# 

[What is Rate Limiter?](#_cmayb2l7vx0b)

[When to use Rate Limiter?](#_unbsmyx6hj67)

[Terminology](#_bn57z7fmrbvo)

[Workflow](#_5jcjk6l94rmr)

[Minimal Raptor Version Required](#_ao31adqgjznq)

[How to onboard Shield to Raptor Service](#_20l6nisku1wx)

[Integrate with Shield Handler](#_q31ay4aje1md)

[Supported Subjects](#_18vojm11duon)

[Create resource of your policy](#_4nd9453dxhyi)

[Create RateLimiter Policy](#_k58vykhs8kxt)

[Setup config in ConfigEditor](#_bded9gdus7nw)

[Sample Project Github](#_yxykml82kjk5)

[How to onboard Shield to Raptor Web](#_jim3g4ju2oey)

[Integrate with Shield Handler](#_dw2fjq79pnn)

[Supported Subjects](#_geq4s6muioij)

[Create resource of your policy](#_jnh0ezqc865u)

[Create RateLimiter Policy](#_bq7ojtm6lror)

[Setup config in ConfigEditor](#_cg0pwfh2h3rp)

[Sample Project Github](#_aua765bkeyme)

[Special Cases](#_dk734f3g85f1)

[Mix use of SpringMVC & Ginger in one application](#_2hd45h74emg)

[Register customized handler to deal with BLOCK|FLAG](#_1pfhnzbjkkb1)

[Contact us](#_39s4tztv2asd)

[FAQ](#_mnpey1uvbbtl)

# 

# What is Rate Limiter?

Rate Limiter helps control the rate of traffic to an application to avoid overuse of resources. It also provides defense against DoS attacks by allowing application owners to set a threshold for a maximum number of requests over a given time period, upon which violators will either be flagged, see a captcha to access the site, or outright be blocked.

RL supports rate-limiting, in general, on subjects that attempt to access a set of resources (pre-)defined in the system. URLs (or web pages) and APIs are examples of resources; so are SOA services and operations. Subjects can be an application, an end user, IP, etc. Rate Limiter has support to limit traffic based on IP, Application/Consumer and Users.

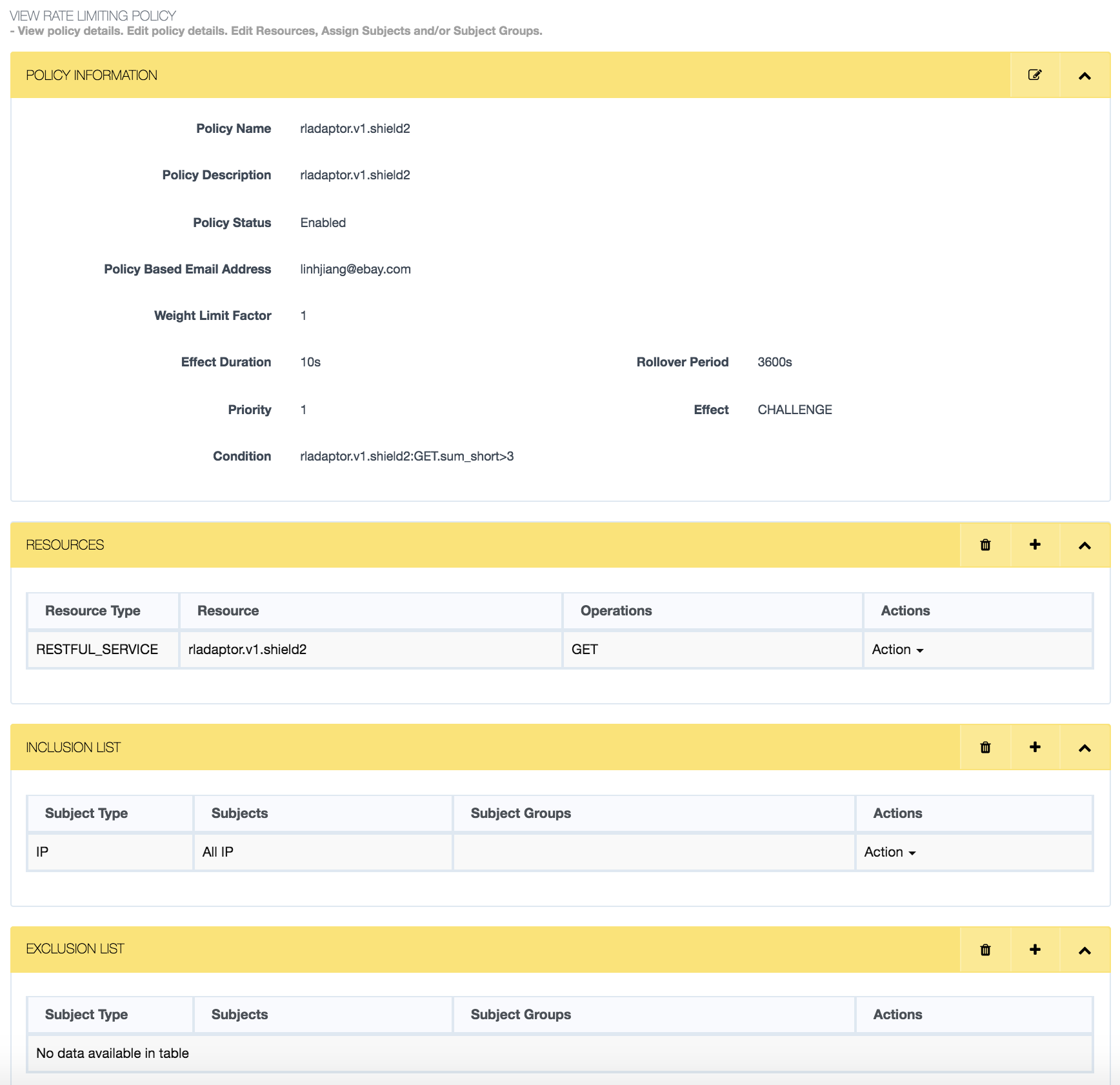
There are two flavors of Rate Limiting engine currently in Production. The legacy engine is called Traffic Limiter (TL) that supports IP based rate limiting only. Rate Limiter (RL) is a successor of Traffic Limiter. RL offers a number of advantages over the prior TL. The most important being support for multiple subject types. Traffic Limiter is out of support and this document will mostly focus on Rate Limiter.

# When to use Rate Limiter?

If you have one of the following requirements, rate limiting would be your choice.

* Budget - Controlling access volumes to your webapp and/or service
* Trust and Security (TnS) - Protecting the site from Denial of Service (DOS) attacks

# Terminology

****

* Policy Name
* Needs to be an alphanumeric string WITHOUT SPACES.
* Policy Description

Brief description of the policy

* Policy Based Email address

This feature is currently disabled. This field can be left empty.

* Weight Limit Factor

Currently this is not being actively used; hence a default value of "1" can be put. Refer Weight for additional information. Contact RL Support DL if you want to use this feature.

* Effect
* There are three options "BLOCK", "CHALLENGE", "FLAG". Rate Limiter will enforce the configured action once the threshold defined in "Condition" field gets crossed. BLOCK will terminate the request, CHALLENGE is used to redirect the user to Captcha page and FLAG can be used as a soft limit.
* Effect Duration
* Displays the time period (in seconds) for which the effect on violation of the rate limiting policy will be enforced. Suppose you have the effect "Block” defined in the rule, once the user crosses the threshold, it will see the response as Block for the next duration as set in “Effect Duration” field.
* Rollover Period
* Displays the time period after which the count for the rate limiting policy is reset. Currently 1 hr (3600 sec) and 24 hr (86400 sec) is supported. More details can be found in following sections.
* Priority
* Displays the priority of the rate limiting policy (1 indicates the highest priority).
* Resource

An accessible but protected element of the system, such as a page or URL identified by an internally assigned ID number and corresponding name. Other resource types include operation and service. For example, REService.GetFees and REService.SetDiscountPercent.

* Rule

Defines the Action taken on condition of satisfying a predicate for the Duration of time.

* Subject

An entity that requests access to the Resource in the system. For example, a client/end-user IP address (as a subject) may access a URL (as a resource).

* Counters: **sum\_long & sum\_short**

Every rollover period has two counters **sum\_long** and **sum\_short** for each pair

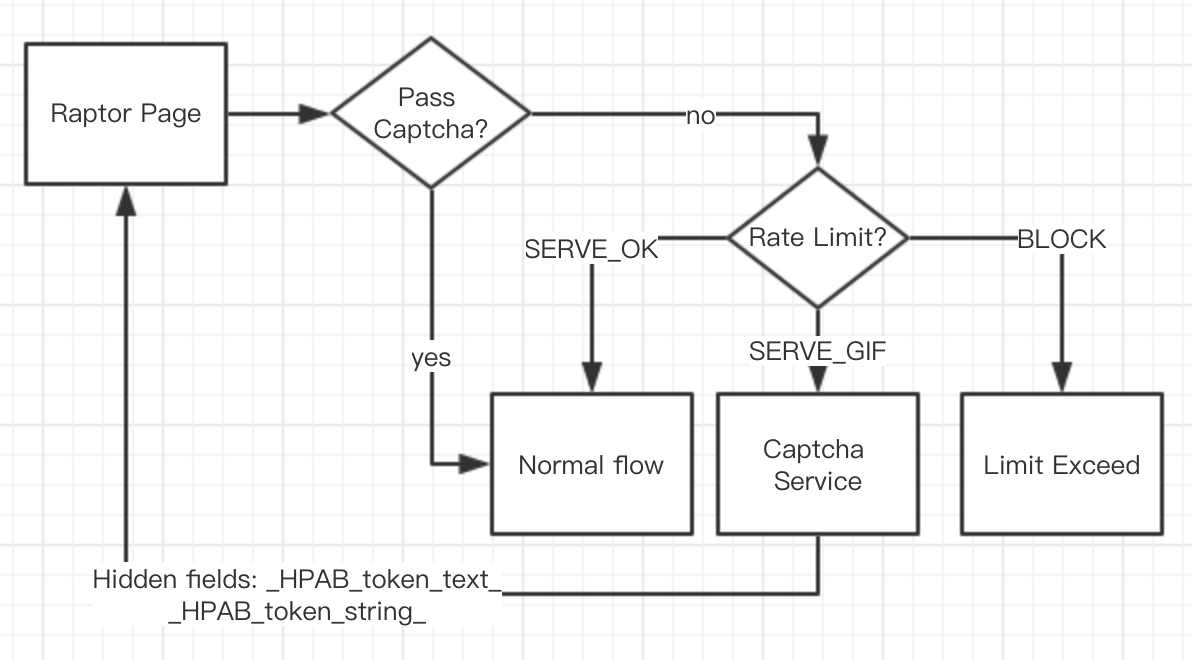
of subject and operation. The former has a period identical to the rollover period, while the latter is reset every 1/240 of the rollover period.

|  |  |  |
| --- | --- | --- |
| sum\_long  (= rollover period) | 24 hours  (86400 sec) | 1 hour  (3600 sec) |
| sum\_short  (= 1/240 rollover period) | 6 min (360 sec) | 15 sec |

So if you select rollover period as • 3600 sec (1 hour), then

* sum\_long counter would reset every 3600 seconds
* sum\_short counter would reset every 15 sec • 86400 sec (24 hours), then
* sum\_long counter would reset every 24 hours o sum\_short counter would reset every 6 min

# Workflow



# Minimal Raptor Version Required

Raptor 2.5.7 is the minimal version required. If you want to onboard to Shield, please upgrade your application to higher Raptor version (>= 2.5.7).

