

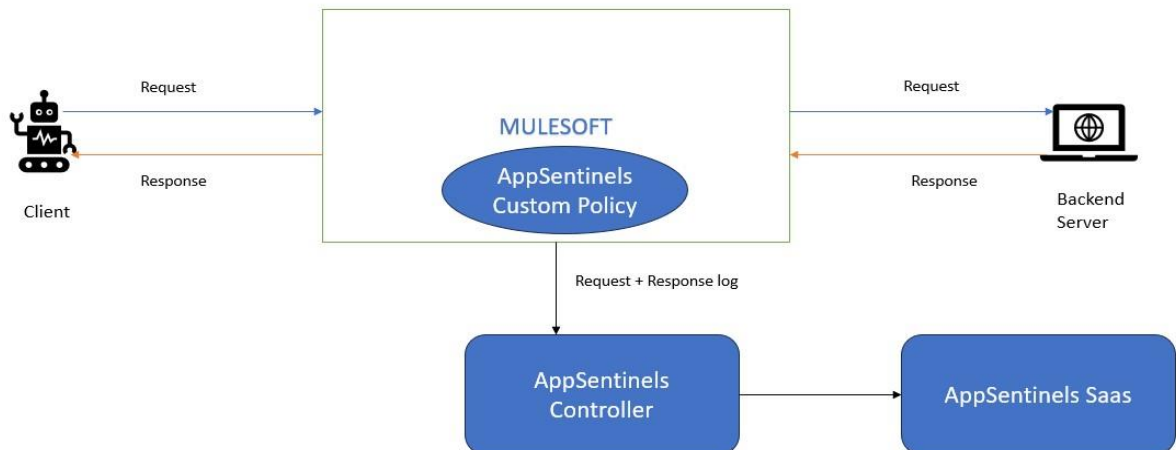
# AppSentinels API Security Platform

## Policy Integration for MuleSoft

## Contents

Prerequisite.....	2
Procedure to deploy policy in anypoint platform.....	3
Procedure to apply policy in API/APIs in anypoint platform .....	4
Specific API:.....	4
Automated Policy: .....	4

**MuleSoft** is an integration and API management platform that helps organizations connect applications, data, and devices — both on-premises and in the cloud. It provides tools to build, manage, and secure APIs and integrations through its core product, **Anypoint Platform**.



## Prerequisite

- Maven (mvn version  $\geq$  3.9.0) must be installed.
- To upload custom policy to MuleSoft Exchange, you must have the exchange contributor's role assigned to you.
- Keep the below parameters handy—
  - Organization Id/Business Group Id
  - Client Id
  - Client Secret
- IP address/FQDN of appsentinels controller

## Procedure to deploy policy in anypoint platform

- Download the policy zip file from below link
  - Link: Please contact appsentinels support
- Unzip the file
- Enter into appsentinels directory
- In pom.xml under appsentinels directory change the group Id in (Group Id Mean Organization Id/Business Group Id):
  - `<exchange.url>https://maven.anypoint.mulesoft.com/api/v1/organizations /$ {group Id}/maven</exchange.url>`
  - `<groupId>$ {group Id}</groupId>`
- In the system where mvn is installed go to C:\Users\\${username}\.m2 location and change **username** and **password** with your anypoint platform in settings.xml file:

