2B Configuration
 - API Processing Action
 - API Assembly
 - Assembly
 - Assembly function
 - Client security assembly action
 - Extract assembly action
 - Function call assembly action
 - GatewayScript assembly action
 - GraphQL cost analysis assembly action
 - GraphQL execute assembly action
 - GraphQL introspect assembly action
 - HTML assembly action
 - Invoke assembly action
 - JSON to XML assembly action
 - JWT generate assembly action

Configure Assembly

Main

Assembly

[Apply](#) [Cancel](#)

Name *

Administrative state ☒ enabled ☐ disabled

Comments

Rule (none) [+](#) [...](#) *

Catch

Error name	Error handler
(empty)	

[Add](#)

Default catch (none) [+](#) [...](#)

Finally (none) [+](#) [...](#)

- Specify the **Name** and add a new **Rule** by clicking on + button.

Configure API rule

Main

API rule

[Apply](#)[Cancel](#)[Help](#)**Name** *

Administrative state

☒ enabled ☐ disabled

Comments

Use dynamic actions

☐

API actions

(empty)

 [add](#) [+](#) [...](#)

- In **Configure API rule** dialog (shown below), specify a rule **Name** and add a new **API action** by clicking on the **+** button, and select **GatewayScript assembly action**.

Configure API rule

Main

API rule

[Apply](#)[Cancel](#)**Name**

Administrative state

☒ enabled ☐ disabled

Comments

Use dynamic actions

☐

API actions

(empty)

 [add](#) [+](#) [...](#)

Create a New:

- [CORS API action](#)
- [Client identification API action](#)
- [Execute API action](#)
- [Final API action](#)
- [Rate limit API action \(deprecated\)](#)
- [Result API action](#)
- [Routing API action](#)
- [Security API action](#)
- [Client security assembly action](#)
- [Extract assembly action](#)
- [Function call assembly action](#)
- [GatewayScript assembly action](#)
- [GraphQL cost analysis assembly action](#)
- [GraphQL execute assembly action](#)
- [GraphQL introspect assembly action](#)
- [HTML assembly action](#)
- [Invoke assembly action](#)
- [JWT generate assembly action](#)
- [JWT validate assembly action](#)
- [JSON to XML assembly action](#)
- [Log assembly action](#)
- [Map assembly action](#)
- [OAuth assembly action](#)
- [Parse assembly action](#)
- [Rate limit assembly action](#)
- [Rate limit details assembly action](#)
- [Redact assembly action](#)
- [Set variable assembly action](#)
- [User security assembly action](#)
- [Validate assembly action](#)
- [WSDL assembly action](#)

- In **Configure GatewayScript assembly action** dialog (shown below), specify the **Name** of the action, and specify the **GatewayScript File** path.

Configure GatewayScript assembly action

Main

GatewayScript assembly action

Apply

Cancel

Help

Name

request-rule *

Administrative state

☒ enabled
 ☐ disabled

Comments

Title

Correlation path

GatewayScript file

local:///gatewayscripts/appsentinels *

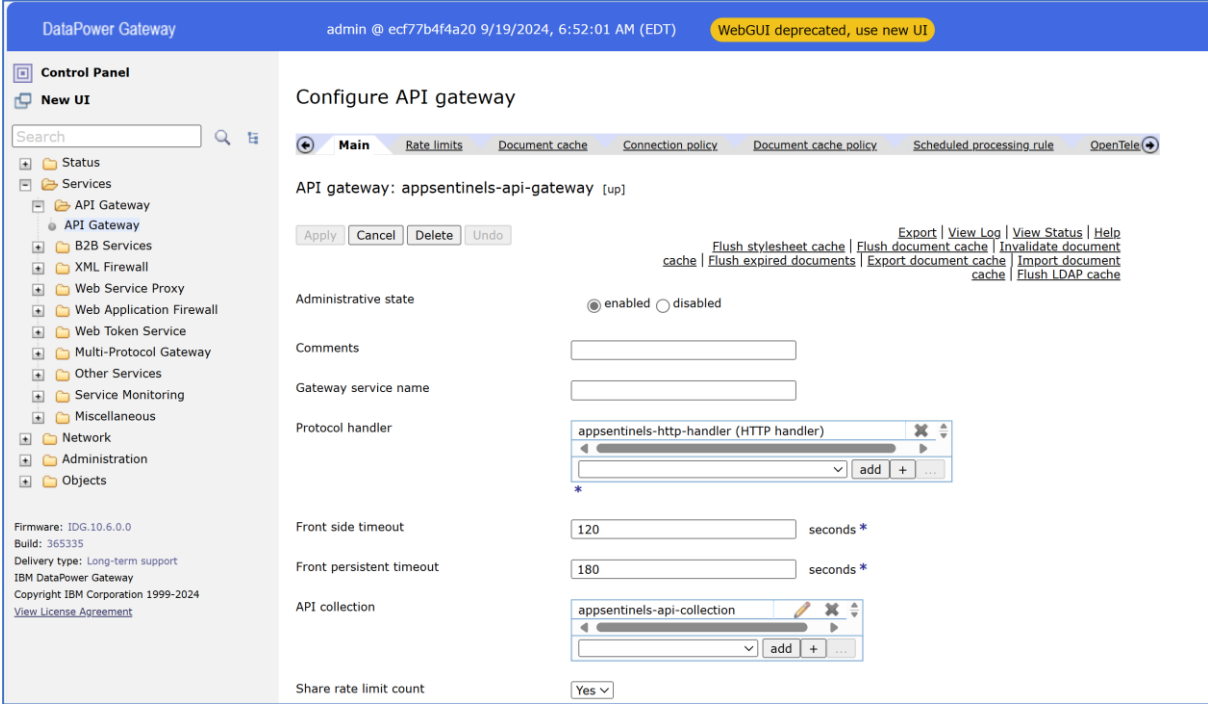
- Click on **Apply** button on all the dialogs to save the assembly rule.
- Repeat the steps to create the rule for the other AppSentinels GatewayScript.

Configure API Gateway policy

At this point, there should be assembly created for AppSentinels request policy GatewayScript and response policy GatewayScript, let us call those *PreprocessingAssembly* and *PostprocessingAssembly*, respectively. Please run the following steps to configure assemblies in API Gateway policy.