# How to onboard Shield to Raptor Service

## Integrate with Shield Handler

First, import maven dependency into pom.xml

<dependency>

<groupId>com.ebay.app.shield.handler</groupId>

<artifactId>ShieldHandler</artifactId>

</dependency>

Please specify the ShieldHandler version 1.0.4-RELEASE, if your application is using lower version(<2.7.0) Raptor.

Second, enable Shield Handler. Specify package of ShieldAspect in component-scan element in contextConfigLocation of GingerServlet, default path is /WEB-INF/spring/ginger-servlet.xml.

|  |
| --- |
| <context:component-scan base-package="com.ebay.app.shield.handler" /> |

It depends on AspectJ, so that you need to make sure your application has enabled the AspectJ auto-proxy.

|  |
| --- |
| <aop:aspectj-autoproxy proxy-target-class="true"/> |

Then, place @RateLimit on class/method level. Using annotation - [com.ebay.app.shield.handler.RateLimit](https://github.corp.ebay.com/linhjiang/ShieldHandler/blob/master/src/main/java/com/ebay/app/shield/handler/RateLimit.java) to specify the resourses you want to limit the traffic.

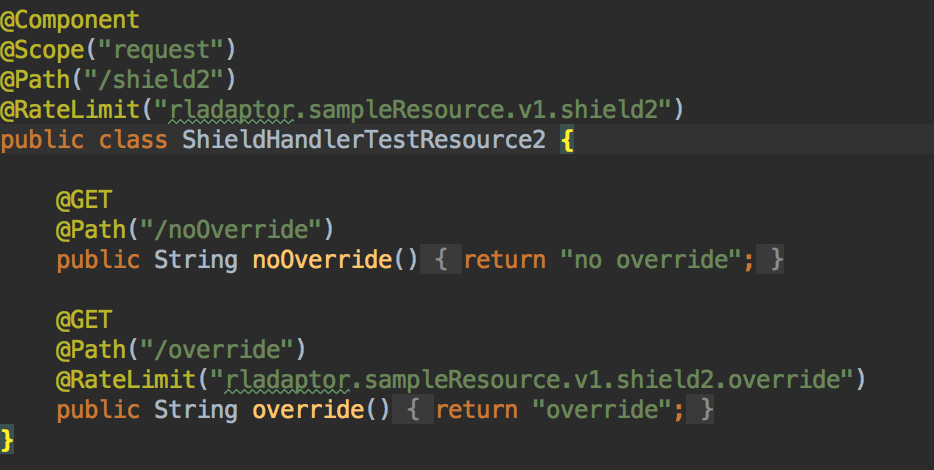
@RateLimit placed in Class level

* all methods in this class will be assessed by SHIELD.
* The value of class level annotation
  + If not defined or blank value, resource name should be AppName+PageName for each method. After removing variables and replace “/” with “.” of relative url, PageName is worked out.
  + If defined, it means all methods will map to same resource name you defined.

@RateLimit placed in Method level

* @RateLimit methods inside @RateLimit class, only the method level take effects.
* The value of method level annotation
  + If not defined or blank value, resource name should be AppName+PageName for each method. After removing variables and replace “/” with “.” of relative url, PageName is worked out.
  + If defined, this method stands for the resource you defined.

Last, cases list below help you understand better

****

Conclusion made for above cases, assume application name is rladaptor and the servlet base path is /rladaptor/sampleResource/v1/\*.

|  |  |  |
| --- | --- | --- |
| **ClassName.MethodName** | **Resource to limit the traffic** | **Where is resource from** |
| ShieldHandlerTestResource1.variables | rladaptor.rladaptor.sampleResource.v1.shield1.variables.and.var\_ | appName + Servlet path + class level @Path value + method level @Path value |
| ShieldHandlerTestResource1.override | rladaptor.sampleResource.v1.shield1.override | Method level @RateLimit |
| ShieldHandlerTestResource2.noOverride | rladaptor.sampleResource.v1.shield2 | Class Level @RateLimit |
| ShieldHandlerTestResource2.override | rladaptor.sampleResource.v1.shield2.override | Method level @RateLimit |

We recommend not override the value of @RateLimit, **using the default name conversion** is better. **More importantly, the resource name is very important to onboard SHIELD to your application. It should be strictly match the resource you define in your Ratelimiter policy.**

## Supported Subjects

SHIELD RateLimiter Handler will provide capability to support subjects - IP, EBAYUSER, EBAYAPP, DEVICEID.

* IP

very easy for application to prepare IP subject, no extra dependencies.

* EBAYUSER & EBAYAPP

Need to import below dependency to enable EBAYUSER & EBAYAPP subject

<dependency>

<groupId>com.ebay.authentication</groupId>

<artifactId>CoreAuthenticationAdaptor</artifactId>

</dependency>

User or app info is from HTTP request header of **Authorization**.

* DEVICEID

Need to import below dependencies to enable DEVICEID subject

<dependency>

<groupId>com.ebay.authentication</groupId>

<artifactId>CoreAuthenticationAdaptor</artifactId>

</dependency>

<dependency>

<groupId>com.ebay.platform.raptor</groupId>

<artifactId>RaptorCOSAdaptor</artifactId>

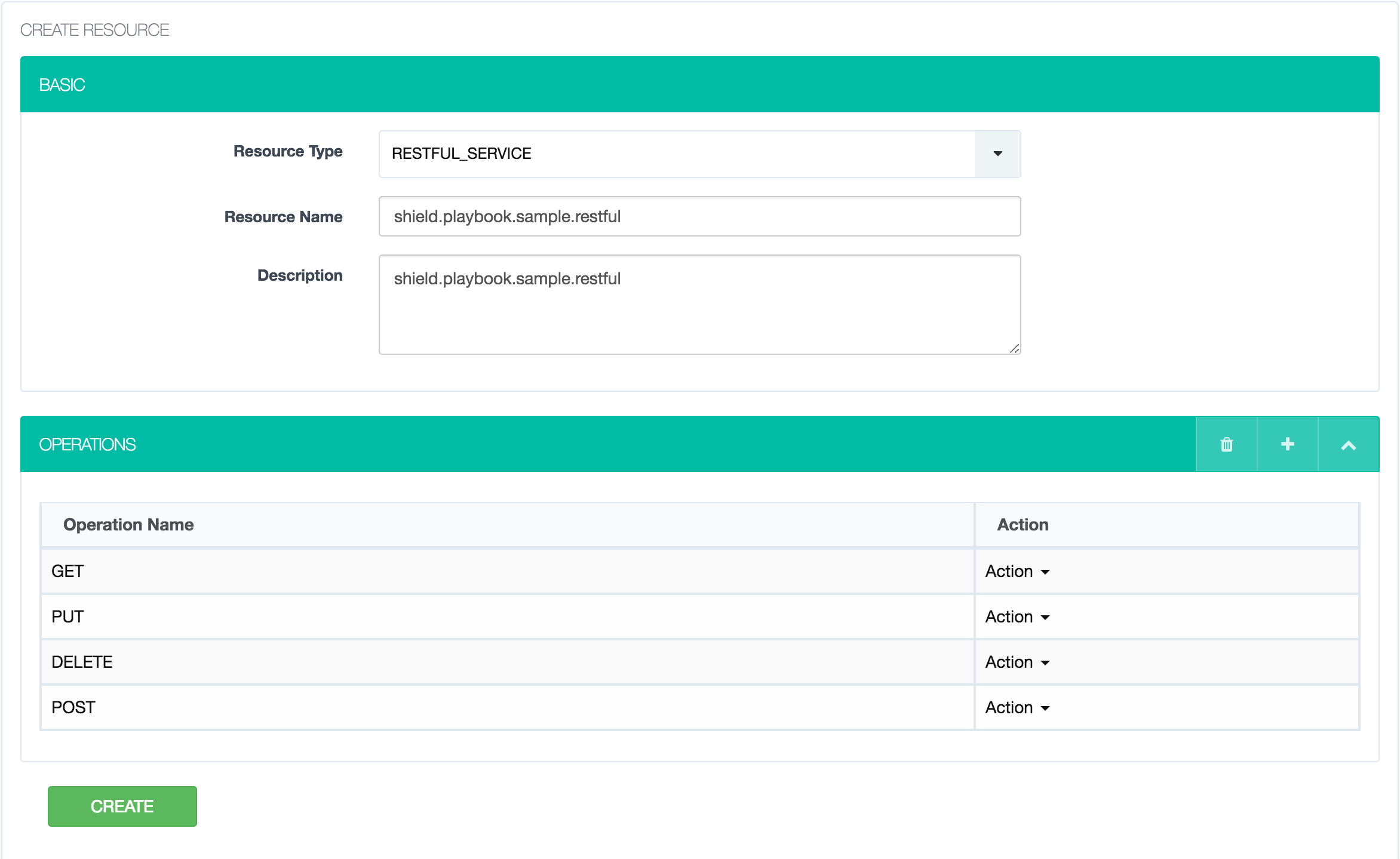
</dependency>

Dependency CoreAuthenticationAdaptor is imported, that means **Authorization** must be present in HTTP Request Header. And DEVICEID will be retrieved from HTTP request header of **X-EBAY-C-ENDUSERCTX**. Below is the sample:

X-EBAY-C-ENDUSERCTX:deviceId=c89d3a3413e0a56a4424af44fff429df,deviceIdType=IDREF,contextualLocation=country%3DRU,ip=0%3A0%3A0%3A0%3A0%3A0%3A0%3A1,userAgentAccept=\*%2F\*,userAgentAcceptEncoding=gzip%2Cdeflate,userAgentAcceptCharset=null,userAgent=Mozilla%2F5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F38.0.2125.111+Safari%2F537.36,uri=%2Fbuy%2Funifiedstream%2Fv1%2Fcontent,origUserId=PRIVATE,clientId=AdminApp,physicalLocation=country%3DUS

