AppSentinels.ai
Application Security Re-invented

AppSentinels API Security Platform

IBM API Connect Integration

Contents

AppSentinels Policy Instrumentation

We can deploy policy in three different ways:

- Catalog-scoped Policy
  - Use this method to manually attach the AppSentinels policy to an API in a specific catalog
- Global Policy (per catalog)
  - Use this method to automatically apply the AppSentinels policy to all APIs in a specific catalog, no manual intervention is required here
- Global-scoped Policy using gateway extension
  - Use this method to ensure AppSentinels Policy is available across all the catalogs in an organization, later manually attach the AppSentinels policy to APIs

Note: Please refer to ***Appsentinels-IBM-DataPower-Integration.pdf*** document for detailed information related to GatewayScripts configurations.

AppSentinels Catalog-Scoped Policy Instrumentation

In this type of deployment, we have to deploy the policy zip file to a specific catalog in API manager. After successful deployment the AppSentinels policy will appear in API assembly palette under user-defined section. We can drag- and-drop to apply the policy to specific API.

This guide describes how to integrate AppSentinels policies (pre-request and post-request) at the catalog level in IBM API Connect. Integration can be achieved using two methods.

1. Through API Manager UI
2. Using the APIC Toolkit CLI

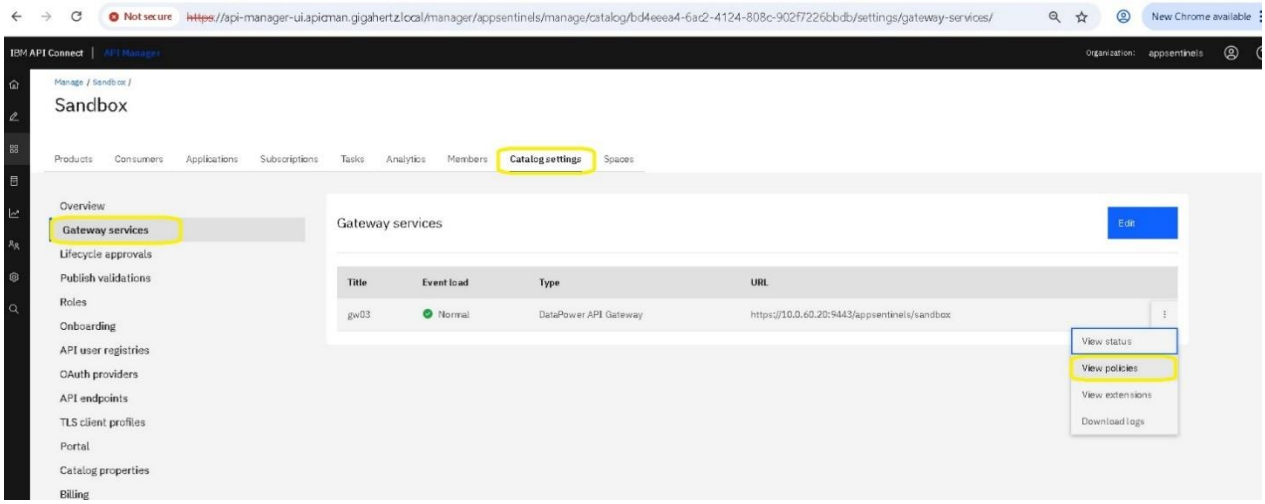
Integration via API Manager UI

To integrate policies via the API Manager UI, follow these steps:

- Download the AppSentinels policy yaml files from location mentioned below. There will be two files
  - appsentinels-pre-proc.yaml
  - appsentinels-post-proc.yaml

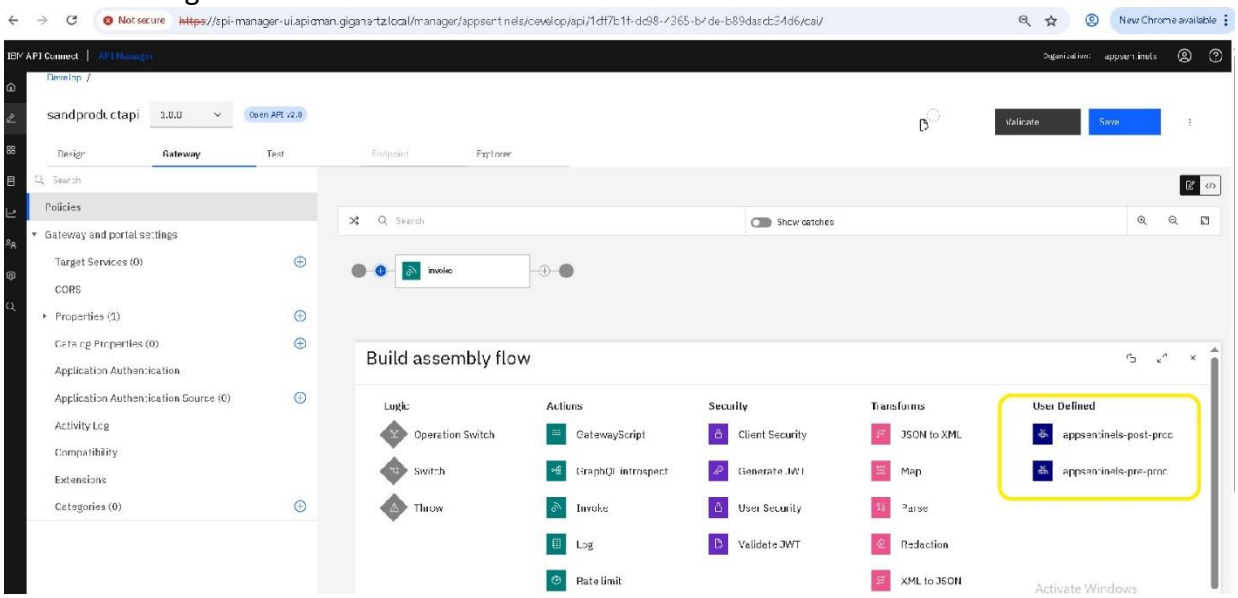
  Location: AppSentinels_Catalog_Scoped_Policy

- Update the `AS_CONTROLLER_URL` with the AppSentinels controller URL and `AS_TLS_CLIENT_PROFILE` with TLS profile in the `appsentinels-pre-proc.yaml` and `appsentinels-post-proc.yaml` files.
- Then create two zip file form it by using the below commands-
  - ***zip appsentinels-pre-proc.zip appsentinels-pre-proc.yaml***
  - ***zip appsentinels-post-proc.zip appsentinels-post-proc.yaml***
- Navigate to API Manager → Manage → Select the specific catalog → Catalog Settings → Gateway Services.

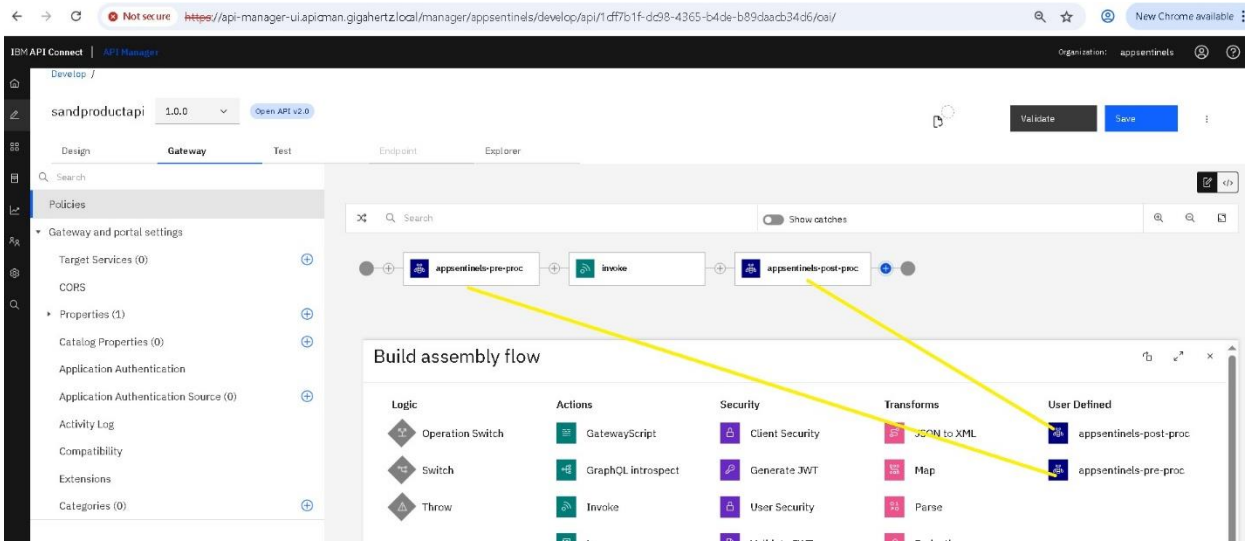


- In the Gateway Services section, click on the 3-dot menu (ellipsis) of your Gateway Service.
- Select 'View Policies', then upload the AppSentinels policy files.