- Go to **Services > API Gateway > API Gateway**.

- Open the API Gateway configuration and Edit the **API collection** to add the assemblies (as shown below in the red box).



DataPower Gateway admin @ ec77b4f4a20 9/19/2024, 6:52:01 AM (EDT) WebGUI deprecated, use new UI

Control Panel
 New UI

Search

- Status
- Services
 - API Gateway
 - B2B Services
 - XML Firewall
 - Web Service Proxy
 - Web Application Firewall
 - Web Token Service
 - Multi-Protocol Gateway
 - Other Services
 - Service Monitoring
 - Miscellaneous
 - Network
 - Administration
 - Objects

Firmware: IDG.10.6.0.0
 Build: 365335
 Delivery type: Long-term support
 IBM DataPower Gateway
 Copyright IBM Corporation 1999-2024
[View License Agreement](#)

Configure API gateway

Main | Rate limits | Document cache | Connection policy | Document cache policy | Scheduled processing rule | OpenTele

API gateway: appsentinels-api-gateway [up]

Apply Cancel Delete Undo

Export | View Log | View Status | Help
 Flush stylesheet cache | Flush document cache | Invalidate document cache | Flush expired documents | Export document cache | Import document cache | Flush LDAP cache

Administrative state ☒ enabled ☐ disabled

Comments

Gateway service name

Protocol handler
 appsentinels-http-handler (HTTP handler)

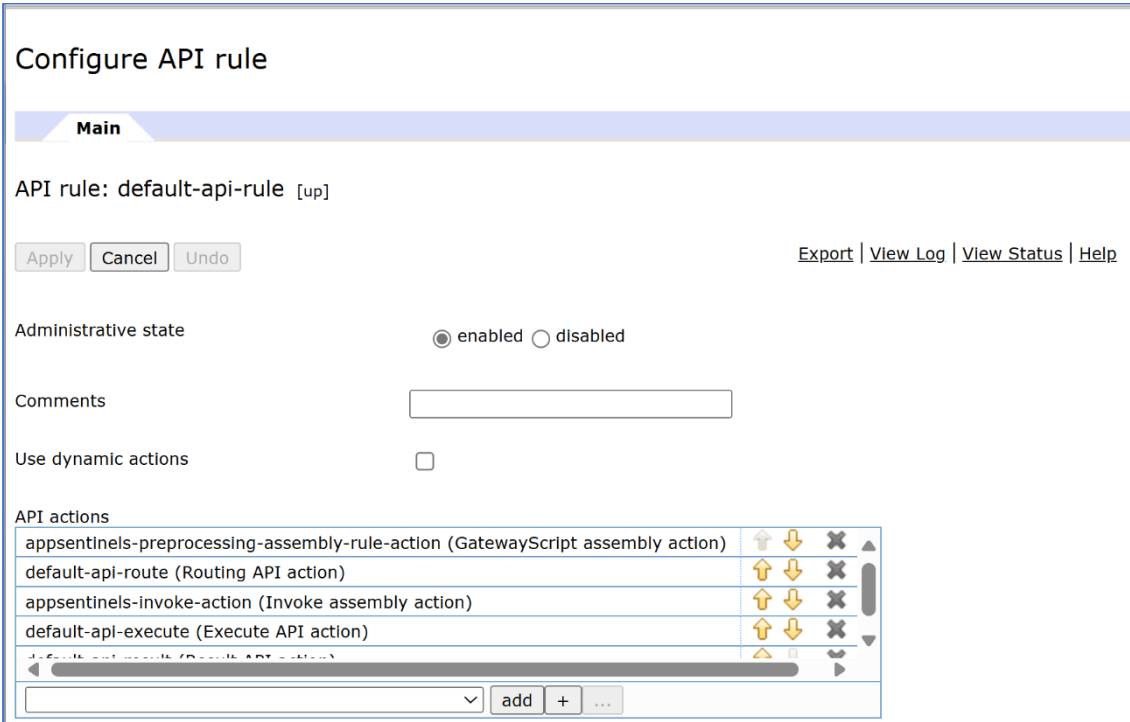
Front side timeout 120 seconds *

Front persistent timeout 180 seconds *

API collection
 appsentinels-api-collection

Share rate limit count Yes

- In the **Configure API collection** dialog, select the assembly action created with *AppSentinels request policy GatewayScript* as the first rule in **API processing rule**.



Configure API rule

Main

API rule: default-api-rule [up]

Apply Cancel Undo

Export | View Log | View Status | Help

Administrative state ☒ enabled ☐ disabled

Comments

Use dynamic actions ☐

API actions

appsentinels-preprocessing-assembly-rule-action (GatewayScript assembly action)	↑ ↓ ×
default-api-route (Routing API action)	↑ ↓ ×
appsentinels-invoke-action (Invoke assembly action)	↑ ↓ ×
default-api-execute (Execute API action)	↑ ↓ ×

add + ...

- Select the assembly created with *AppSentinels response policy GatewayScript* in the **Assembly postprocessing** drop-down.

Catalog ID	default-catalog-id									
Catalog name	default									
Routing prefixes	<table border="1"> <thead> <tr> <th>Type</th> <th>Prefix</th> <th></th> </tr> </thead> <tbody> <tr> <td>URI</td> <td>/</td> <td> </td> </tr> <tr> <td colspan="2"> </td> <td> Add </td> </tr> </tbody> </table> *	Type	Prefix		URI	/				Add
Type	Prefix									
URI	/									
		Add								
Enforce preassembly rate limits	☐ on ☒ off									
API processing rule	default-api-rule + ... *									
API error rule	default-api-error-rule + ...									
Assembly preprocessing	(none) + ...									
Assembly postprocessing	appsentinels-postprocessing-assembly + ...									
Plans	appsentinels-api-plan add + ... *									
Analytic endpoint	(none) + ...									

- Click **Apply** and **Save**.

After this the logs for the API requests going through API Gateway should reach AppSentinels Edge Controller.

Configure health check

The following points summarize the steps to configure periodic scheduled policy rule to consume logs from IBM message queue.

- Search **XML Manager** in the left pane in the Datapower Gateway UI.