## Create resource of your policy

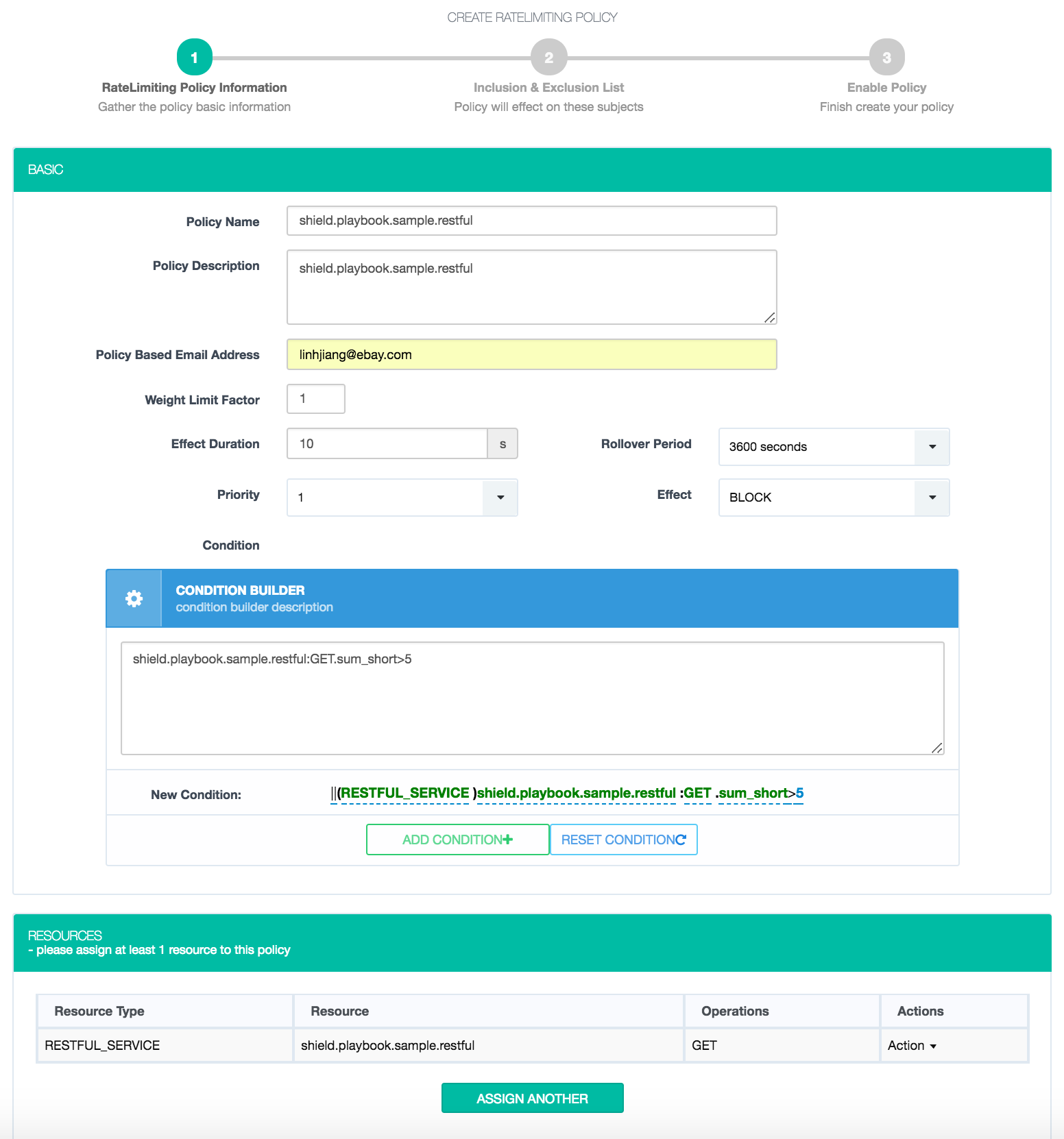
Before creating your policy, you should have resource available in SMC console. You can create your resources by accessing to [resource creation page of SMC Console](http://soteriafe-1538520.phx02.dev.ebayc3.com:8080/resource/add). Then you will see the page same with below:



For Resource Type - RESTFUL SERVICE, GET/PUT/POST/DELETE are available operation names.

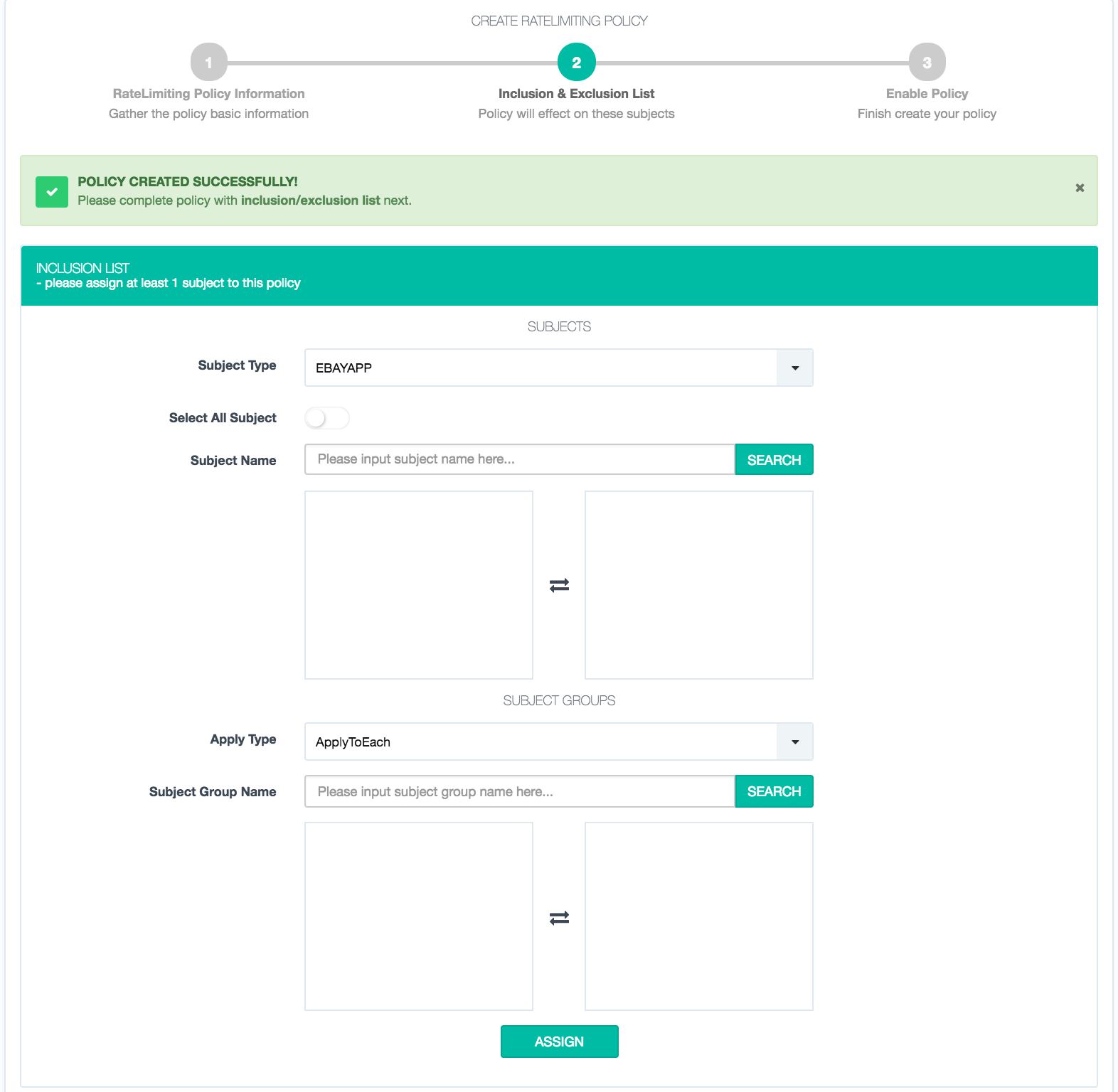
For Resource Type - WEB, you should always use operation name - “any”.

## Create RateLimiter Policy

You can create your policy by accessing to [RateLimiter policy creation page of SMC console](http://soteriafe-1538520.phx02.dev.ebayc3.com:8080/policy/add/rl).

You can refer to the [Terminology](#_bn57z7fmrbvo) to fill above form. Condition builder would be helpful for you to configure the policy threshold.

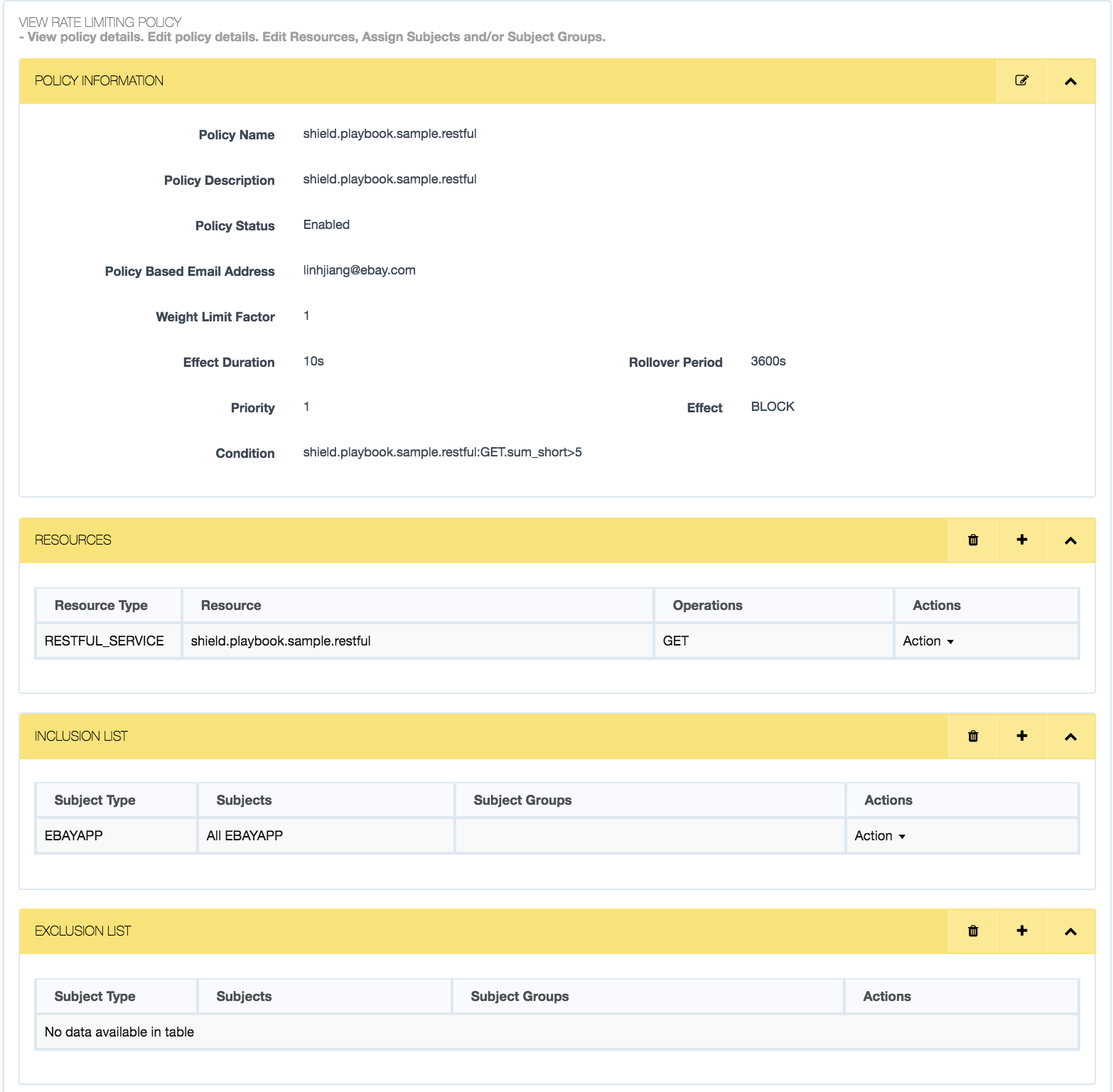
Next, assign subject to inclusion/exclusion list. Subjects in exclusion list will be ignored for this policy, while subjects in inclusion list will be counted.



Choose subject type, and input specific subject name or toggle button “Select All Subject”. There are two values of Apply Type - ApplyToEach and ApplyToAll. They take effect when subject group is specified. ApplyToEach means all subjects in subject group will be counted separatly, while ApplyToAll means subject in group will share the threshold together.

After assign subjects to your policy, you can enable your policy to make it work.

Here is a sample RateLimiter policy and interpretation.