- After uploading, the policies will be available in the API Assembly palette for new or existing APIs.



- You can then drag and drop the policies into the API Assembly and save the configuration.



Integration through API toolkit CLI

Execute the following commands to integrate the policies:

- Login to Api Manager:

apic login --server <Api manager URL> --username <username> --password <password> --realm <realm>

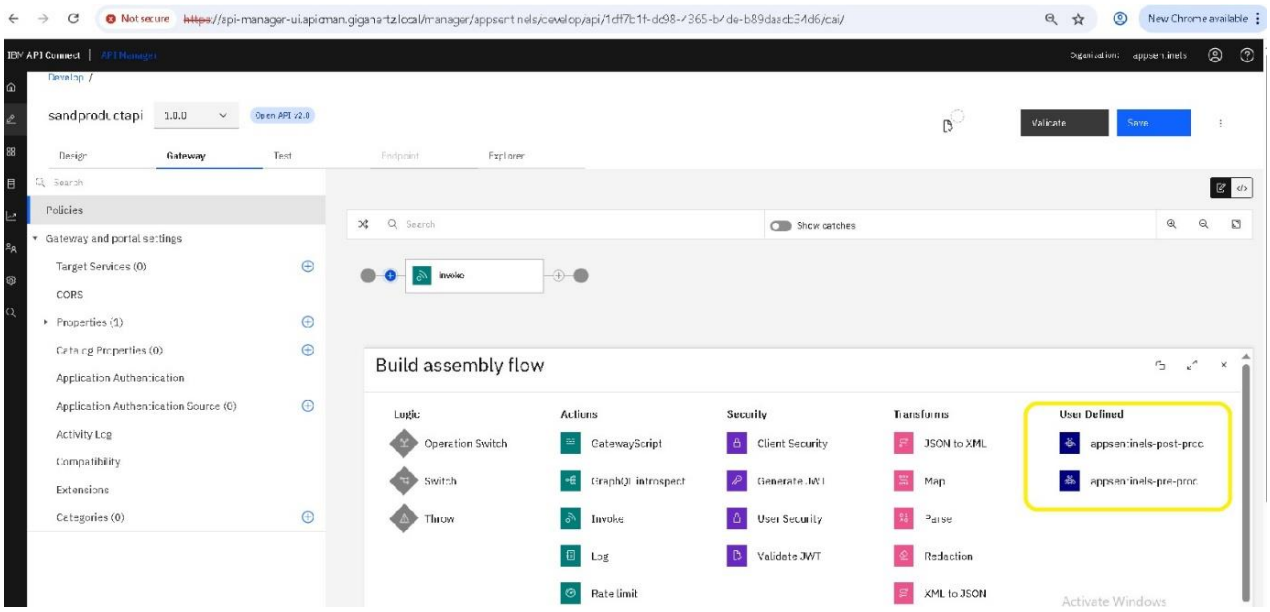
- Create Pre-request Policy:

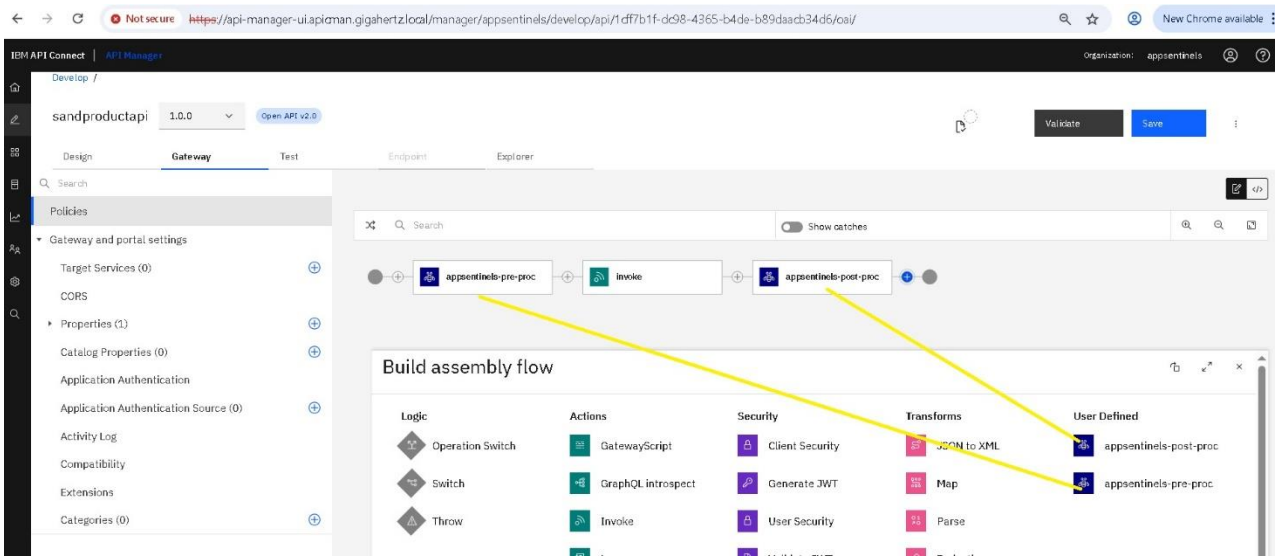
apic policies:create --scope catalog <POLICY_FILE for preprocessing > -c <catalog name> -o <ORG name> --server <management server endpoint> --configured-gateway-service <Configured Gateway Service name or id >

- Create Post-request Policy:

apic policies:create --scope catalog <POLICY_FILE for post processing > -c <catalog name> -o <ORG name> --server <management server endpoint> --configured-gateway-service <Configured Gateway Service name or id >

Once Created these policies will be available in the API Assemble for drag-and-drop usage





Note: Ensure the correct catalog and gateway service are specified when executing CLI commands.

AppSentinels Global Policy Instrumentation (Per catalog)

In this type of deployment, we must deploy the policy zip to a specific catalog in API manager. There is a script called **manage_global_policy.sh** through which we can deploy/remove the policy through CLI. After running the script, the policy will be applied to all the APIs under the specific catalog

This section provides a step-by-step guide for applying the AppSentinels global policy instrumentation using the IBM API Connect CLI. Once applied, this policy will be enforced on all APIs under the configured catalog

Prerequisites

Ensure that you have access to the API Connect CLI and a valid credential file before proceeding.
Please download the required files from AppSentinels_Global_Policy

Register Toolkit Credentials

Run the following command to set your credentials:
Command: apic client-creds:set <path to your downloads>/credentials. Json
Example: apic client-creds:set credentials. Json

Authenticate with API Connect

Run the login command with your credentials and server information:
Command: apic login --server <API Manager URL> --username <username> --password <password> --realm <realm>
Example: apic login --server https://api-manager-ui.apicman.local --username user.name --password password --realm provider/default-idp-2

Deploy the Policy Globally

Use the following command to apply the policy:
Command: ***./manage_global_policy.sh -d -c <Controller IP> -t <TLS profile name> -s <API Manager URL> -o <Organization> -g <Catalog name> -w <Gateway name>***
Example: ./manage_global_policy.sh -d -c 104.154.155.131 -t test-tls-prof -s https://api-manager-ui.apicman.local -o appsentinels -g catalog1 -w gw03

Remove the Policy Globally

Use the following command to remove the policy:
Command: ***./manage_global_policy.sh -r -c <Controller IP> -t <TLS profile name> -s <API Manager URL> -o <Organization> -g <Catalog name> -w <Gateway name>***
Example: ./manage_global_policy.sh -r -c 104.154.155.131 -t test-tls-prof -s https://api-manager-ui.apicman.local -o appsentinels -g catalog1 -w gw03

Usage of the manage_global_policy.sh Script

The script `manage_global_policy.sh` is used to deploy or remove the policy globally within a specific catalog. It accepts the following parameters:

-d: Deploy the policy
-r: Remove the policy
-c: AppSentinels Controller Hostname/IP
-t: TLS Client Profile name
-s: API Manager URL
-o: Organization under API Manager
-g: Catalog name to be instrumented
-w: DataPower Gateway Service Name