DataPower Gateway admin @ ecf77b4f4a20 3/12/2025, 9:23:15 AM (EDT) WebGUI deprecated, use new UI

Control Panel

New UI

XML Manager

- XML Manager

Firmware: IDG.10.6.0.0
Build: 365335
Delivery type: Long-term support
IBM DataPower Gateway
Copyright IBM Corporation 1999-2024
[View License Agreement](#)

Control Panel

B2B

B2B Partner Profile

B2B Gateway Service

B2B Transaction Viewer

Services

Web Service Proxy

Multi-Protocol Gateway

XML Firewall

Web Application Firewall

Monitoring and Troubleshooting

View Logs

Troubleshooting

View Status

- Click on **XML Manager** in the left pane.

DataPower Gateway admin @ ecf77b4f4a20 3/12/2025, 9:24:53 AM (EDT) WebGUI deprecated, use new UI

Control Panel

New UI

Search

- Status
- Services
- Network
- Administration
- Objects
 - Network Settings
 - Protocol Handlers
 - B2B Configuration
 - API Processing Action
 - API Assembly
 - Service Configuration
 - Parsing
 - XML Processing
 - AAA policy
 - Compile Options Policy
 - Compile Settings
 - Conformance Policy
 - Document Crypto Map
 - HTTP Input Conversion Map
 - Matching Rule
 - MTOM Policy
 - Processing action
 - Processing Metadata
 - Processing Policy
 - Processing Rule
 - SAML Attributes
 - Schema Exception Map
 - SOAP Header Disposition Table
 - URL Map
 - URL Refresh Policy
 - URL Rewrite Policy
 - XML Manager**
 - XPath Routing Map

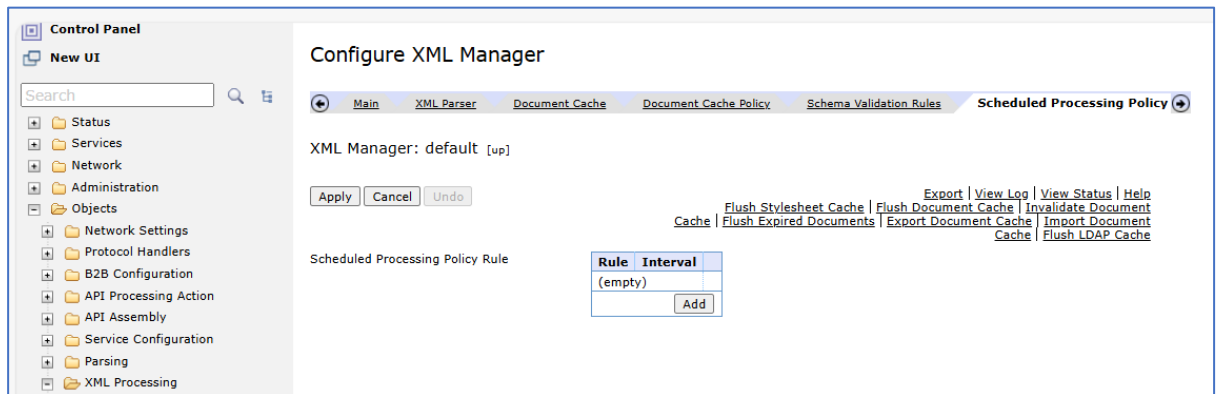
Configure XML Manager

[Refresh List](#)

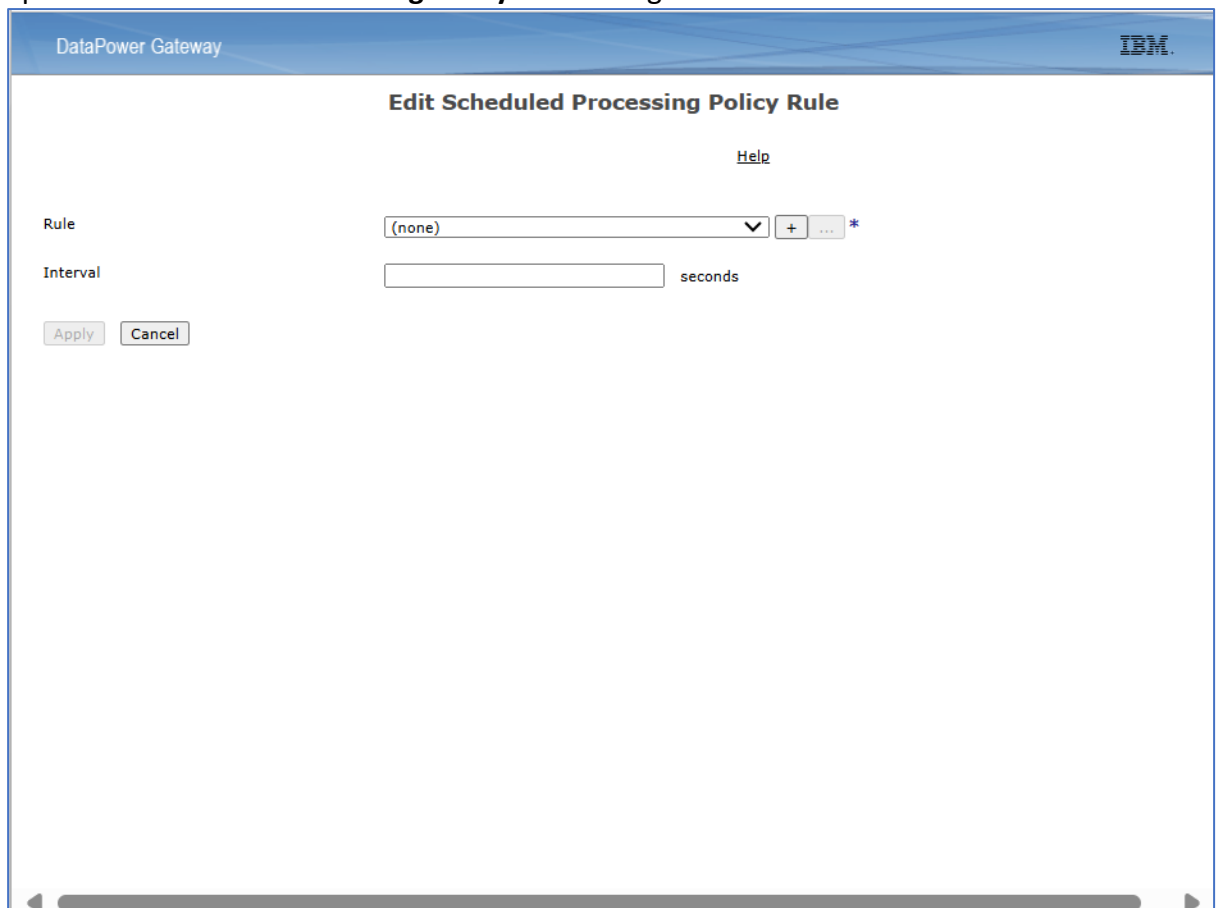
Name	Status	Op-State	Logs	Stylesheet cache size	Stylesheet cache count	Document Cache Size	Cached Documents
default	saved	up		2147483647	256	0	0
default-attempt-stream	saved	up		2147483647	256	0	0
default-wsrr	saved	up		2147483647	256	0	0