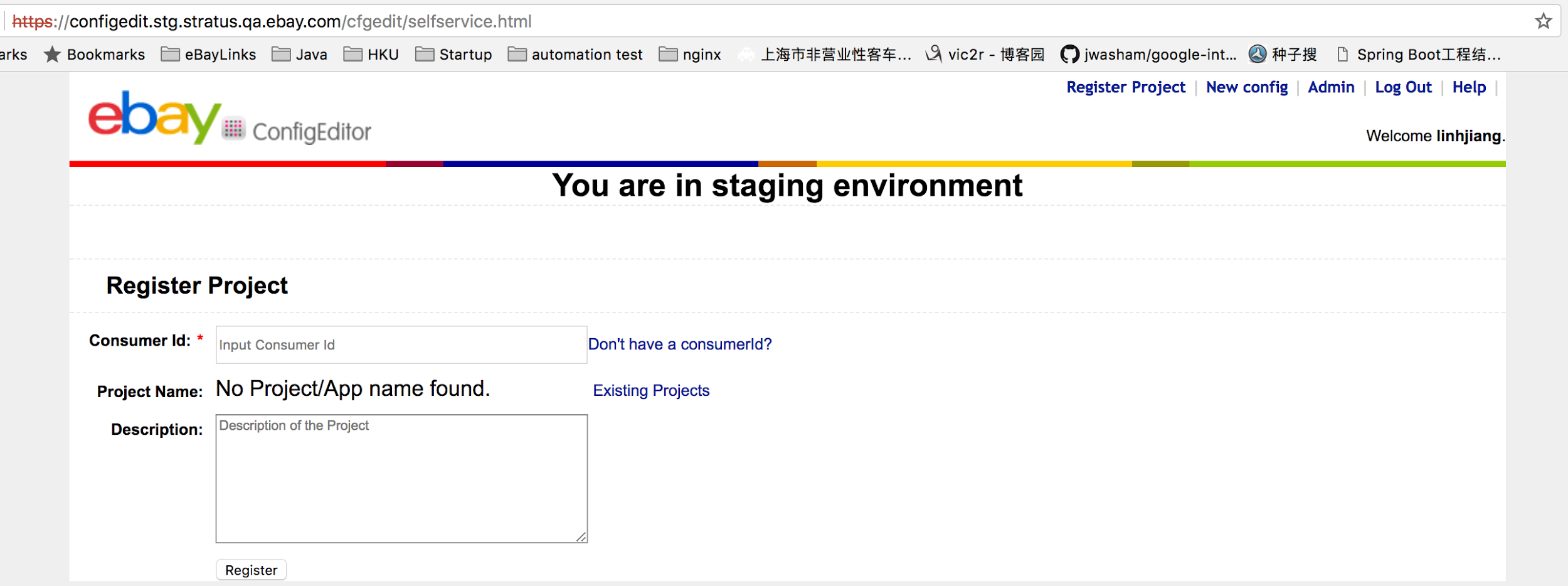
For every access of the resource "shield.playbook.sample.restful", the counters sum\_short and sum\_long get incremented. For the first 5 access calls, “SERVE\_OK” is returned in the response. Once the threshold of 5 is met, the configured Effect "Block " is returned The Condition implies that "GET" operation on the resource "shield.playbook.sample.restful" done more than 5 times within 15 sec (sum\_short=3600s/240) would trigger an Alert and it would stay in the cache for the next 10 seconds and return the Effect "Block" to the user. Once 10 sec period is elapsed further requests get “SERVE\_OK” unless the threshold is met again.

## Setup config in ConfigEditor

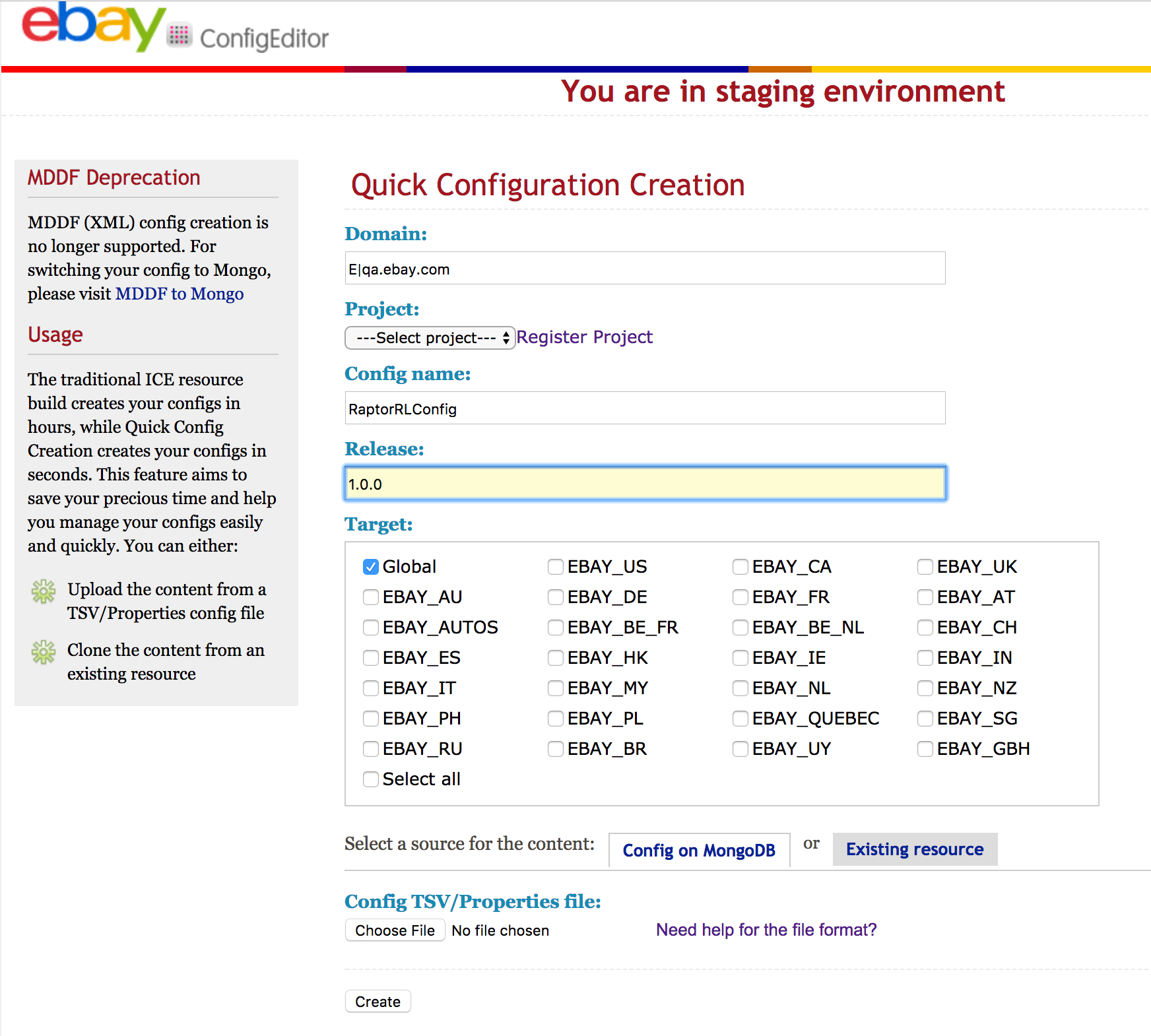
ConfigEditor of staging: <https://configedit.stg.stratus.qa.ebay.com/cfgedit/login.html>

ConfigEditor of prodution: <https://www.cfgedit.stratus.ebay.com/cfgedit/login.html>

1. Register your application If it is not registered in configEditor. Click “Register Project” will redirect you to below page. You can find consumer id of your application in Altus/InfoHub.Fill it in below form and click register.



2. Create config - **RaptorRLConfig** for your application if haven’t. Click “New config” then you will see below page.



Domain: E|qa.ebay.com (default value, no need to change it)

Project: the application you just registered at 1st step.

Config name: RaptorRLConfig

Release: 1.0.0

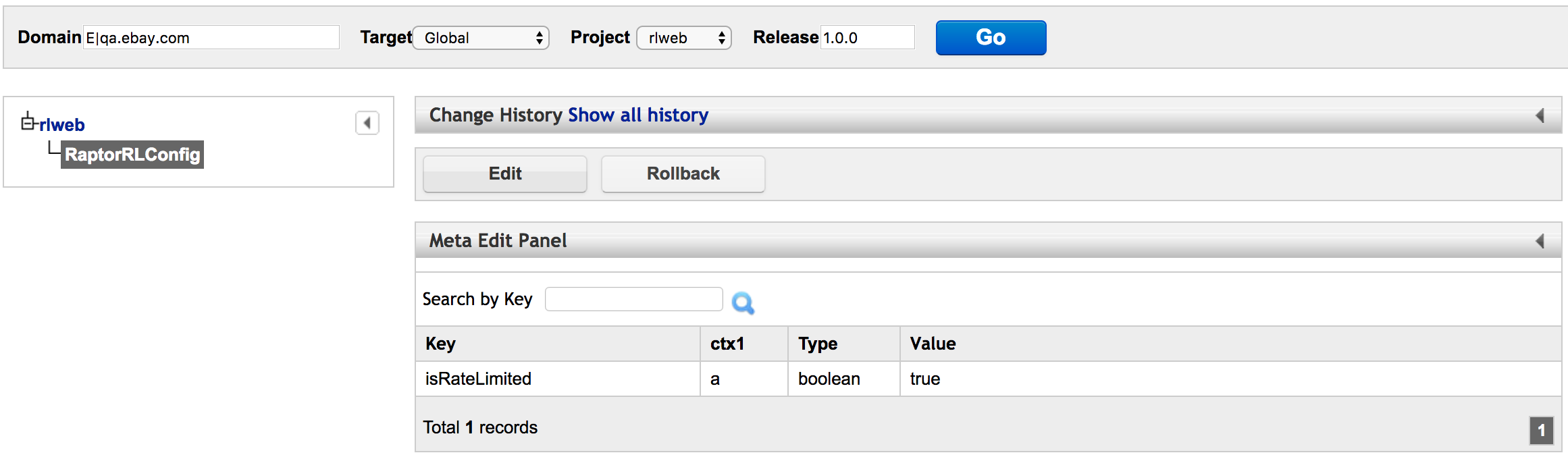
Target: Global

Config TSV/Properties file: [sample tsv file](https://wiki.vip.corp.ebay.com/download/attachments/435569435/RaptorRLConfig.tsv?version=1&modificationDate=1504246910000&api=v2)

Click “Create” button after fill in all these information to finish create your application config.

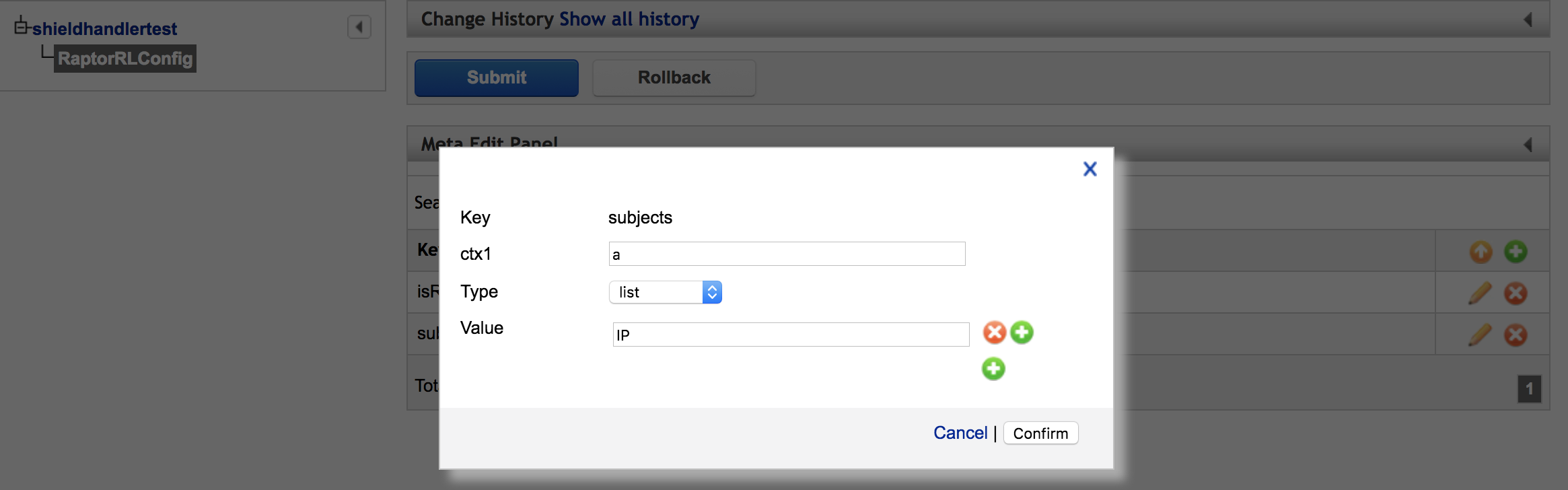
3. Add config key - **isRateLimited** to config, if haven’t. If you use sample tsc file provided by us, you will find config key is already added.