Reference

For more information, refer to the IBM documentation:
https://www.ibm.com/docs/en/api-connect/10.0.x_cd?topic=applications-working-global-policies

AppSentinels Global-Scoped Policy Instrumentation

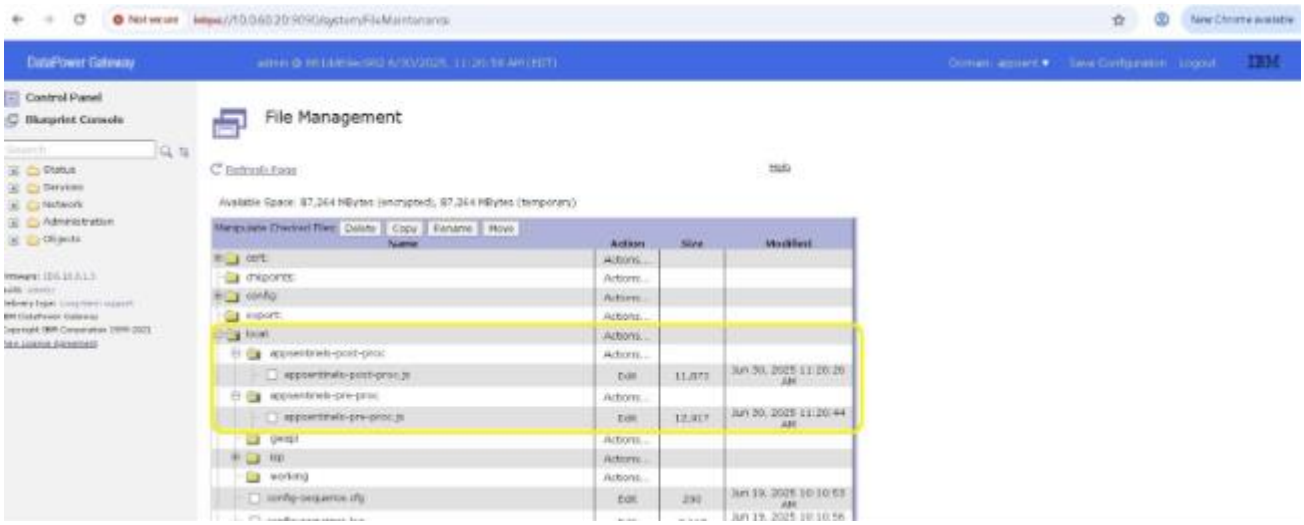
In this type of deployment, we have to deploy the gateway-extension.zip file in cloud manager. After successful deployment the policy will be appeared in API assembly pallet for all APIs across all catalog under an organization. User has to drag-and-drop the policy to specific API to apply the policy.
Please download the required file from Appsentinels_Global_Scoped_Policy

This section describes the steps to deploy AppSentinels global-scoped policy in IBM DataPower Gateway and API Connect using gateway-extension.

IBM DataPower API Gateway Configuration

- Update the `AS_CONTROLLER_URL` with the AppSentinels controller URL and `AS_TLS_CLIENT_PROFILE` with TLS profile in the `appsentinels-pre-proc.js` and `appsentinels-post-proc.js` files.
- Upload these JS files to the following locations in DataPower:
- appsentinels-pre-proc.js:
- Navigate to: File Management → local → Create subdirectory named `appsentinels-pre-proc`.
- Upload the `appensentinels-pre-proc.js` file.
- Final path: `local:///appsentinels-pre-proc/appsentinels-pre-proc.js`.
- appsentinels-post-proc.js:
- Navigate to: File Management → local → Create a subdirectory named `appsentinels-post-proc`.
- Upload the `appensentinels-post-proc.js` file.

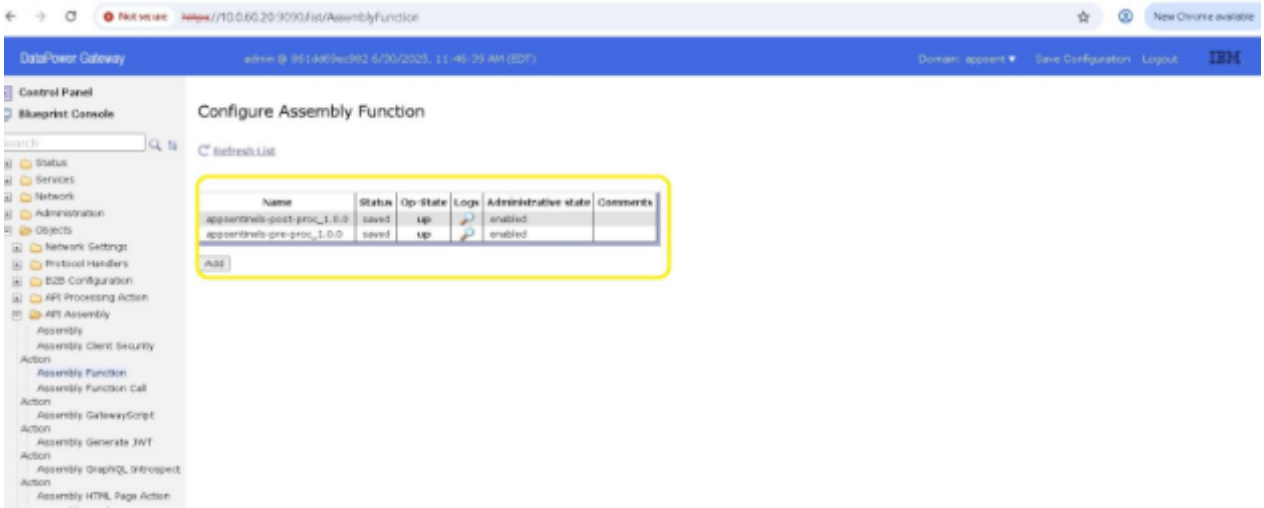
- Final path: `local:///appsentinels-post-proc/appsentinels-post-proc.js`.



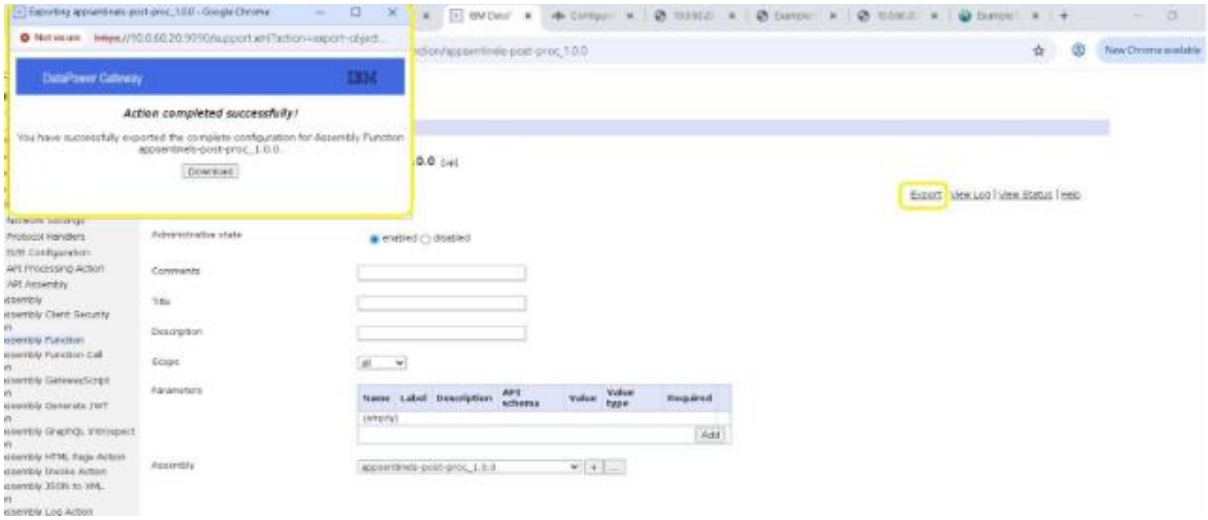
- Create Assembly Function object `appsentinels-pre-proc_1.0.0` with:
  - New Assembly under the object.
  - New Rule under the Assembly.
  - GatewayScript Action under the Rule.
  - Specify script path: `local:///appsentinels-pre-proc/appsentinels-pre-proc.js`.