[Add](#)

- In **Configure XML Manager** dialog, click on the required XML Manager and then click on the **Scheduled Processing Policy Rules** tab.



- Click on **Add** button in **Scheduled Processing Policy Rules** configuration, this will open **Edit Scheduled Processing Policy Rule** dialog.



- In **Edit Scheduled Processing Policy Rule** dialog, click on **+** button in **Rule** configuration to open **Configure Processing Rule** dialog.

Configure Processing Rule

Apply Cancel Help

Processing Rule

Name *

Administrative state ☒ enabled ☐ disabled

Comments

Rule Action add + ...

Rule Direction *

Input Filter *

Output Filter *

Non-XML Processing ☐ on ☒ off

Unprocessed ☐ on ☒ off

- In **Configure Processing Rule** dialog, specify the **Name** of the rule.
- Click on **+** button in **Rule Action** configuration, this will open **Configure Processing Action** dialog.
- In **Configure Processing Action** dialog, specify the **Name** of the action.
- In **Action Type** configuration, select **GatewayScript** as action type.
- Configure **Input** and **Output** fields with values **INPUT** and **OUTPUT**.
- Specify the GatewayScript path as `local:///gatewayscripts/appsentinels_health_check.js`.

Configure Processing action

Apply Cancel Help

Processing action

Name *

Administrative state ☒ enabled ☐ disabled

Comments

Action type *

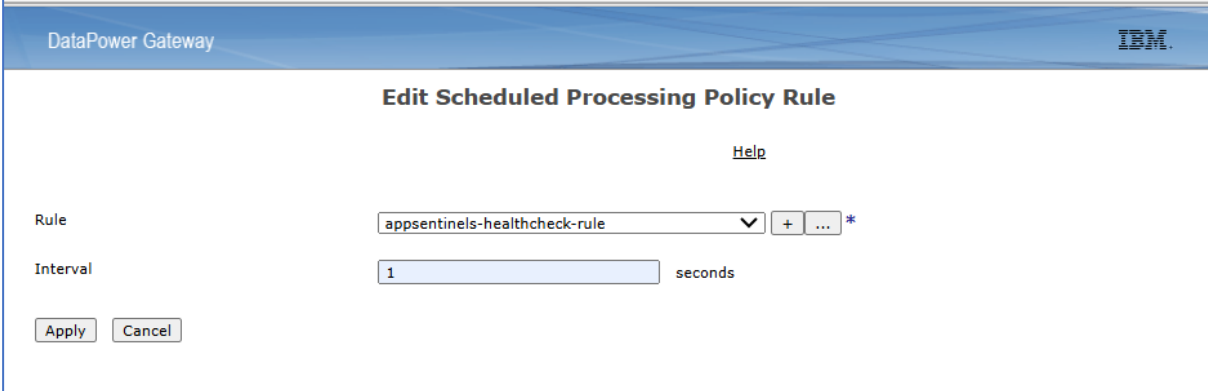
Input *

GatewayScript file *

Output *

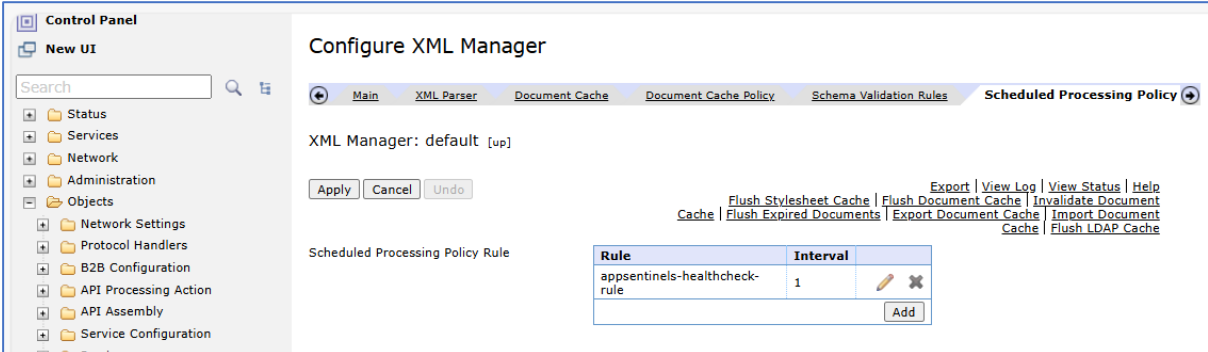
Policy identifier (for internal use)

- Click on **Apply** button.
- Click on **Apply** button in **Configure Processing Rule** dialog.
- In the **Edit Scheduled Processing Policy Rule** dialog, specify **Interval** as 1 second, and click on **Apply** button.



The screenshot shows the 'Edit Scheduled Processing Policy Rule' dialog box. At the top, it says 'DataPower Gateway' and 'IBM'. The title is 'Edit Scheduled Processing Policy Rule'. There is a 'Help' link. Below that, the 'Rule' is set to 'appsentinels-healthcheck-rule' with a dropdown arrow and a '+' button. The 'Interval' is set to '1' with a text input field and the unit 'seconds'. At the bottom, there are 'Apply' and 'Cancel' buttons.