Here is sample Raptor config to enable the Shield.



4. Specify subject types you want to limit traffic (**Optional**)

Add config key - subjects, and list subjects in this config, like below:



If without this config, ShieldHandler will try to extract IP, EBAYUSER, EBAYAPP, DEVICEID from the context and send to Shield Service for Raptor Service.

## Sample Project Github

<https://github.corp.ebay.com/linhjiang/rladaptor>

# How to onboard Shield to Raptor Web

## Integrate with Shield Handler

First, import maven dependency into pom.xml

<dependency>

<groupId>com.ebay.app.shield.handler</groupId>

<artifactId>ShieldHandler</artifactId>

</dependency>

Please specify the ShieldHandler version 1.0.4-RELEASE, if your application is using lower version(<2.7.0) Raptor.

Second, enable Shield Handler. Specify package of ShieldAspect in component-scan element in context.xml.

|  |
| --- |
| <context:component-scan base-package="com.ebay.app.shield.handler" /> |

It depends on AspectJ, so that you need to make sure your application has enabled the AspectJ auto-proxy.

|  |
| --- |
| <aop:aspectj-autoproxy proxy-target-class="true"/> |

Then, place @RateLimit on class/method level. Using annotation - [com.ebay.app.shield.handler.RateLimit](https://github.corp.ebay.com/linhjiang/ShieldHandler/blob/master/src/main/java/com/ebay/app/shield/handler/RateLimit.java) to specify the resourses you want to limit the traffic.

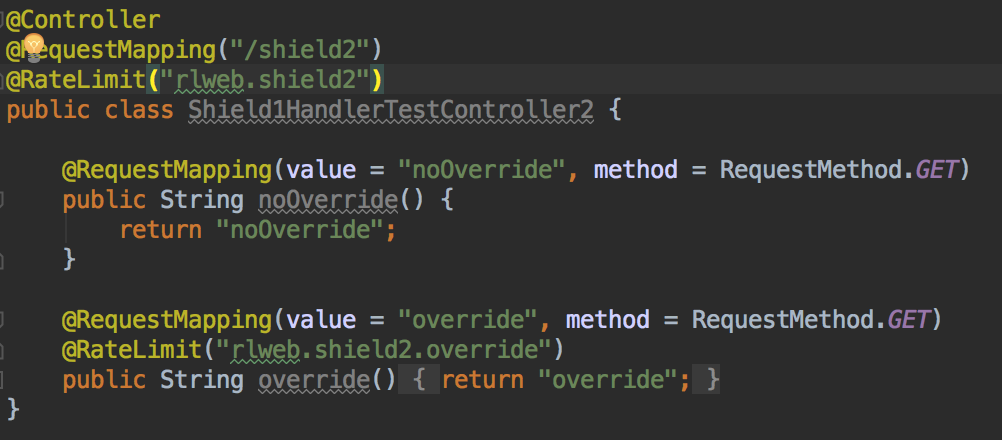
@RateLimit placed in Class level

* all methods in this class will be assessed by SHIELD.
* The value of class level annotation
  + If not defined or blank value, resource name should be AppName+PageName for each method. After removing variables and replace “/” with “.” of relative url, PageName is worked out.
  + If defined, it means all methods will map to same resource name you defined.

@RateLimit placed in Method level

* @RateLimit methods inside @RateLimit class, only the method level take effects.
* The value of method level annotation
  + If not defined or blank value, resource name should be AppName+PageName for each method. After removing variables and replace “/” with “.” of relative url, PageName is worked out.
  + If defined, this method stands for the resource you defined.

Last, cases list below help you understand better

****

Conclusion made for above cases, assume application name is rlweb and the servlet base path is /rlweb/\*.

|  |  |  |
| --- | --- | --- |
| **ClassName.MethodName** | **Resource to limit the traffic** | **Where is resource from** |
| ShieldHandlerTestController1.variables  (two paths in @RequestMapping) | rlweb.rlweb.shield1.variables.and  rlweb.rlweb.shield1.variables.and.var\_ | appName + Servlet path + class level @Path value + method level @Path value |
| ShieldHandlerTestController1.override | rlweb.shield1.override | Method level @RateLimit |
| ShieldHandlerTestController2.noOverride | rlweb.shield2 | Class Level @RateLimit |
| ShieldHandlerTestController2.override | rlweb.shield2.override | Method level @RateLimit |

We recommend not override the value of @RateLimit, **using the default name conversion** is better. **More importantly, the resource name is very important to onboard SHIELD to your application. It should be strictly match the resource you define in your Ratelimiter policy.**

## Supported Subjects

SHIELD RateLimiter Handler will provide capability to support subjects - IP, EBAYUSER, EBAYAPP, DEVICEID.

* IP

very easy for application to prepare IP subject

* EBAYUSER & EBAYAPP

Need to import below dependency to enable EBAYUSER & EBAYAPP subject

<dependency>

<groupId>com.ebay.authentication</groupId>

<artifactId>CoreAuthenticationAdaptor</artifactId>

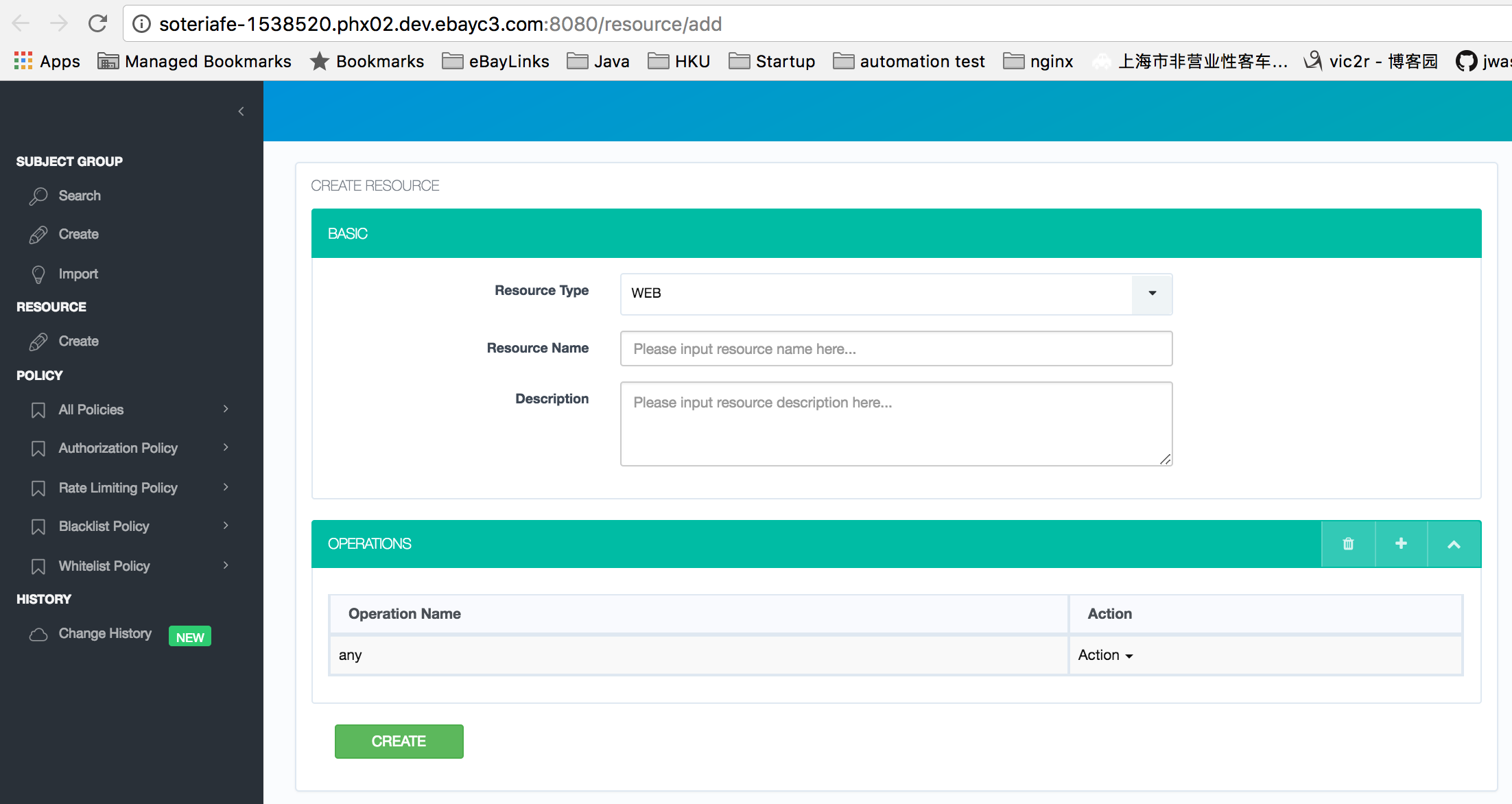
</dependency>

User or app info is from HTTP request header of Authorization.

Default only IP will be used for web app. If you want use EBAYUSER & EBAYAPP, please refer to step 4 of the section of [Setup config in ConfigEditor](#_cg0pwfh2h3rp).