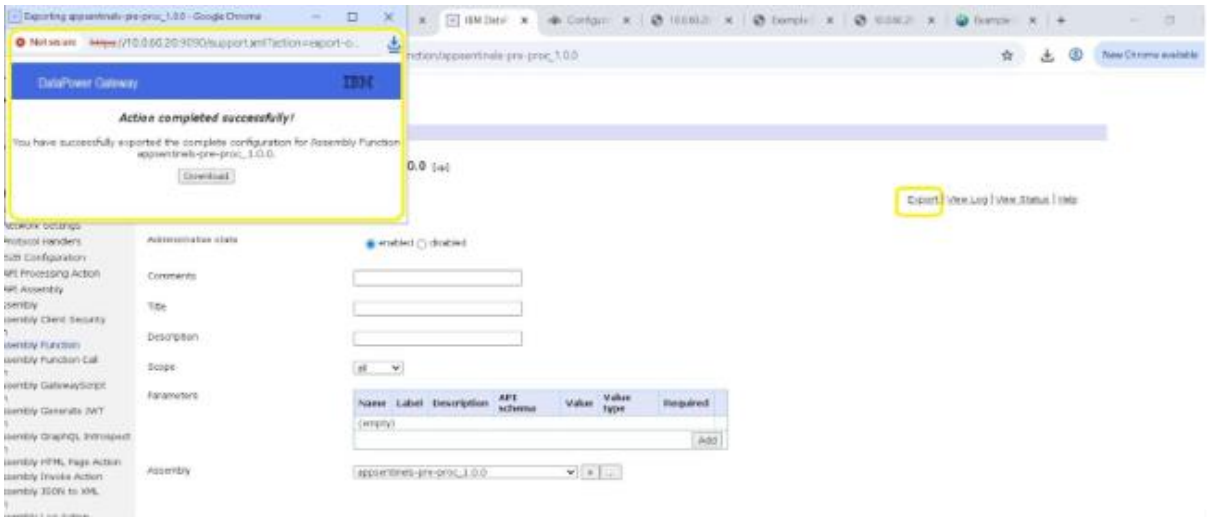
  Note: Please use name 'appsentinels-pre-proc_1.0.0' for all object created here
- Repeat the same steps for `appsentinels-post-proc` policy, replacing file and object names accordingly.

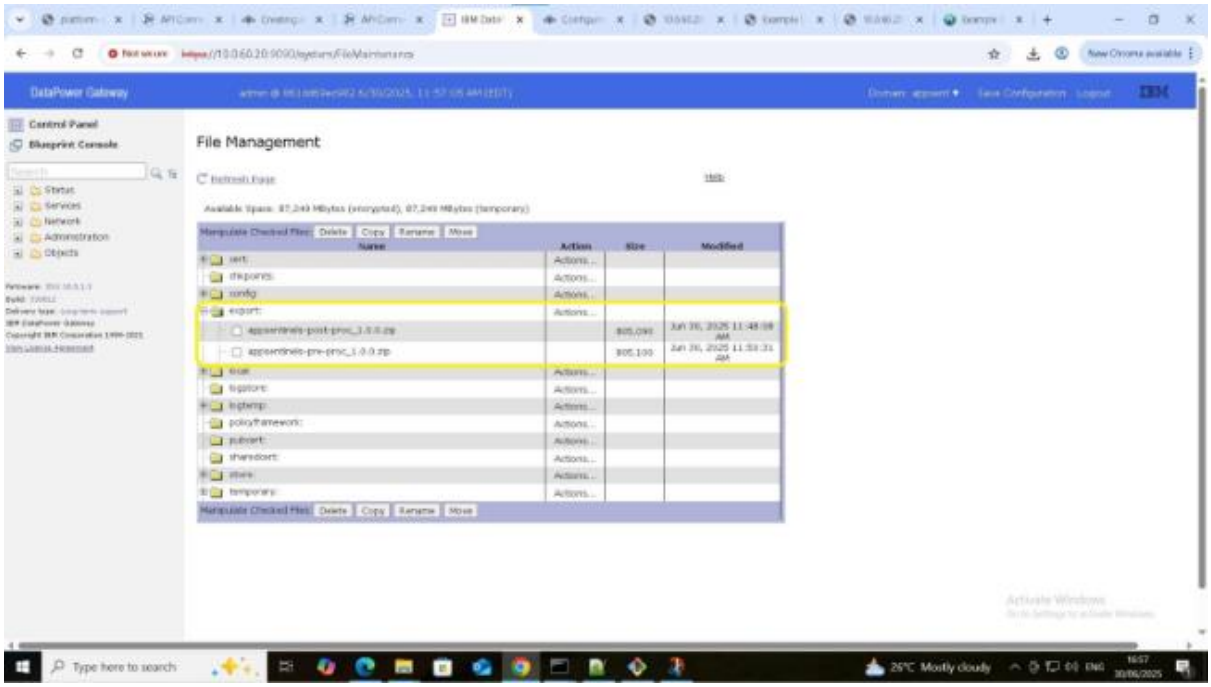
  Note: Please use name 'appsentinels-post-proc_1.0.0' for all object created here
- After creating both the assembly function it will appear like below



- Export both `appsentinels-pre-proc_1.0.0` and `appsentinels-post-proc_1.0.0` from Assembly Function as ZIPs.
- Confirm each ZIP contains:
  - `dp-aux` folder
  - `local` folder with the JS file
  - `export.xml` file







IBM API Connect Configuration

- Rename the ZIP files by removing version numbers:
- `appsentinels-pre-proc_1.0.0.zip` → `appsentinels-pre-proc.zip`
- `appsentinels-post-proc_1.0.0.zip` → `appsentinels-post-proc.zip`
- Create folder structure for each policy:
- `pre-proc/implementation/` and `post-proc/implementation/`
- Place ZIPs inside respective implementation folders.
- Add a YAML file under pre-proc and post-proc with the following format:
- Under pre-proc folder create `appsentinels-pre-proc.yaml`
- Under post-proc folder create `appsentinels-post-proc.yaml`
- Content:

  ```
  policy: 1.0.0
  info:
    title: appsentinels-<pre/post>-proc
    name: appsentinels-<pre/post>-proc
    version: 1.0.0
    description: Global scoped <pre/post> policy
  ```