- Click on **Apply** and **Save** button in **Configure XML Manager** dialog.



The screenshot shows the 'Configure XML Manager' dialog box. On the left is a 'Control Panel' sidebar with a search bar and a tree view containing folders like Status, Services, Network, Administration, Objects, Network Settings, Protocol Handlers, B2B Configuration, API Processing Action, API Assembly, Service Configuration, and Policies. The main area has tabs: Main, XML Parser, Document Cache, Document Cache Policy, Schema Validation Rules, and Scheduled Processing Policy (selected). Below the tabs, it says 'XML Manager: default [up]'. There are 'Apply', 'Cancel', and 'Undo' buttons. To the right, there are links: Export, View Log, View Status, Help, Flush Stylesheet Cache, Flush Document Cache, Invalidate Document Cache, Flush Expired Documents, Export Document Cache, Import Document Cache, and Flush LDAP Cache. Below these links is a table for 'Scheduled Processing Policy Rule'.

Rule	Interval	
appsentinels-healthcheck-rule	1	 

At the bottom right of the table is an 'Add' button.

Configure message queue

The following points summarize the steps to configure periodic scheduled policy rule to consume logs from IBM message queue.

- Search **XML Manager** in the left pane in the Datapower Gateway UI.

DataPower Gateway admin @ ecf77b4f4a20 3/12/2025, 9:23:15 AM (EDT) WebGUI deprecated, use new UI

Control Panel

New UI

XML Manager

- XML Manager

Firmware: IDG.10.6.0.0
Build: 365335
Delivery type: Long-term support
IBM DataPower Gateway
Copyright IBM Corporation 1999-2024
[View License Agreement](#)

Control Panel

B2B

B2B Partner Profile

B2B Gateway Service

B2B Transaction Viewer

Services

Web Service Proxy

Multi-Protocol Gateway

XML Firewall

Web Application Firewall

Monitoring and Troubleshooting

View Logs

Troubleshooting

View Status

- Click on **XML Manager** in the left pane.

DataPower Gateway admin @ ecf77b4f4a20 3/12/2025, 9:24:53 AM (EDT) WebGUI deprecated, use new UI

Control Panel

New UI

Search

- Status
- Services
- Network
- Administration
- Objects
 - Network Settings
 - Protocol Handlers
 - B2B Configuration
 - API Processing Action
 - API Assembly
 - Service Configuration
 - Parsing
 - XML Processing
 - AAA policy
 - Compile Options Policy
 - Compile Settings
 - Conformance Policy
 - Document Crypto Map
 - HTTP Input Conversion Map
 - Matching Rule
 - MTOM Policy
 - Processing action
 - Processing Metadata
 - Processing Policy
 - Processing Rule
 - SAML Attributes
 - Schema Exception Map
 - SOAP Header Disposition Table
 - URL Map
 - URL Refresh Policy
 - URL Rewrite Policy
 - XML Manager**
 - XPath Routing Map

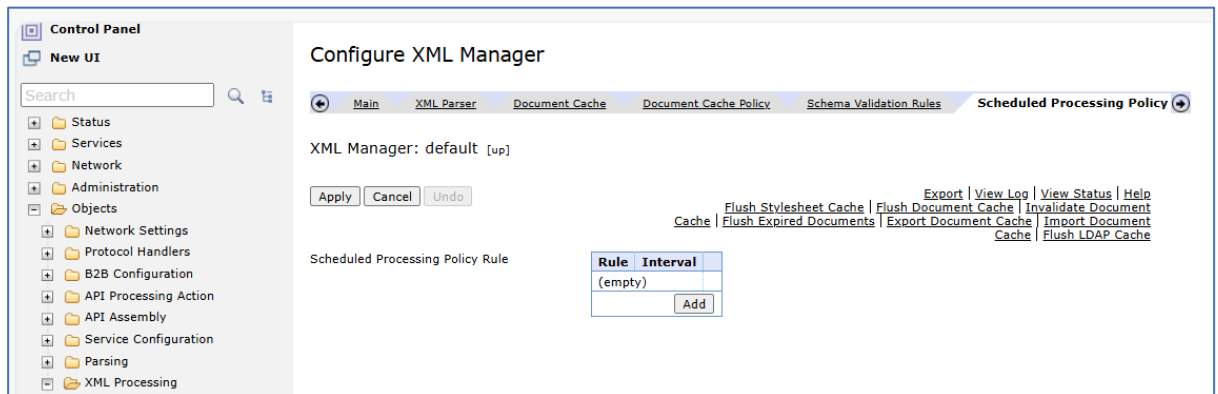
Configure XML Manager

[Refresh List](#)