## Create resource of your policy

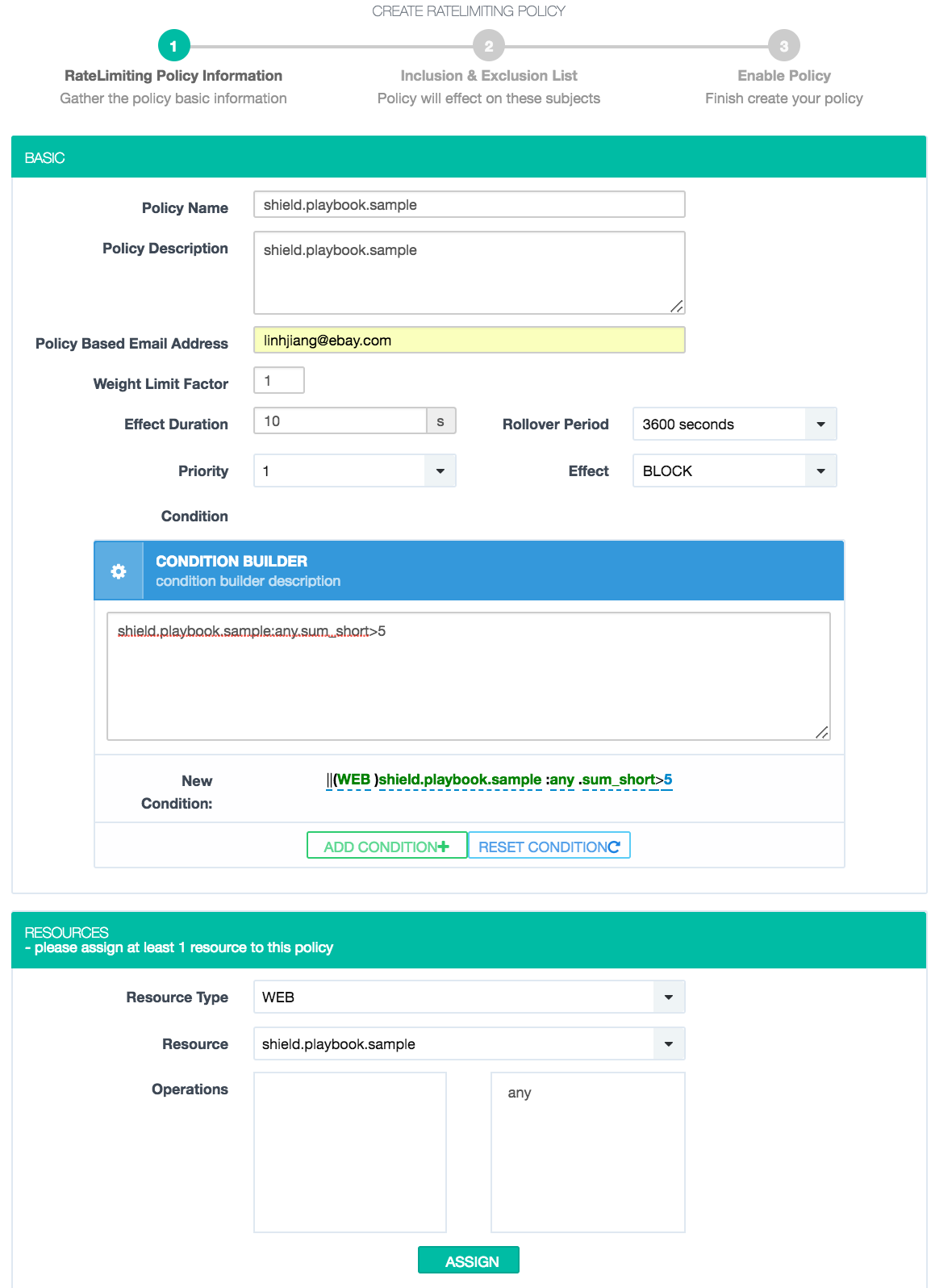
Before creating your policy, you should have resource available in SMC console. You can create your resources by accessing <http://soteriafe-1538520.phx02.dev.ebayc3.com:8080/resource/add>. Then you will see the page same with below:



For Resource Type - RESTFUL SERVICE, GET/PUT/POST/DELETE are available operation names.

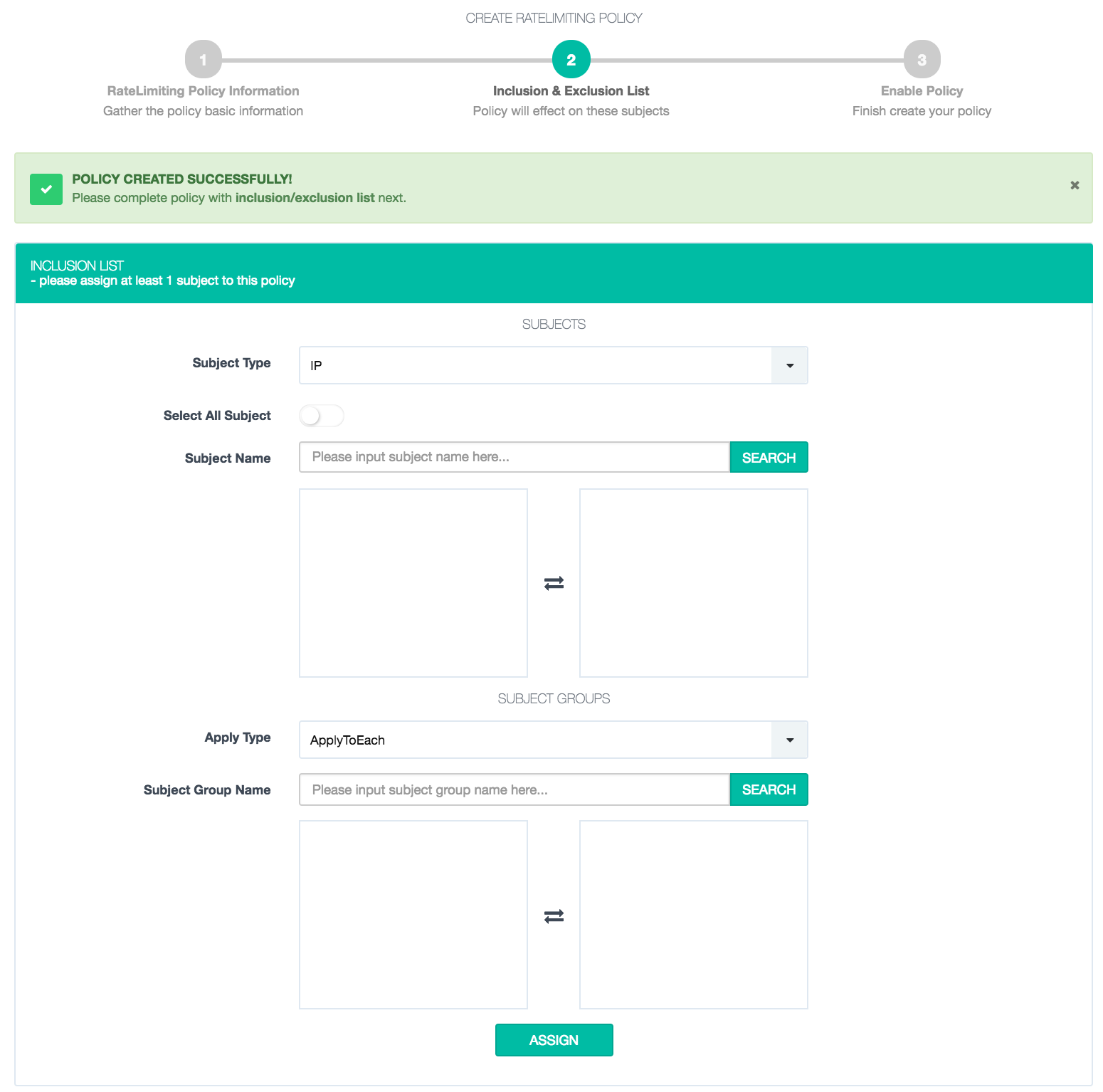
For Resource Type - WEB, you should always use operation name - “any”.

## Create RateLimiter Policy

You can create your policy by accessing to <http://soteriafe-1538520.phx02.dev.ebayc3.com:8080/policy/add/rl>. 

You can refer to the [Terminology](#_bn57z7fmrbvo) to fill above form. Condition builder would be helpful for you to configure the policy threshold.

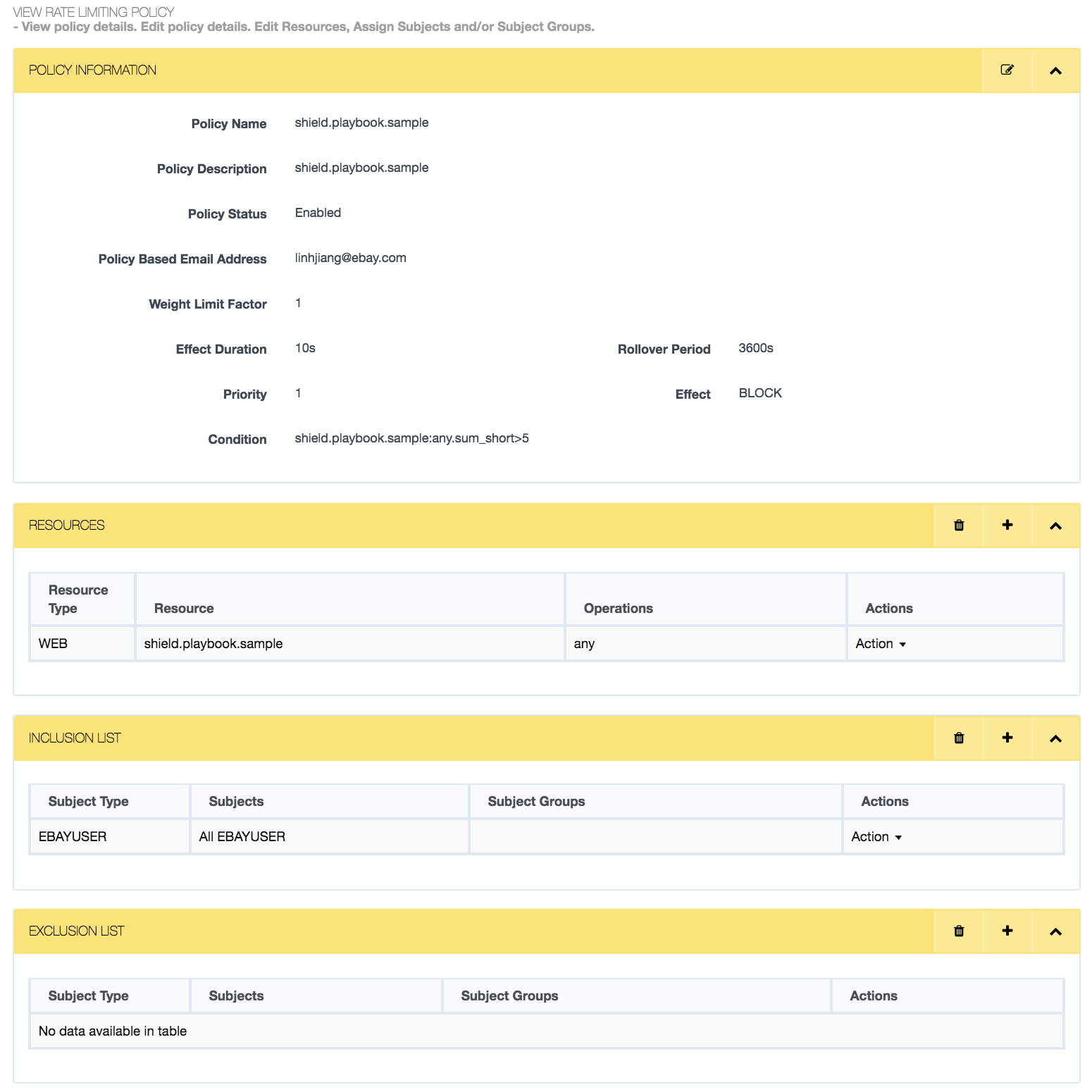
Next, assign subject to inclusion/exclusion list. Subjects in exclusion list will be ignored for this policy, while subjects in inclusion list will be counted.



Choose subject type, and input specific subject name or toggle button “Select All Subject”. There are two values of Apply Type - ApplyToEach and ApplyToAll. They take effect when subject group is specified. ApplyToEach means all subjects in subject group will be counted separatly, while ApplyToAll means subject in group will share the threshold together.

After assign subjects to your policy, you can enable your policy to make it work.

Here is a sample RateLimiter policy and interpretation.