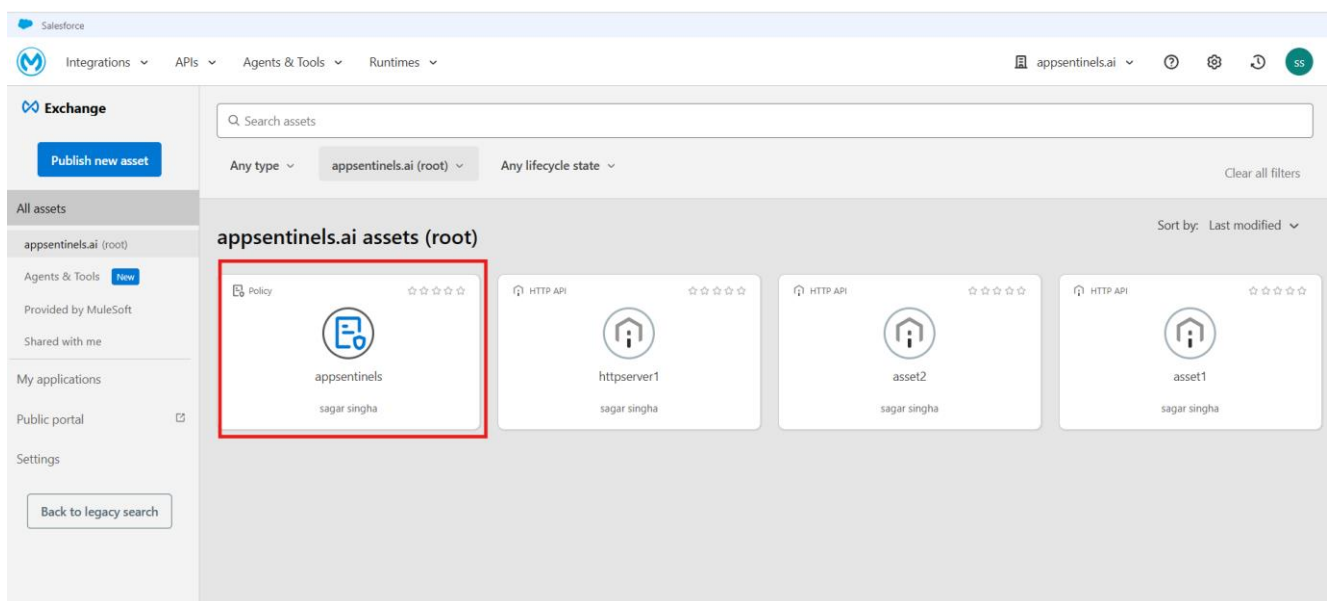
```

<servers>
  <server>
    <id>cloudhub</id>
    <username>${Username}</username>
    <password>${Password}</password>
  </server>
</servers>

```

- Then run below command to deploy the policy to anypoint platform
  - Command: mvn clean deploy

Now policy will be accessible from API manager in anypoint platform. Now appsentinels policy will be appeared under Exchange:



## Procedure to apply policy in API/APIs in anypoint platform

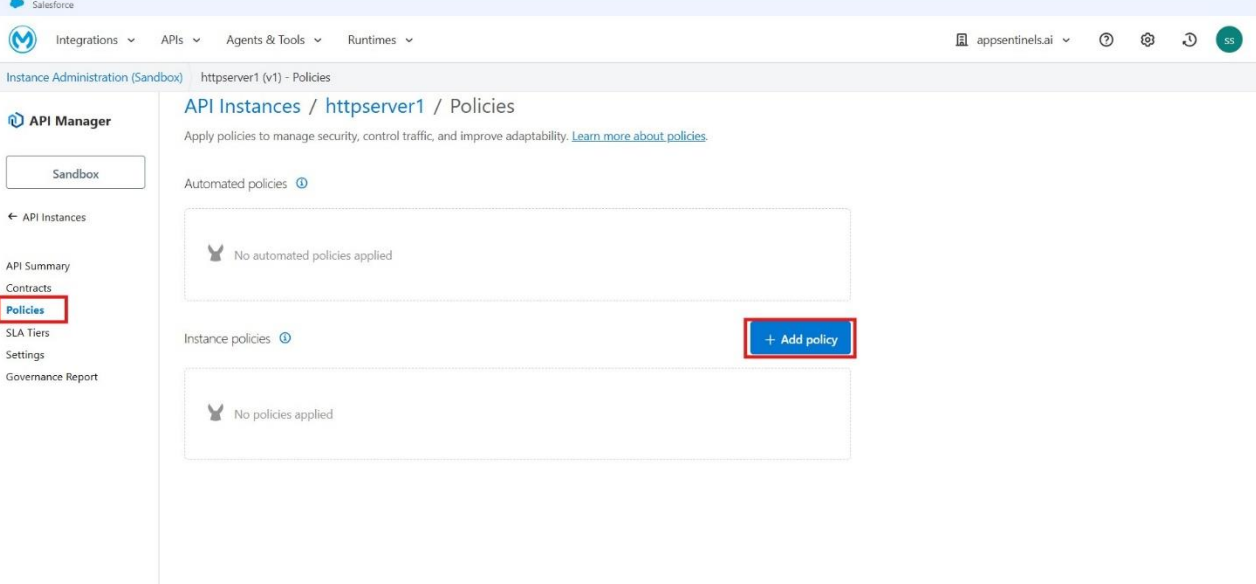
You can apply the policy in anypoint platform in two ways –