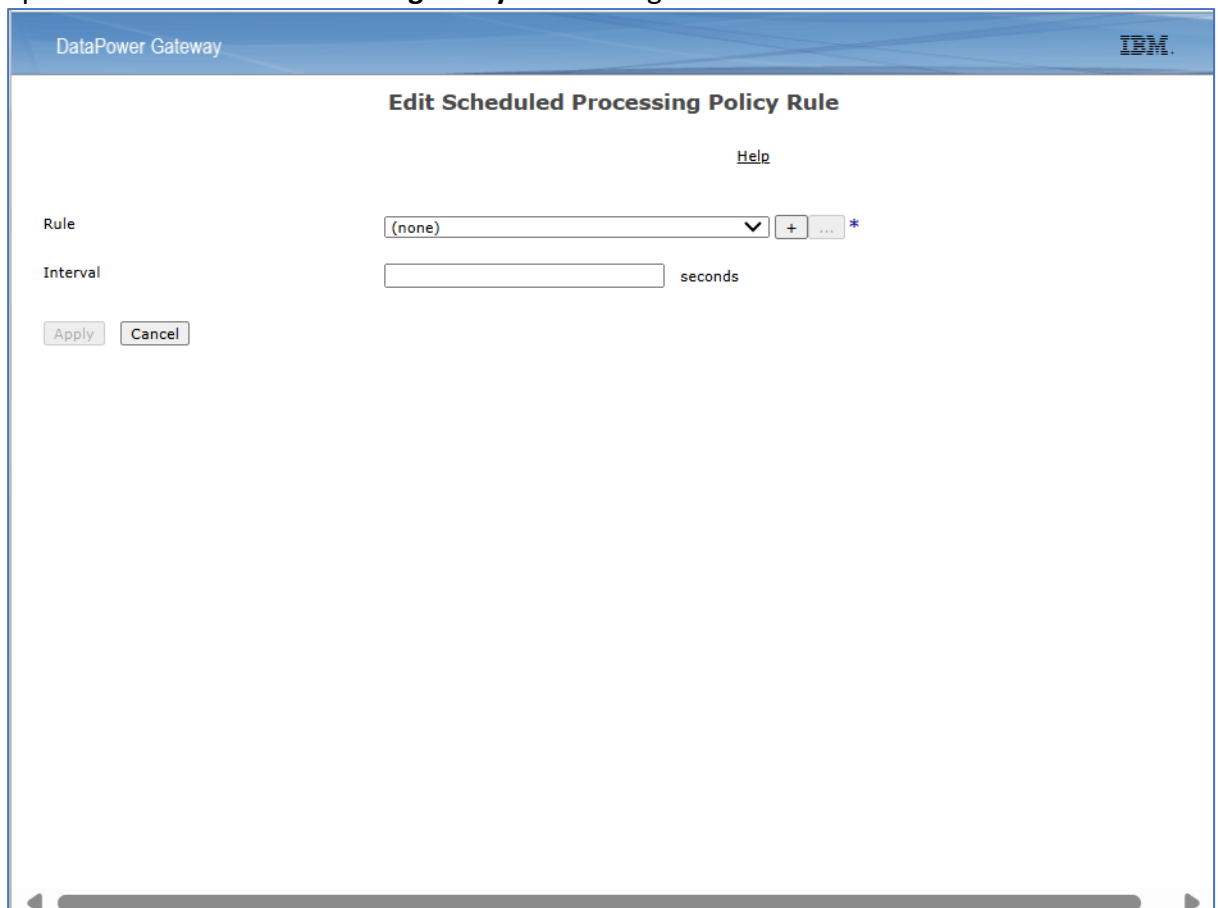
Name	Status	Op-State	Logs	Stylesheet cache size	Stylesheet cache count	Document Cache Size	Cached Documents
default	saved	up		2147483647	256	0	0
default-attempt-stream	saved	up		2147483647	256	0	0
default-wsrr	saved	up		2147483647	256	0	0

[Add](#)

- In **Configure XML Manager** dialog, click on the required XML Manager and then click on the **Scheduled Processing Policy Rules** tab.



- Click on **Add** button in **Scheduled Processing Policy Rules** configuration, this will open **Edit Scheduled Processing Policy Rule** dialog.



- In **Edit Scheduled Processing Policy Rule** dialog, click on + button in **Rule** configuration to open **Configure Processing Rule** dialog.

Configure Processing Rule

Main

Processing Rule

Apply

Cancel

Help

Name

appsentinels-mq-rule *

Administrative state

☒ enabled
 ☐ disabled

Comments

Rule Action

(empty)

add

+

...

Rule Direction

Both Directions ▼ *

Input Filter

None ▼ *

Output Filter

None ▼ *

Non-XML Processing

☐ on
 ☒ off

Unprocessed

☐ on
 ☒ off

- In **Configure Processing Rule** dialog, specify the **Name** of the rule.
- Click on **+** button in **Rule Action** configuration, this will open **Configure Processing Action** dialog.
- In **Configure Processing Action** dialog, specify the **Name** of the action.
- In **Action Type** configuration, select **GatewayScript** as action type.
- Configure **Input** and **Output** fields with values **INPUT** and **OUTPUT**.
- Specify the GatewayScript path as `local:///gatewayscripts/appsentinels_mq.js`.

Configure Processing action

Main

Parse settings

Named inputs

Named outputs

Stylesheet parameters

Condition

Processing action

Apply

Cancel

Help

Name

appsentinels-mq-rule-action *

Administrative state

☒ enabled
 ☐ disabled

Comments

Action type

GatewayScript ▼ *

Input

INPUT *

GatewayScript file

local:///gatewayscripts/appsentinels *

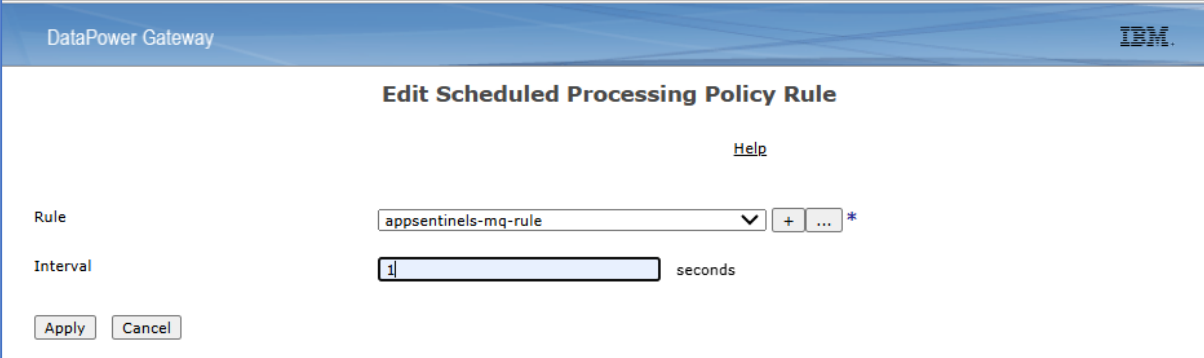
Output

OUTPUT *

Policy identifier (for internal use)

- Click on **Apply** button.

- Click on **Apply** button in **Configure Processing Rule** dialog.
- In the **Edit Scheduled Processing Policy Rule** dialog, specify **Interval** as 1 second, and click on **Apply** button.