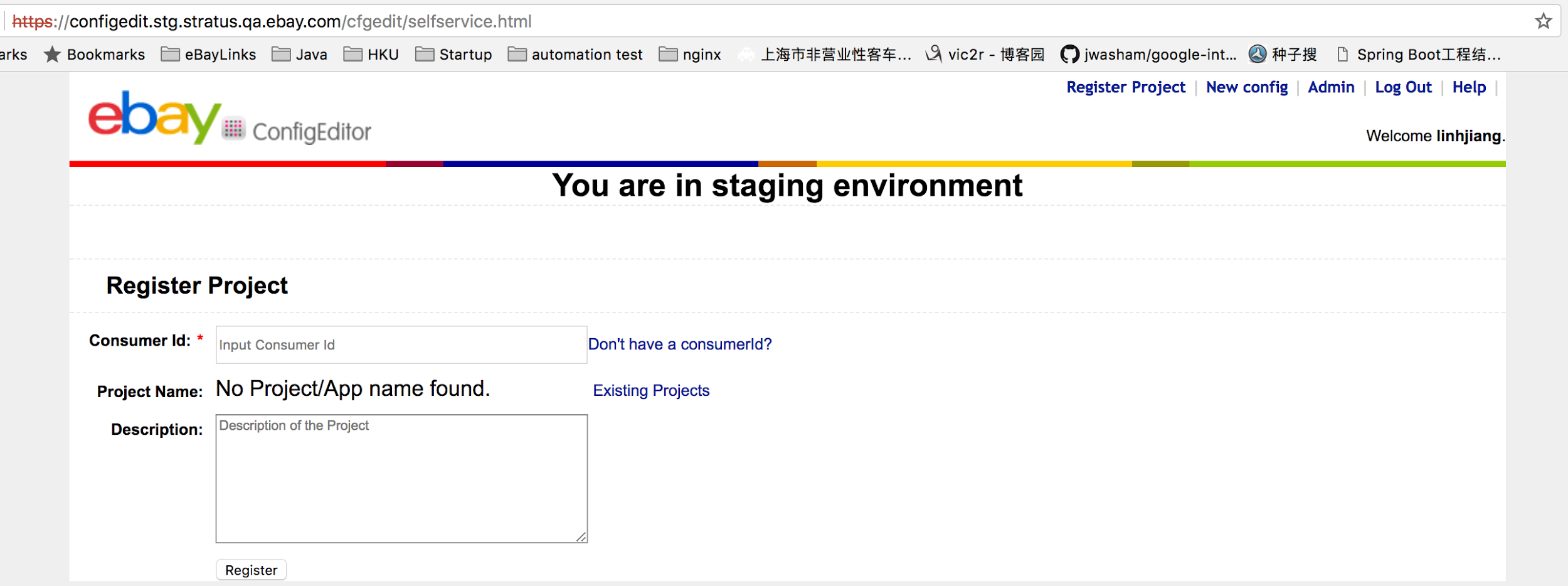
For every access of the resource "shield.playbook.sample", the counters sum\_short and sum\_long get incremented. For the first 5 access calls, “SERVE\_OK” is returned in the response. Once the threshold of 5 is met, the configured Effect "Block " is returned The Condition implies that "any" Operation on the resource "shield.playbook.sample" done more than 5 times within 15 sec (sum\_short=3600s/240) would trigger an Alert and it would stay in the cache for the next 10 seconds and return the Effect "Block" to the user. Once 10 sec period is elapsed further requests get “SERVE\_OK” unless the threshold is met again.

## Setup config in ConfigEditor

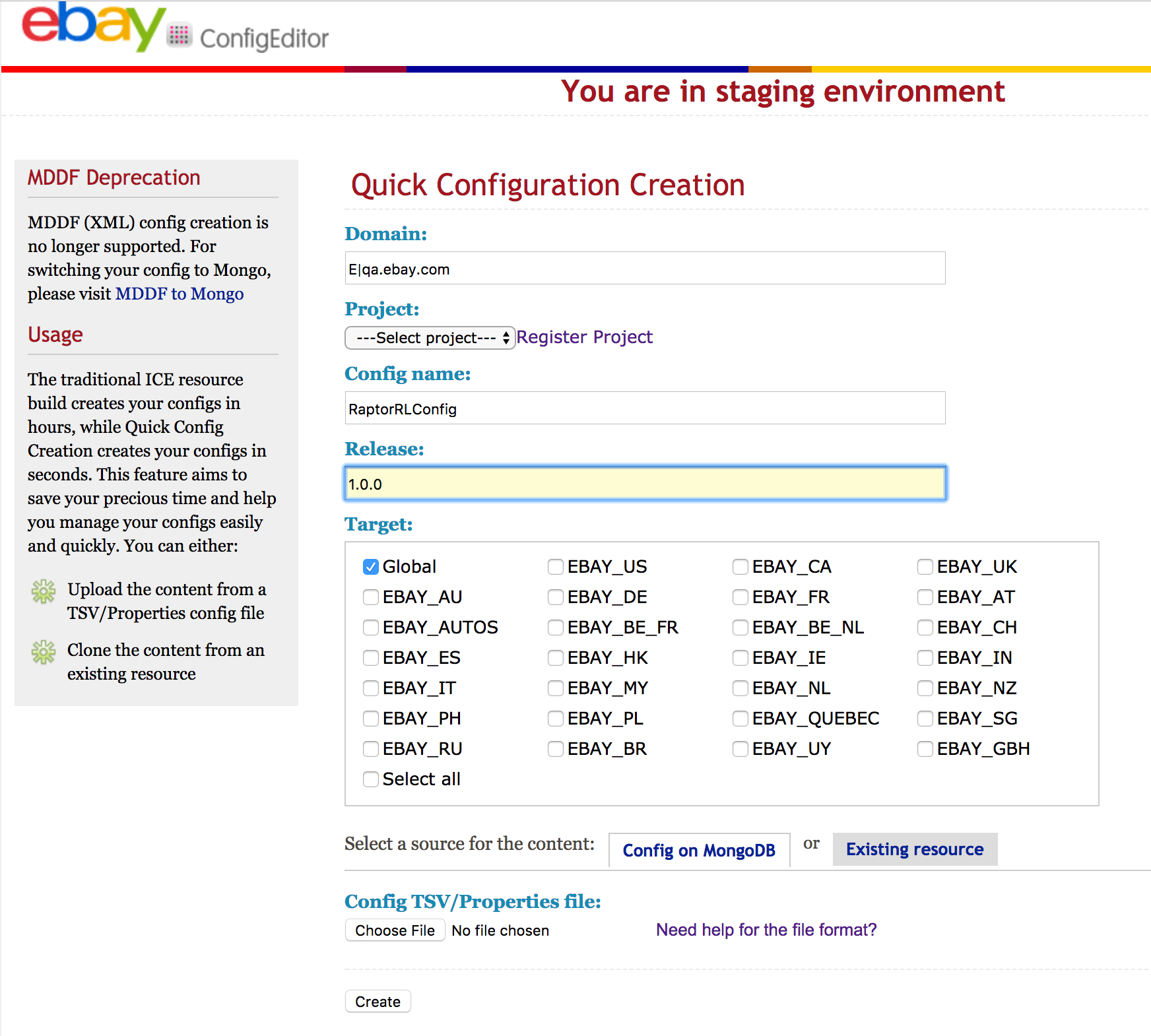
ConfigEditor of staging: <https://configedit.stg.stratus.qa.ebay.com/cfgedit/login.html>

ConfigEditor of prodution: <https://www.cfgedit.stratus.ebay.com/cfgedit/login.html>

1. Register your application If it is not registered in configEditor. You can find consumer id of your application in Altus/InfoHub.Fill it in below form and click register.



2. Create config - **RaptorRLConfig** for your application if haven’t.



Domain: E|qa.ebay.com (default value, no need to change it)

Project: the application you just registered at 1st step.

Config name: RaptorRLConfig

Release: 1.0.0

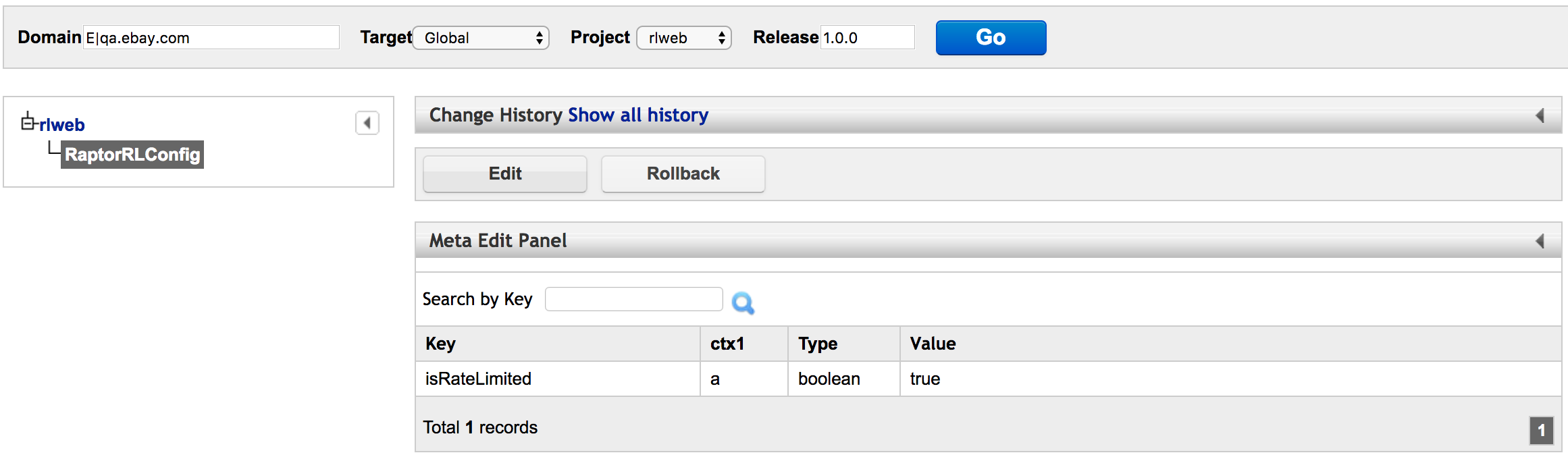
Target: Global

Config TSV/Properties file: [sample tsv file](https://wiki.vip.corp.ebay.com/pages/viewpage.action?pageId=417890318&preview=%2F417890318%2F435565290%2FRaptorRLConfig.tsv)

Click “Create” button after fill in all these information to finish create your application config.

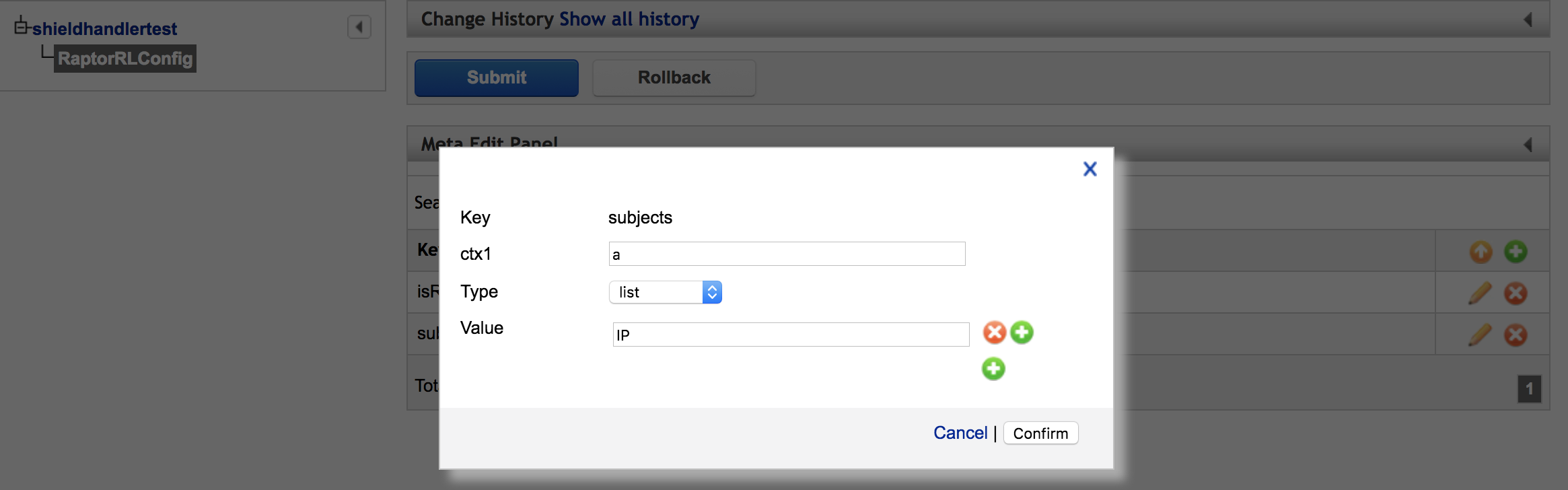
3. Add config key - **isRateLimited** to config, if haven’t. If you use sample tsc file provided by us, you will find config key is already added.