- Create new ZIPs from `pre-proc` and `post-proc` folders named:
- `appsentinels-pre-proc_1.0.0.zip`
  zip -r appsentinels-pre-proc_1.0.0.zip implementation appsentinels-pre-proc.yaml
- `appsentinels-post-proc_1.0.0.zip`
  zip -r appsentinels-post-proc_1.0.0.zip implementation appsentinels-post-proc.yaml
- Create a `manifest. Json` file with the following content:
- ```
  {
  ```


  ```

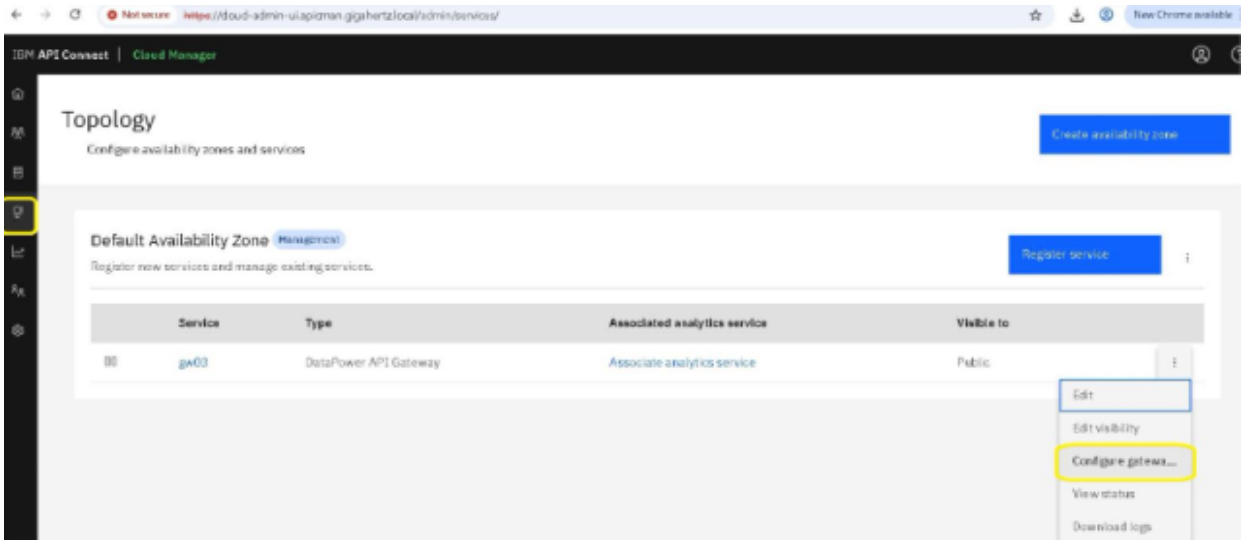
```
"extension": {
  "properties": {
    "deploy-policy-emulator": false,
    "deploy-policies": ["gatewayscript_1.0.0"]
  },
  "files": [
    {
      "filename": "appsentinels-pre-proc_1.0.0.zip",
      "deploy": "immediate",
      "type": "user-defined-policy"
    },
    {
      "filename": "appsentinels-post-proc_1.0.0.zip",
      "deploy": "immediate",
      "type": "user-defined-policy"
    }
  ]
 }
}
```

- Create final ZIP: `gateway-extension.zip` including:
- `manifest. Json`
- `appsentinels-pre-proc_1.0.0.zip`
- `appsentinels-post-proc_1.0.0.zip`

Upload using one of the methods:

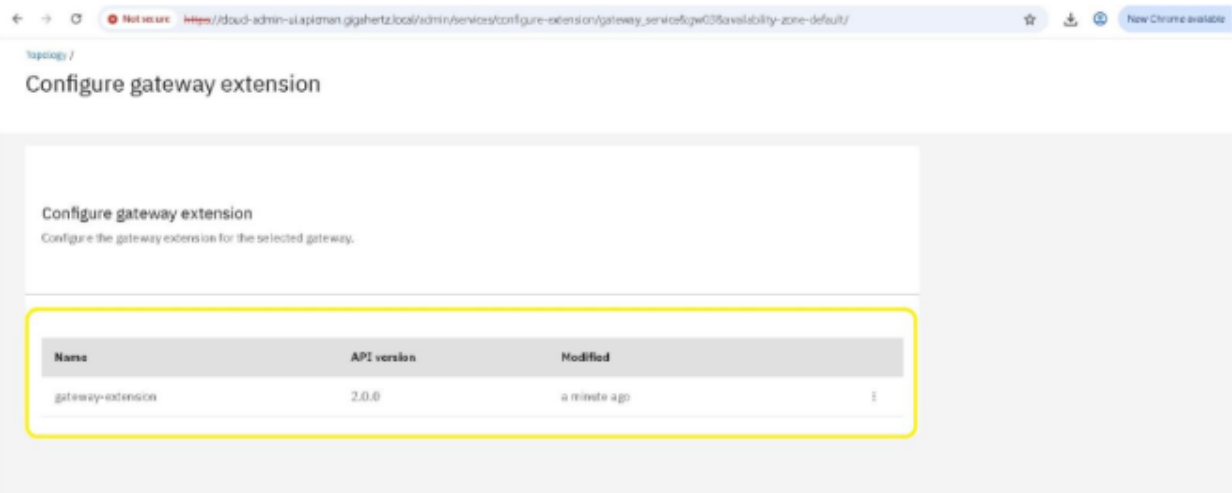
Cloud Manager UI

Navigate through Topology → Select Gateway → Configure gateway extension → Upload

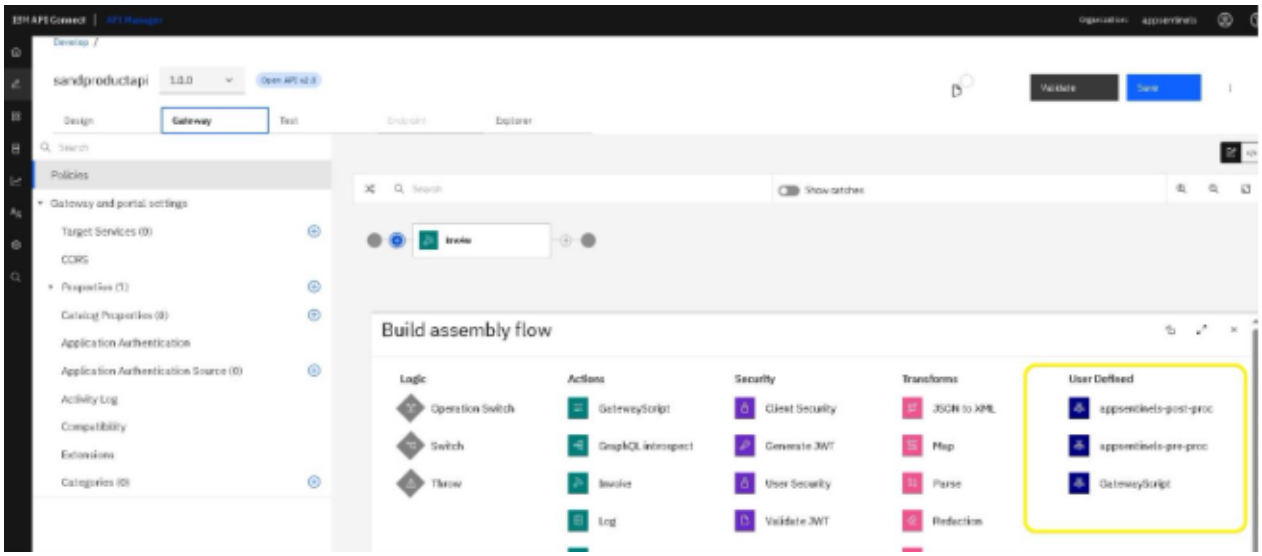


APIC CLI

- Login to Cloud manager as admin:
  apic login --server <URL> --username <user> --password <password> --realm admin/default-idp-1
- Upload gateway-extension file to specific gateway:
  apic gateway-extensions:create --scope org gateway-extension.zip --org admin --gateway-service <gw-name> --availability-zone availability-zone-default --server <URL>
- After completion of gateway-extension.zip file you can see like below



- After upload, validate policy visibility in API assembly palette and use drag-and-drop to apply

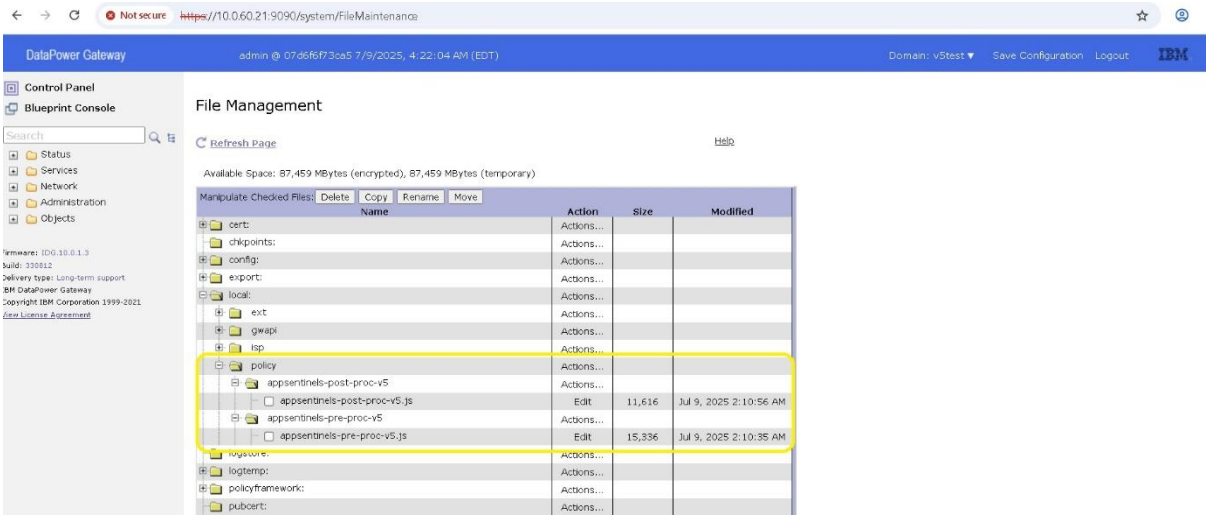


AppSentinels Catalog-Scoped Policy Instrumentation (V5 Compatible Gateway)

This section describes how to deploy policy for V5 compatible API in API Connect.

IBM DataPower Gateway Configuration

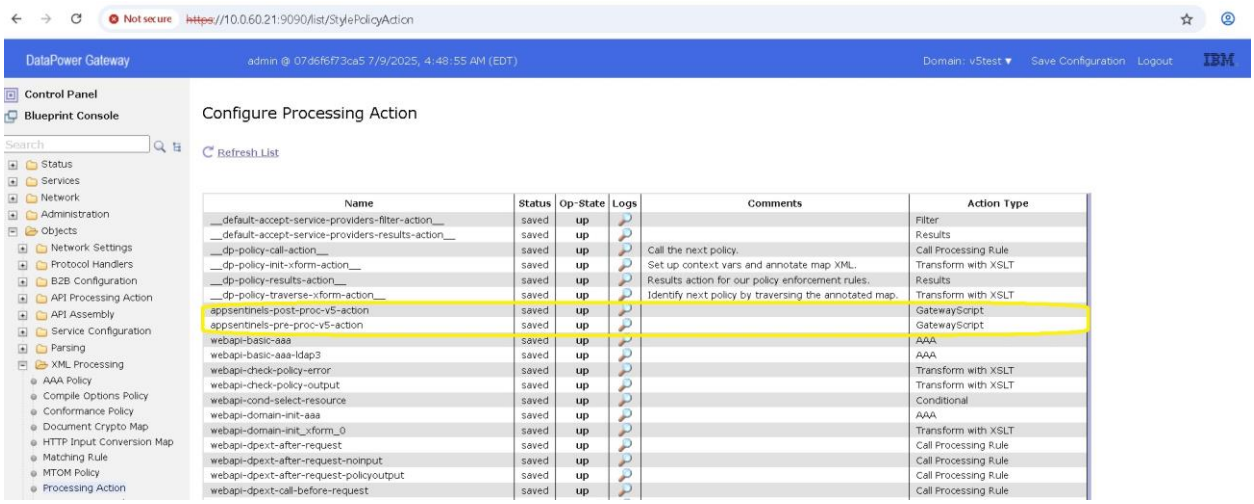
- Download the necessary files from the below link