DataPower Gateway

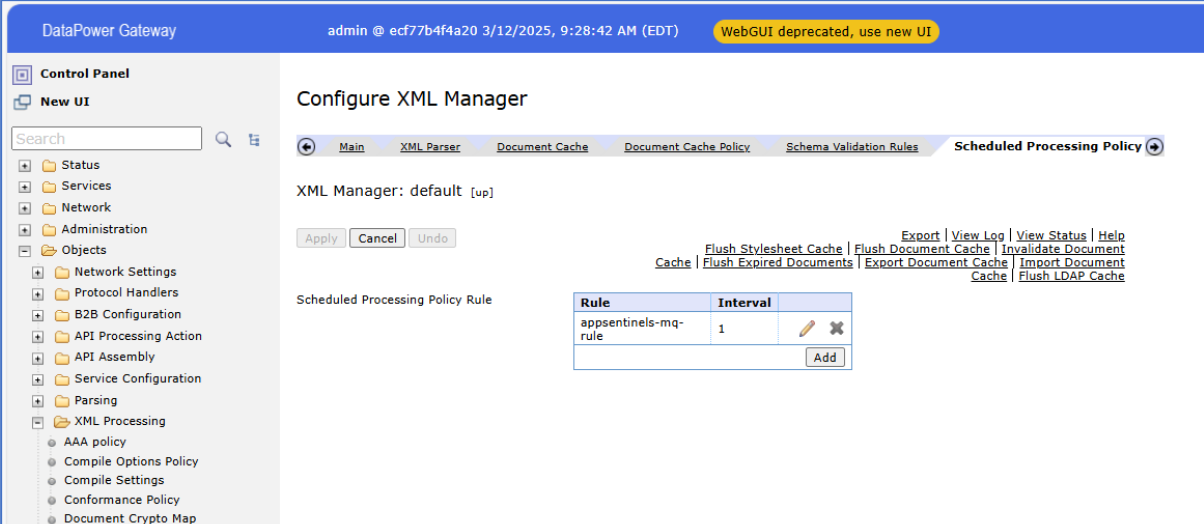
Edit Scheduled Processing Policy Rule

[Help](#)

Rule: + ... *

Interval: seconds

- Click on **Apply** and **Save** button in **Configure XML Manager** dialog.



DataPower Gateway admin @ ecf77b4f4a20 3/12/2025, 9:28:42 AM (EDT) WebGUI deprecated, use new UI

Control Panel New UI

Configure XML Manager

XML Manager: default [up]

Scheduled Processing Policy Rule

Rule	Interval	
appsentinels-mq-rule	1	

[Export](#) | [View Log](#) | [View Status](#) | [Help](#)
[Flush Stylesheet Cache](#) | [Flush Document Cache](#) | [Invalidate Document Cache](#) | [Flush Expired Documents](#) | [Export Document Cache](#) | [Import Document Cache](#) | [Flush LDAP Cache](#)

Datapower Multi-Protocol Gateway (MPGW)

GatewayScripts

Following table lists the AppSentinels GatewayScripts for Datapower Multi-Protocol Gateway.

GatewayScript name	API Gateway policy rule
appsentinels_mpgw_request_policy.js	Preprocessing rule
appsentinels_mpgw_response_policy.js	Postprocessing rule
mpgw_error_handling.js	Error handling rule
appsentinels_mq.js	Message queue Log consumer GatewayScript
Appsentinels_health_check.js	GatewayScript for AppSentinels Controller periodic health check

The same GatewayScripts are used in inline (or auth) mode and OOB (or transparent) mode. The policy mode is defined in the GatewayScripts using a configuration variable. In subsequent sections, the terms *request policy GatewayScript* and *response policy GatewayScript* refer to request and response policy files. The GatewayScript *mpgw_error_handling.js* defines the error handling in auth mode, specifically for sending appropriate error response to the client.

Edit configuration in GatewayScripts

Each of the GatewayScripts has a configuration section containing definitions of the attributes used by the GatewayScripts. The following picture displays configuration parameters for the *appsentinels_mpgw_response_policy_auth.js* GatewayScript. Other GatewayScripts have similar configuration parameter definitions.

```
// Configuration
const config = {
  // Deployment mode - 'transparent' or 'auth'
  deploymentMode: 'transparent',

  // Appsentinels controller configuration
  controllerHost: '<controller-url>',
  controllerPort: '9004',
  scheme: 'http', // or 'https'

  // TLS client profile name - needed for HTTPS communication
  tlsClientProfileName: '<TLS client profile name>',

  // Payload configuration
  maxSupportedPayload: 131072,
  supportedContentTypes: ["json", "xml", "graphql", "form"],

  // Sensor visibility configuration
  pluginVersion: '1.0.0',
  sensorHostname: 'datapower-gateway',
  sensorInstanceName: 'datapower-mpgw',

  // Health check enabled or not
  healthCheckDisabled: true,
  // Don't send log if health check response not received within this threshold
  healthCheckThreshold: 2000, // in milliseconds

  // Configuration for IBM message queue
  mqPostLogToQueue: false,
  mqQueueManager: '<queue-manager-name>',
  mqQueueName: '<queue-name>',
  mqScheme: 'idgmq'
}
```

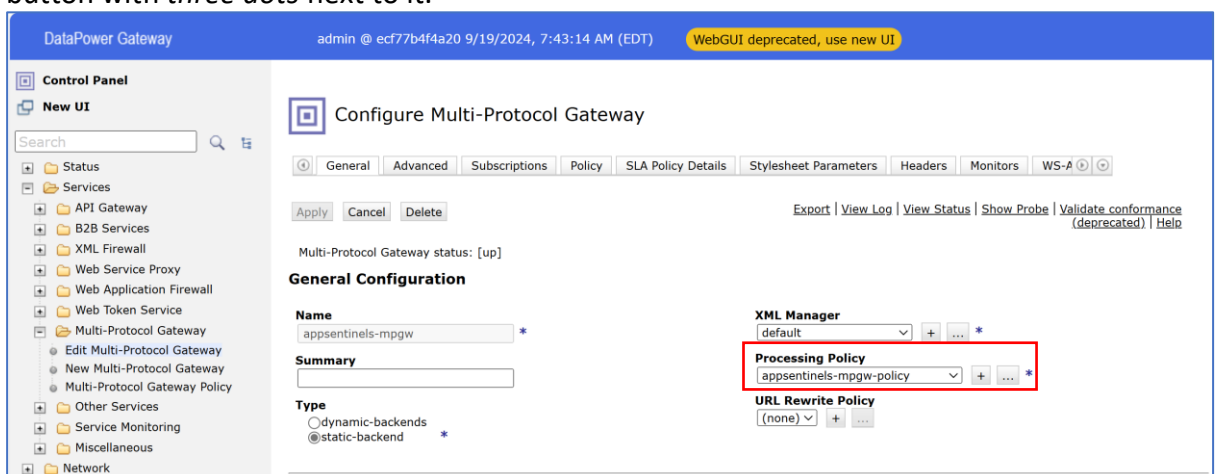
Following points summarize steps to update configuration parameter