- Specific API
- Automated Policy

### Specific API:

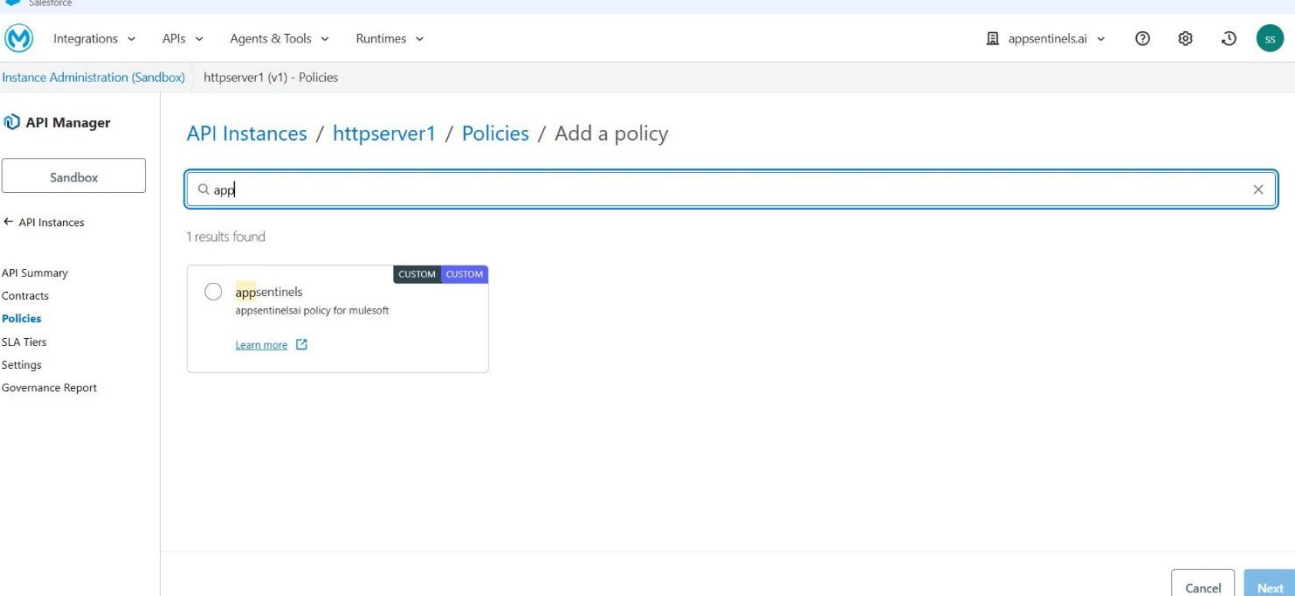
Follow the below steps to apply the appsentinels policy to the APIs that you wish to secure:

- Login to your Anypoint Platform and navigate to API Manager.
- Select the API to which you wish to attach the Traceable policy.
- Click on the **Policies** option and do add policy as shown below