  - File Link: Appsentinels_V5_Catalog_Scoped_Policy
- In gateway navigate through File Management --> local-->policy and create two new directory
  - appsentinels-pre-proc-v5
  - appsentinels-post-proc-v5
- Upload appsentinels-pre-proc-v5.js file in appsentinels-pre-proc-v5 directory and upload appsentinels-post-proc-v5.js file in appsentinels-post-proc-v5 directory

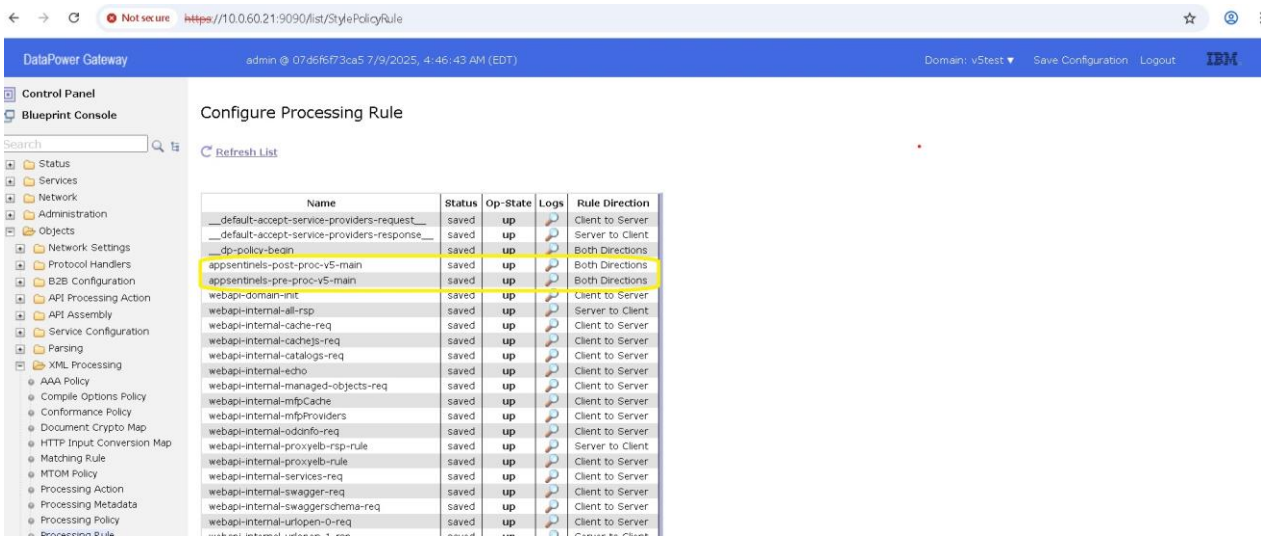


- Go to “Processing Rule” and create two new rules:
  - **For appsentinels-pre-proc-v5:**
    - **Name:** appsentinels-pre-proc-v5-main
    - **Rule Direction:** Both Direction
    - **Non-XML Processing:** on
    - **Rule Action:** create new action
      - **Name:** appsentinels-pre-proc-v5-action
      - **Action Type:** GatewayScript
      - **INPUT:** INPUT
      - **GatewayScript file:** local:///policy/appsentinels-pre-proc-v5/appsentinels-pre-proc-v5.js
      - **OUTPUT:** OUTPUT
    - Now save and apply the action and rule
  - **For appsentinels-post-proc-v5:**
    - **Name:** appsentinels-post-proc-v5-main
    - **Rule Direction:** Both Direction
    - **Non-XML Processing:** on
    - **Rule Action:** create new action

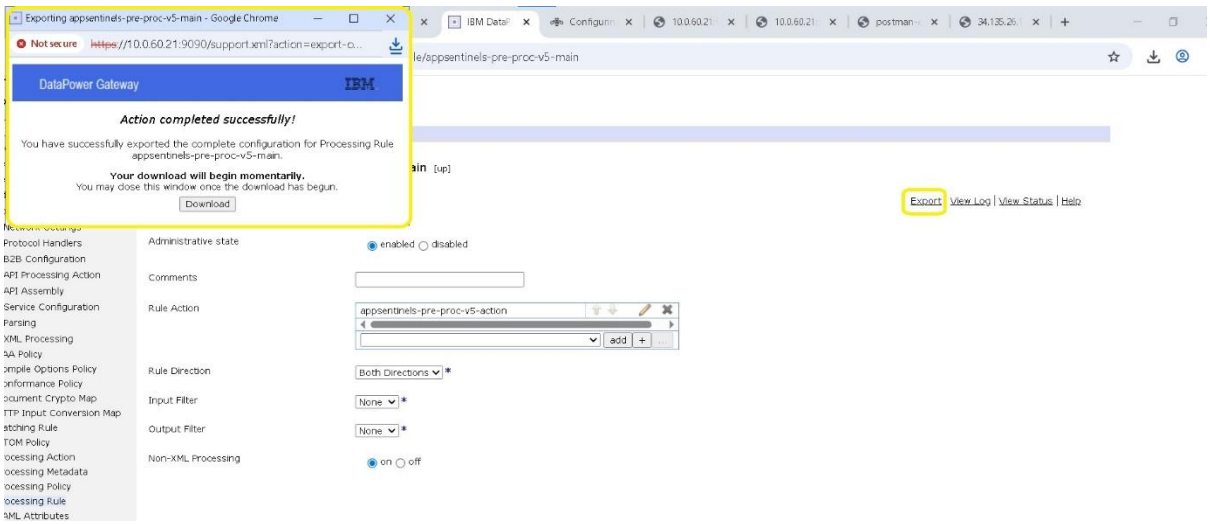
- **Name:** appsentinels-post-proc-v5-action
- **Action Type:** GatewayScript
- **INPUT:** INPUT
- **GatewayScript file:** local:///policy/appsentinels-post-proc-v5/appsentinels-post-proc-v5.js
- **OUTPUT:** OUTPUT

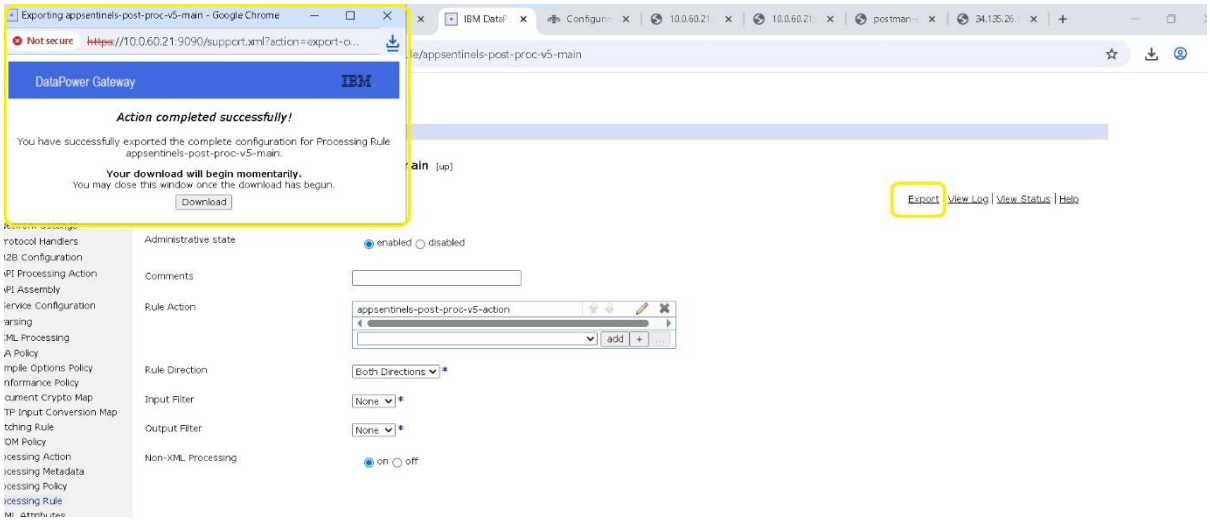
- Now save and apply the action and rule





- Go to newly created rules and do export and download the exported files

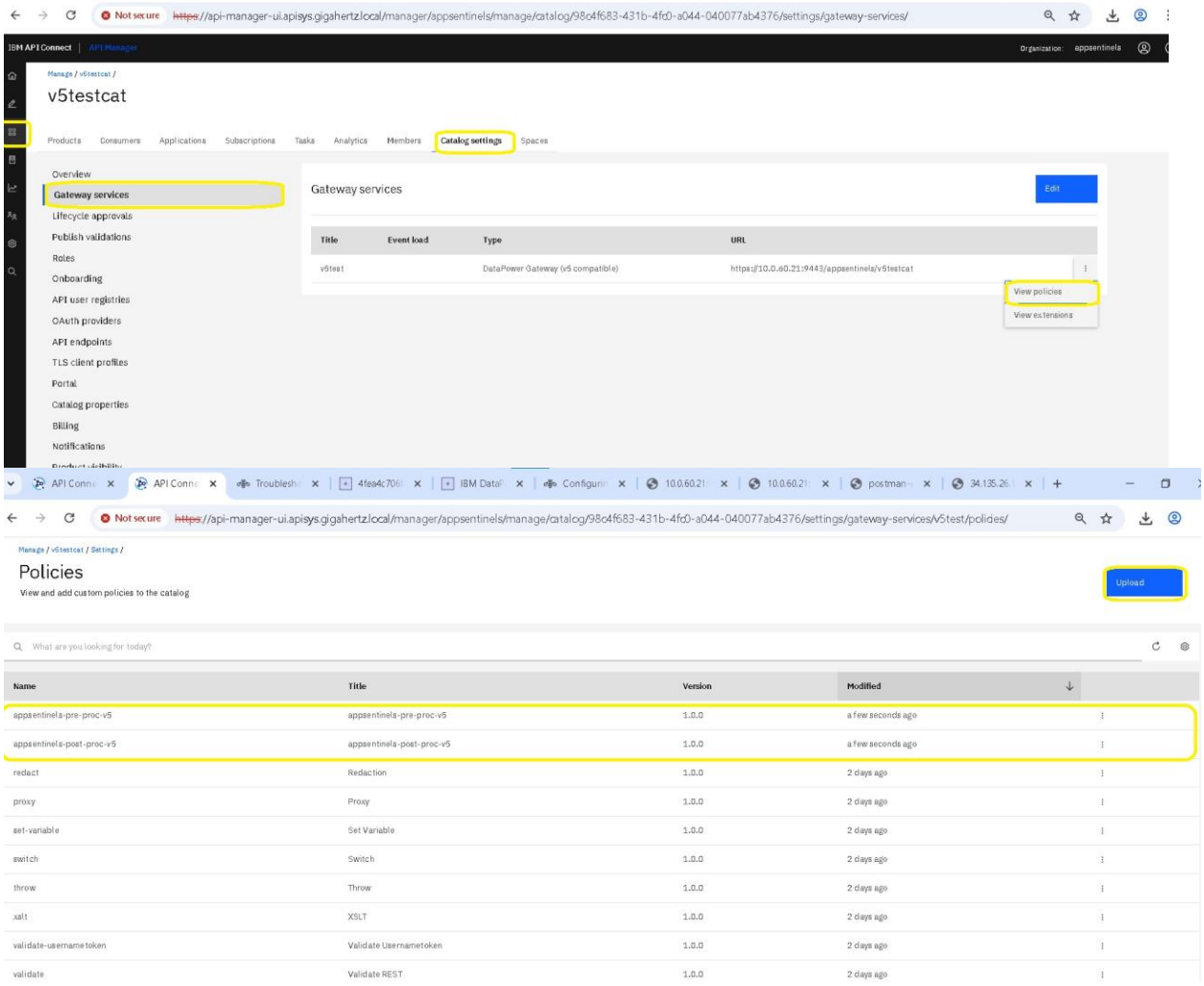


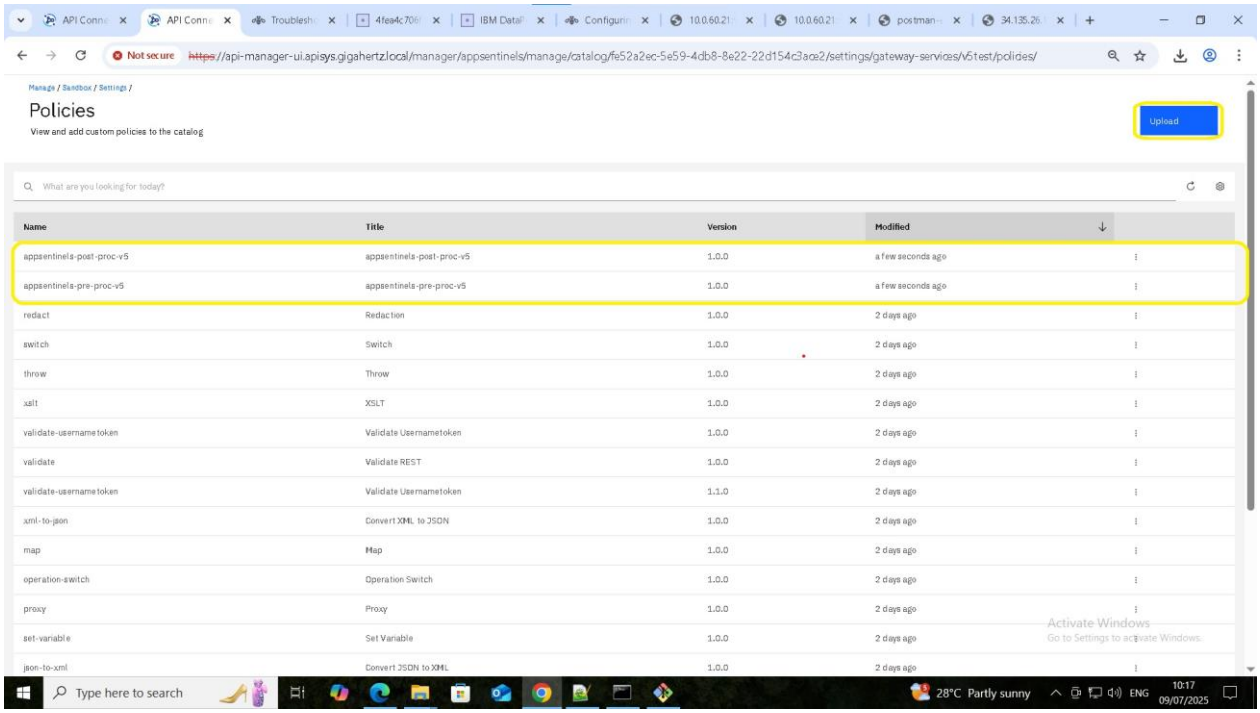


- Rename the downloaded files like below:
  - appsentinels-pre-proc-v5-main.zip --> appsentinels-pre-proc-v5.zip
  - appsentinels-post-proc-v5-main.zip --> appsentinels-post-proc-v5.zip
- Now create a pre-proc folder and do below steps:
  - Under pre-proc folder create a folder name “implementation”
  - Copy the downloaded appsentinels-pre-proc-v5.zip file in implementation folder
  - Copy appsentinels-pre-proc-v5.yaml file in pre-proc folder