Here is sample Raptor config to enable the Shield.



4. Specify subject types you want to limit traffic (**Optional**)

Add config key - subjects, and list subjects in this config, like below:



If without this config, ShieldHandler will only extract IP from the context and send to Shield Service for Raptor Web.

## Sample Project Github

<https://github.corp.ebay.com/linhjiang/rlweb>

# Special Cases

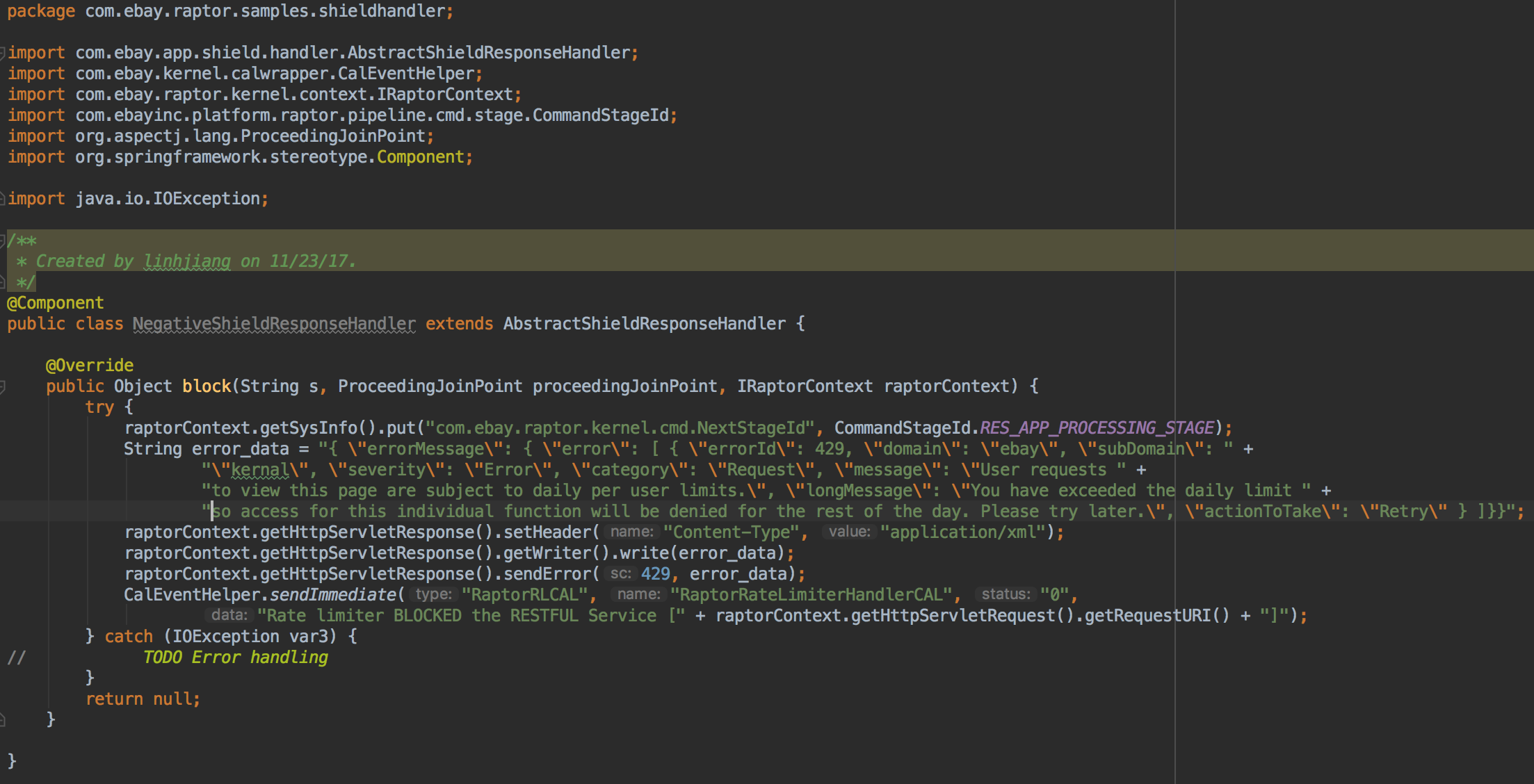
## Mix use of SpringMVC & Ginger in one application

In some situation, developer may use both Ginger & SpringMVC in one application, Ginger for service and SpringMVC for page view. For this case, the resource type would not be same. Resources of Ginger will be recognized as RESTFUL\_SERVICE, while Resources of SpringMVC will be regarded as WEB.

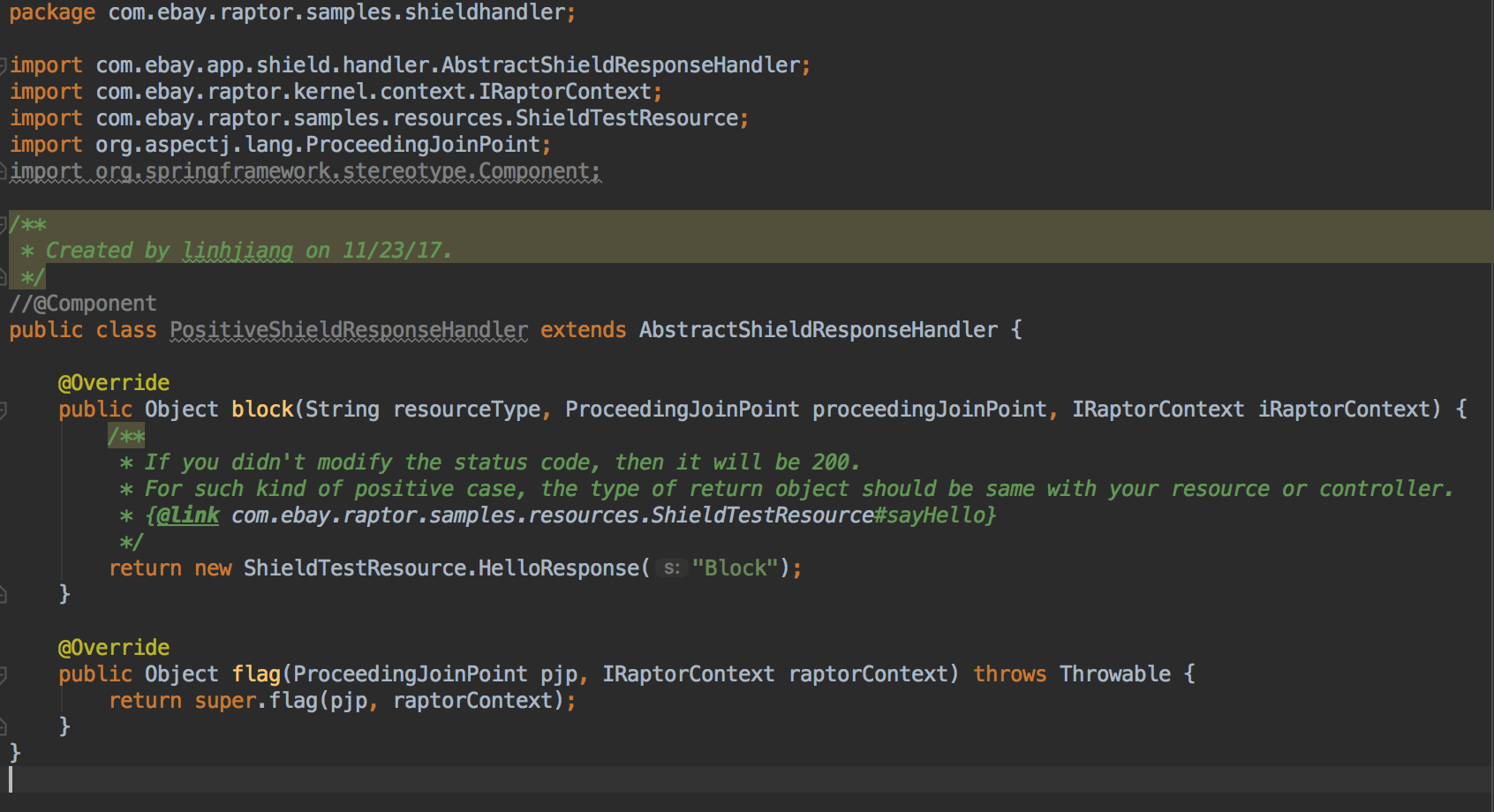
## Register customized handler to deal with BLOCK|FLAG

Create a new java class which inherits com.ebay.app.shield.handler.AbstractShieldResponseHandler and register this class into Spring application context, either by xml or @Component annotation.

Here is a negative case to return non-200 status code with error message:



You can also use status code 200 and return the original biz object:



If you use annotation way, don’t forget add the package of your class for auto scanning, like:

<context:component-scan base-package="com.ebay.raptor.samples.shieldhandler" />

This feature is available in ***ShieldHandler 1.0.6-SNAPSHOT*** or higher version.

Only **one** AbstractShieldResponseHandler should be registered, if multiple handlers are registered, *org.springframework.beans.factory.NoUniqueBeanDefinitionException* will be thrown.

Make sure the request to your service specifies the header - **Accept**, or it will redirect to error page when return non-200 status code.

Please see samples here - <https://github.corp.ebay.com/linhjiang/shieldhandlertest/tree/customize-handler-ex/shieldhandlertestService/src/main/java/com/ebay/raptor/samples/shieldhandler>

# Contact us

JIRA: <https://jirap.corp.ebay.com/browse/RL>

Team DL: [DL-eBay-Ratelimiter@ebay.com](mailto:DL-eBay-Ratelimiter@ebay.com)

Slack: <https://ebay-eng.slack.com/messages/C6911BGF8>

# FAQ

**How to onboard Shield to SOA application?**

Please see <https://docs.google.com/document/d/1Lud_P45FQvrDZc_nrWMY9Vn-WdLTjNq5vbD73nePCqA/edit#>

**How to enable/disable Shield per box?**

We provide the capability to turn on/off Shield for box level. You can go the VI page [http://{host:port}/admin/v3console/UpdateConfigCategoryXml?id=com.ebay.app.shield.handler.ShieldVIConfig](about:blank) and change the value of **shieldSwitch**. The default value is **INHERITED**, that means the value will be inherited from Raptor Config. The alternative values are **ON** & **OFF**.

If above link is not accessible, please visit your ratelimiter resource first.