- Change the *deploymentMode* to 'auth' if inline (or auth) mode policy needs to be deployed.
- Controller URL is the only mandatory configuration parameter. So, find out AppSentinels Edge Controller DNS name or IP address.
- Open the request policy GatewayScript file.
- Search for <controller-url> in the file and replace it with AppSentinels Edge Controller DNS name or IP address.
- If Datapower Gateway communicates with AppSentinels Controller over HTTPS, then update the *scheme* and *tlsClientProfileName*. Please configure a TLS client profile in **Objects > Crypto Configuration > TLS client profile** in Datapower Gateway configuration.
- The parameters *sensorHostName* and *sensorInstanceName* are used for sensor visibility. Please modify the default values of these parameters appropriately depending on sensor visibility requirement.
- The configuration of health check and IBM MQ related parameters is same as that described earlier in the API Gateway configuration. Please refer to that sub-section if health check or IBM MQ is enabled.
- The configuration in the request policy GatewayScript is a subset of the configuration described above in the response policy GatewayScript.

Policy configuration

Following points list down the steps to deploy AppSentinels policy in Datapower Multi-Protocol Gateway.

- Create a checkpoint of the existing working configuration in **Administration > Configuration > Configuration Checkpoints**.
- Go to **Services > Multi-Protocol Gateway > Edit Multi-Protocol Gateway**.
- Click on the Multi-Protocol Gateway instance.
- In **Configure Multi-Protocol Gateway** dialog, modify the **Processing Policy** by clicking button with *three dots* next to it.



- In **Multi-Protocol Gateway Style Policy** dialog, configure three rules as shown in the picture below.


Configure Multi-Protocol Gateway Style Policy

Policy:
 Policy Name: *

[Export](#) | [View Log](#) | [View Status](#) | [Close Window](#)

Rule:
 Rule Name: Rule Direction:

Create rule: Click New, drag action icons onto line. Edit rule: Click on rule, double-click on action.

Filter
 Sign
 Verify
 Validate
 Encrypt
 Decrypt
 Transform
 Route
 GatewayScript
 AAA
 Results
 Advanced

CLIENT

 ORIGIN SERVER

Configured Rules					
Order	Rule Name	Direction	Actions		
1	appsentinels-mpgw-policy_rule_0	Client to Server			delete rule
2	appsentinels-mpgw-policy_rule_1	Server to Client			delete rule
3	appsentinels-mpgw-policy_rule_2	Error			delete rule

[Scroll to top](#)

Following points summarize these three rules:

- First rule has **Client to Server** direction. This rule executes the request policy GatewayScript on API request. Please select the appropriate **Match** conditions required to hit the rule for desired API traffic.
- Second rule has **Server to Client** direction. This rule executes the response policy GatewayScript on API response from backend. Please select the appropriate Match conditions needed for the desired API response traffic.
- The third rule has the rule direction **Error**. This rule manages the errors occurred while executing client to server, or server to client policy. In *Auth mode* policy, the request Policy GatewayScript can reject the session if the AppSentinels policy blocks the API request. In this case, the Client to Server GatewayScript returns an error. The AppSentinels error handling gateway script manages the error and returns an appropriate response to the client.
- The Auth mode policy requires error handling GatewayScript, but transparent mode policy does not require it.
- Please configure appropriate **Match** and **Result** parameters in all the three rules.
- Select the **Client to Server** rule, and double click on the GatewayScript icon () to open the **Configure GatewayScript action** dialog (as shown below).

DataPower Gateway IBM



Configure GatewayScript Action

[Help](#)

Basic

Advanced

Input

Input

*

Options



GatewayScript

GatewayScript file

local:/// ▾

(none) ▾

Upload...

Fetch...

Edit...

View...

Var Builder

*

Output

Output

- Click on the **Upload** button, this will open a new dialog to choose the GatewayScript to upload. Click **Choose File** button and select the *appsentinels_mpgw_request_policy.js* file and then click the **Upload** button to upload the file (please see below).

Upload File to Directory local:///

File to upload:
*

appsentinels...uest_policy.js

Save as:
*

appsentinels_mpgw_request_policy.

☐
Overwrite Existing File

- Click on the Done button in the **Configure Gateway action** dialog.
- Select the **Server to Client** rule, double click on the GatewayScript icon (🔗).
- Repeat the same procedure to upload the *appsentinels_mpgw_response_policy.js* file.
- In Auth mode, select the Error rule, and double click on the GatewayScript icon (🔗).
- Repeat the same steps to upload the *error handling GatewayScript* file.
- After uploading the GatewayScript files, click on Apply Policy button in **Configure Multi-Protocol Gateway Style Policy** dialog. Click **Cancel** to exit this dialog.
- In **Configure Multi-Protocol Gateway** dialog, Click **Apply** followed by **Save** button.

After execution of the steps mentioned above, Datapower Multi-Protocol Gateway should start forwarding API logs to AppSentinels Edge Controller.

XML Manager scheduled policy rules for IBM MQ consumer and health check

XML Manager scheduled policy rules configuration for enabling AppSentinels Controller health check or for consuming AppSentinels logs from IBM MQ remains identical for Datapower MPGWS. Please refer to earlier sub-sections *Configure health check* and *Configure message queue* in previous section for details.

Troubleshooting

- Please check the Datapower gateway logs for errors in case of any problem.
- Make sure that *administrative state* of each component is up.
- Go to **Administration > Main > File Management** and check AppSentinels policies exist in **local:** directory.
- If APIs are not visible in AppSentinels portal, please check the network connectivity between Datapower Gateway and AppSentinels Edge Controller.
- Capture Datapower Gateway logs and contact AppSentinels support for further assistance.