  - Create a zip file named **appsentinels-pre-proc-v5.zip** which contain “implementation” folder and appsentinels-pre-proc-v5.yaml file
- Now create a post-proc folder and do below steps:
  - Under post-proc folder create a folder name “implementation”
  - Copy the downloaded appsentinels-post-proc-v5.zip file in implementation folder
  - Copy appsentinels-post-proc-v5.yaml file in post-proc folder
  - Create a zip file named **appsentinels-post-proc-v5.zip** which contain “implementation” folder and appsentinels-post-proc-v5.yaml file

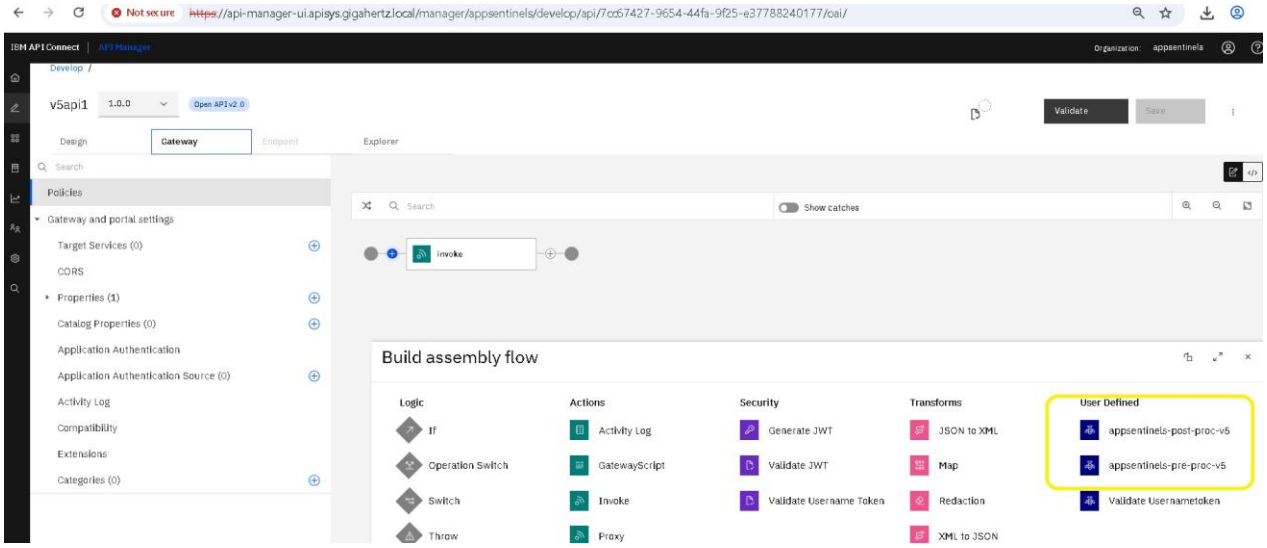
Upload and apply the Policy in IBM API Manager

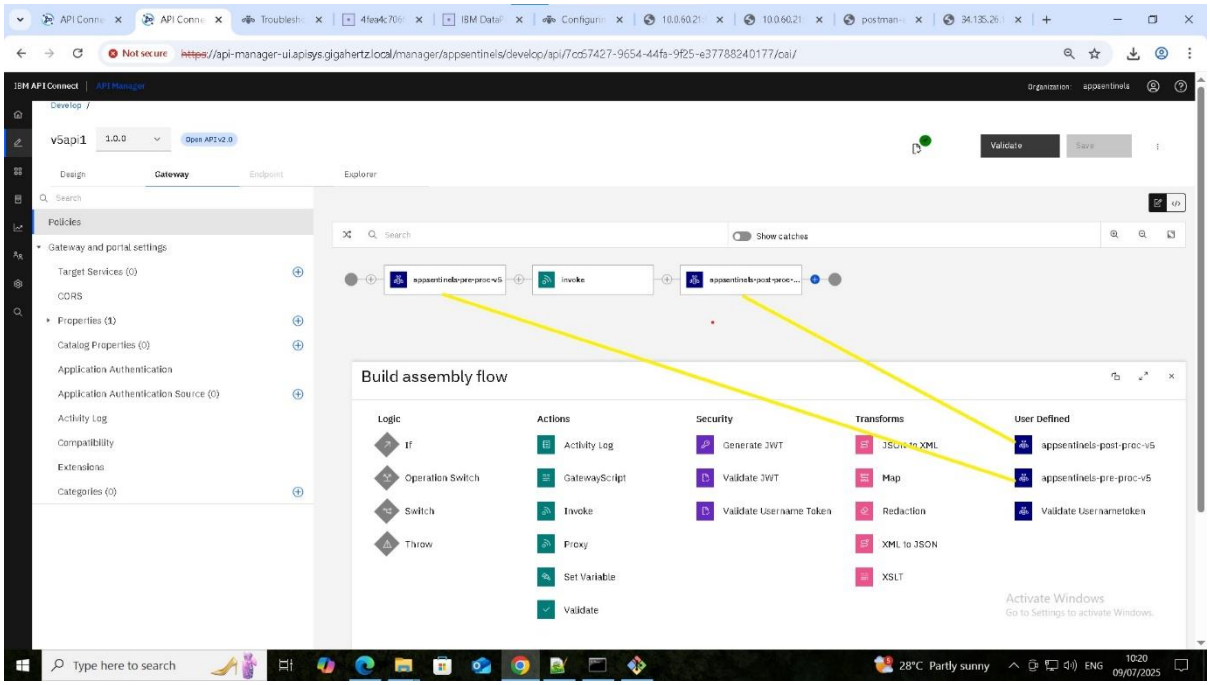
- After creating the two policy zip files (**appsentinels-pre-proc-v5.zip and appsentinels-post-proc-v5.zip**) now you must upload the policy to specific catalog and apply the policy to specific API
- Log in to API manager UI and navigate through
    - Manage--> Select the catalog --> Catalog Settings --> Gateway Service -->3dots --> View Policy --> Upload
    - Manage--> Sandbox --> Catalog Settings --> Gateway Service -->3dots --> View Policy --> Upload
    - **Note:** You must upload the policy in Sandbox catalog along with the intended catalog, otherwise it will not appear in API assembly pallet.





- So, after upload the policies, both the policies will appear in API assemble pallet, now just drag and drop the policy and save and publish the API to activate the policy





AppSentinels Global Policy Instrumentation (Per catalog) (V5 Compatible Gateway)

Prerequisites

Ensure that you have access to the API Connect CLI and a valid credential file before proceeding.

Please download the required files from: [Appsentinels_V5_Global_Policy]

Register Toolkit Credentials

Run the following command to set your credentials:

Command: apic client-creds:set <path to your downloads>/credentials. Json

Example: apic client-creds:set credentials. Json

Authenticate with API Connect

Run the login command with your credentials and server information:

Command: apic login --server <API Manager URL> --username <username> --password <password> --realm <realm>

Example: apic login --server https://api-manager-ui.apicman.local --username user.name --password password --realm provider/default-idp-2

Deploy the Policy Globally

Use the following command to apply the policy:

Command: ***./manage_global_policy-v5.sh -d -c <Controller IP> -t <TLS profile name> -s <API Manager URL> -o <Organization> -g <Catalog name> -w <Gateway name>***

Example: ./manage_global_policy-v5.sh -d -c 104.154.155.131 -t test-tls-prof -s https://api-manager-ui.apicman.local -o appsentinels -g catalog1 -w gw03

Remove the Policy Globally

Use the following command to remove the policy:
Command: ***./manage_global_policy-v5.sh -r -c <Controller IP> -t <TLS profile name> -s <API Manager URL> -o <Organization> -g <Catalog name> -w <Gateway name>***
Example: ./manage_global_policy-v5.sh -r -c 104.154.155.131 -t test-tls-prof -s https://api-manager-ui.apicman.local -o appsentinels -g catalog1 -w gw03

Usage of the manage_global_policy-v5.sh Script

The script `manage_global_policy-v5.sh` is used to deploy or remove the policy globally within a specific catalog. It accepts the following parameters:

-d: Deploy the policy
-r: Remove the policy
-c: AppSentinels Controller Hostname/IP
-t: TLS Client Profile name
-s: API Manager URL
-o: Organization under API Manager
-g: Catalog name to be instrumented
-w: DataPower Gateway Service Name

Troubleshoot

- To see the failure logs login to IBM DataPower UI and in home page select the 'view logs' tab

Reference

- https://www.ibm.com/docs/en/api-connect/10.0.8_lts?topic=topology-registering-gateway-service
- https://www.ibm.com/docs/en/api-connect/10.0.8_lts?topic=connect-configuring-datapower-api-gateway
- https://www.ibm.com/docs/en/api-connect/10.0.x_cd?topic=apdag-defining-packaging-publishing-catalog-scoped-policy-api-gateway
- https://www.ibm.com/docs/en/api-connect/10.0.x_cd?topic=apdag-defining-packaging-publishing-global-scoped-policy-api-gateway
- https://www.ibm.com/docs/en/api-connect/10.0.8_lts?topic=applications-working-global-policies