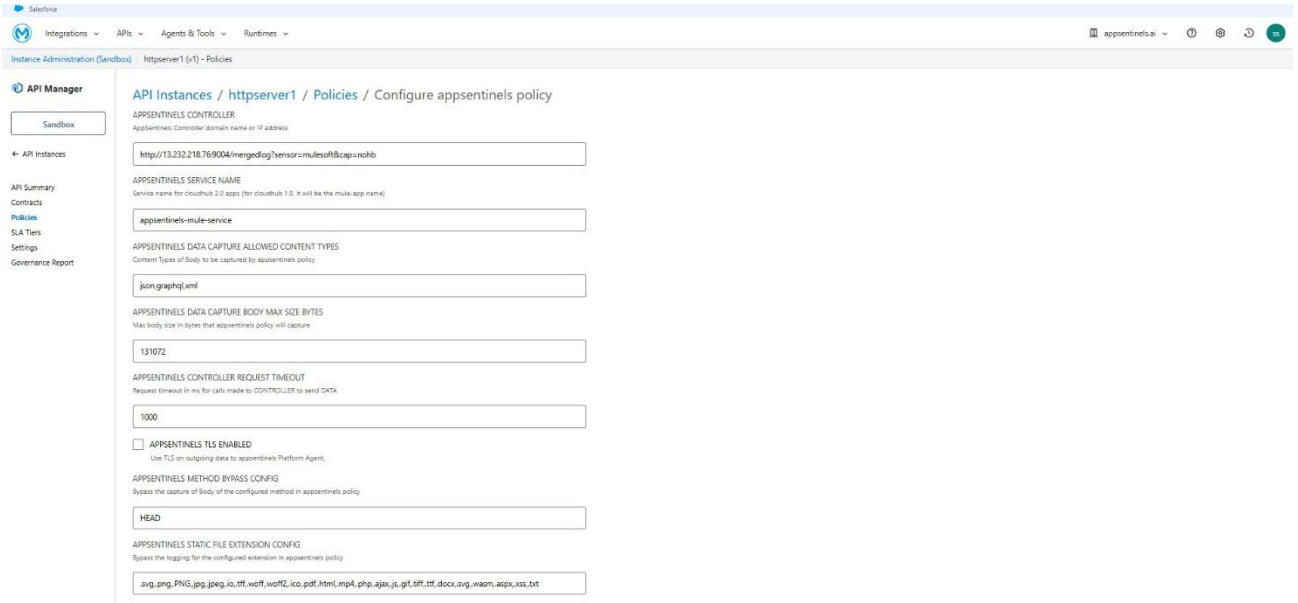
The screenshot shows the Salesforce API Manager interface. The breadcrumb trail is "Instance Administration (Sandbox) / httpserver1 (v1) - Policies". The main heading is "API Instances / httpserver1 / Policies". Below this, there are two sections: "Automated policies" and "Instance policies". Both sections currently show "No [type] policies applied". A red box highlights the "+ Add policy" button in the "Instance policies" section. On the left sidebar, the "Policies" menu item is also highlighted with a red box.

- Search for appsentinels



The screenshot shows the "Add a policy" page in Salesforce API Manager. The breadcrumb trail is "Instance Administration (Sandbox) / httpserver1 (v1) - Policies / Add a policy". A search bar at the top contains the text "app". Below the search bar, it says "1 results found". A search result is displayed with a radio button, the name "appsentinels", and the description "appsentinels policy for mulesoft". There are two "CUSTOM" tags next to the result name. A "Learn more" link is also present. At the bottom right, there are "Cancel" and "Next" buttons.

- Update the appsentinels controller URL like below in APPSENTINELS CONTROLLER box (Ex: **http://20.165.225.120:9004/mergedlog?sensor=mulesoft&cap=nohb**)



The screenshot shows the 'Configure appsentinels policy' page for the 'httpserver1' instance. The left sidebar contains navigation options: API Manager (selected), Sandbox, API Instances, API Summary, Contracts, Policies, SLA Tiers, Settings, and Governance Report. The main content area includes the following configuration fields:

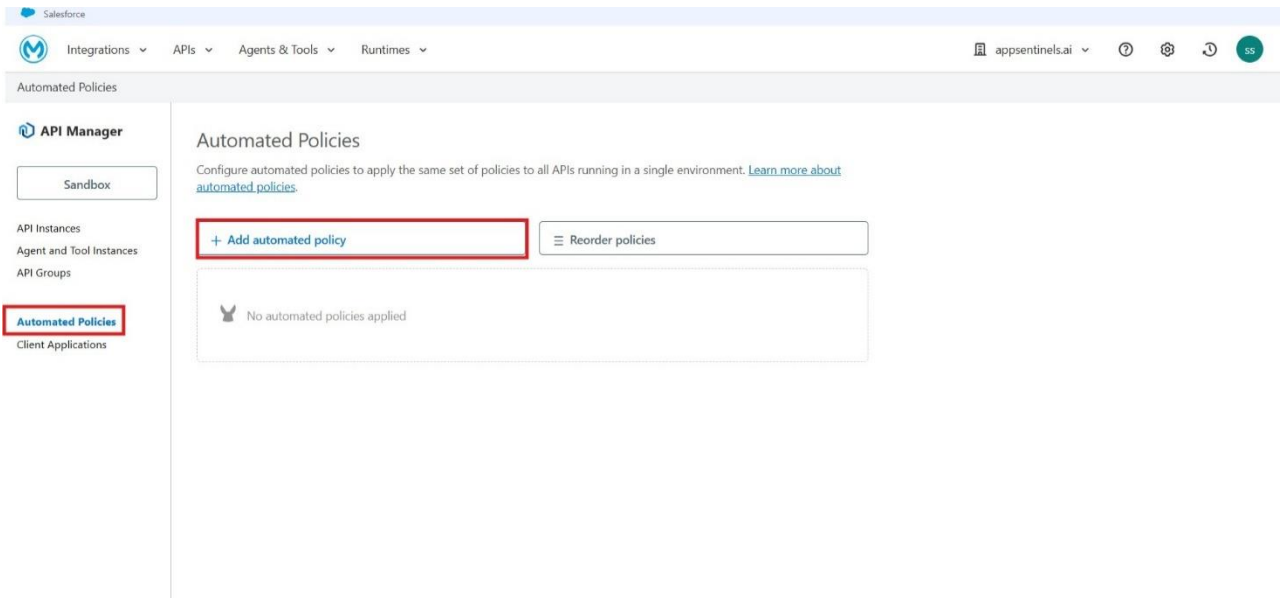
- APPSENTINELS CONTROLLER:** AppSentinels Controller domain name or IP address: `http://13.232.218.76:9004/mergedlog?sensor=mulesoft&cap=ncbb`
- APPSENTINELS SERVICE NAME:** Service name for cloudhub 2.0 apps (for cloudhub 1.0, it will be the mule-app name): `appsentinels-mule-service`
- APPSENTINELS DATA CAPTURE ALLOWED CONTENT TYPES:** Content Types of Body to be captured by appsentinels policy: `json,graphql.xml`
- APPSENTINELS DATA CAPTURE BODY MAX SIZE BYTES:** Max body size in bytes that appsentinels policy will capture: `131072`
- APPSENTINELS CONTROLLER REQUEST TIMEOUT:** Request timeout in ms for calls made to CONTROLLER to send DATA: `1000`
- APPSENTINELS TLS ENABLED:** Use TLS on outgoing data to appsentinels Platform Agent.
- APPSENTINELS METHOD BYPASS CONFIG:** Bypass the capture of Body of the configured method in appsentinels policy: `HEAD`
- APPSENTINELS STATIC FILE EXTENSION CONFIG:** Bypass the logging for the configured extension in appsentinels policy: `.svg,.png,.jpg,.jpeg,.ico,.ttf,.woff,.woff2,.ico,.pdf,.html,.mp4,.php,.aspx,.js,.gif,.tiff,.tif,.docx,.org,.msam,.aspx,.xml,.txt`

- Apply the Policy

### Automated Policy:

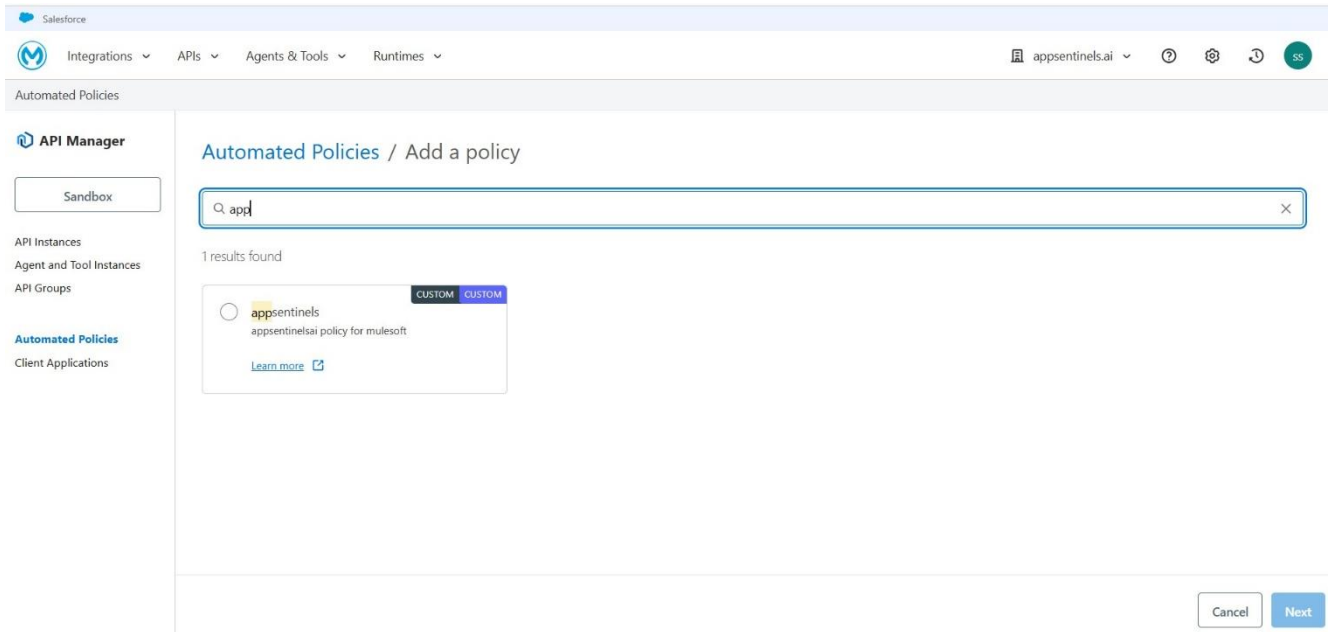
Follow the below steps to apply the appsentinels policy to all the APIs:

- Login to your Anypoint Platform and navigate to API Manager.
- Click on Automated Policies from the left navigation menu.

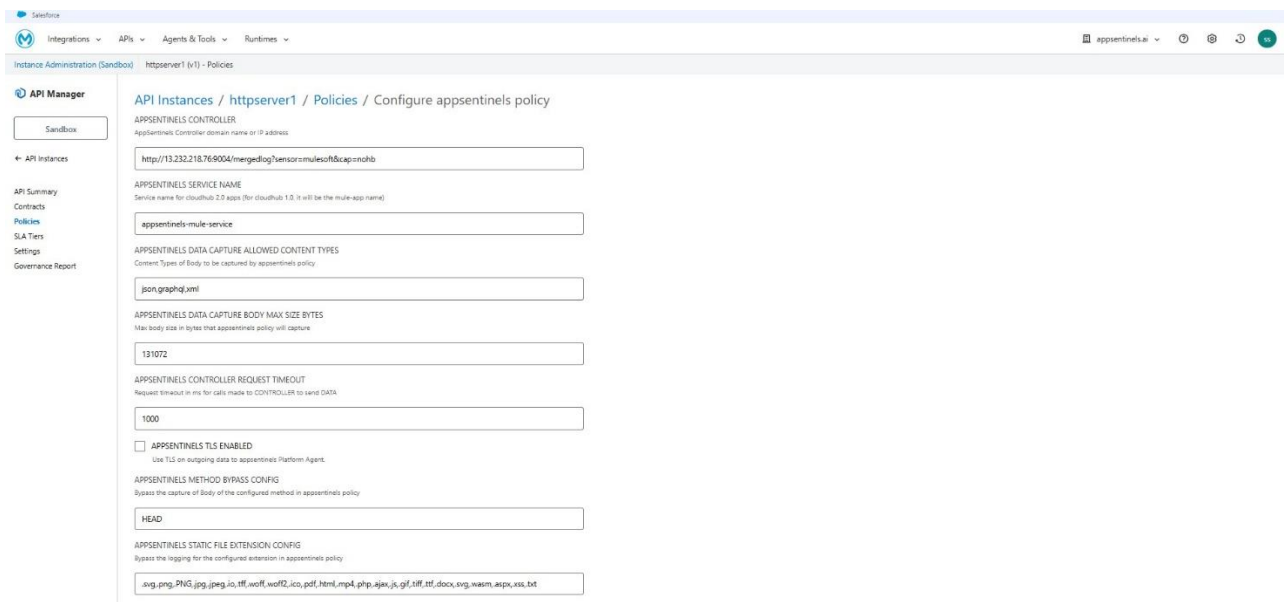


The screenshot shows the 'Automated Policies' page in the API Manager. The left sidebar has 'Automated Policies' highlighted in a red box. The main content area shows the 'Automated Policies' section with a description: 'Configure automated policies to apply the same set of policies to all APIs running in a single environment. [Learn more about automated policies](#)'. There is a '+ Add automated policy' button highlighted in a red box, and a 'Reorder policies' button. Below these buttons, a message states 'No automated policies applied' with a shield icon.

- Search for appsentinels



- Update the appsentinels controller URL like below in APPSENTINELS CONTROLLER box (Ex: <http://20.165.225.120:9004/mergedlog?sensor=mulesoft&cap=nohb>)



- Apply the policy