

Lab - Connecting to a Secure Backend

Wherein ...

- We modify our APIEaternity Proxy to point to a different back end, and
- Find out we are required to Authentication to the new back end, and
- Provide sufficient credentials to exercise access

Modify the backend target

- In the Target Endpoint | HttpConnection change from:
<http://baas-ug000sr.apigee.net/apigee-training/sandbox/ratings>
- to:
<https://apigee-edu-prod.apigee.net/v1/apieatery>
- Test again with the /chefs resource to:
<http://<your-orgname>-test.apigee.net/v1/apieatery-<yr-intls>/chefs>
 - You should get a "401" Error. Why?

Modify proxy to connect to a Basic Authenticated backend

- **Step One:** Create KVM
- **Step Two:** Access KVM
- **Step Three:** Build Authorization Header
- **Step Four:** Test your code

Create a Key Value Map

The screenshot shows the 'Environment Configuration' page for an environment named 'test'. The 'Key Value Maps' tab is selected. A table lists the maps, with 'unpw' expanded to show two entries: 'username' with value 'foundationUser' and 'password' with value 'Test1234'. Red callout boxes highlight the 'test' environment name, the 'Key Value Maps' tab, the 'unpw' map name, and the 'your map name' placeholder.

ADMIN

Manage roles, environments, and access to your organization.

Users

Roles

Environments

Audit Logs

Environment Configuration **test**

Caches Flow Hooks **Key Value Maps** Target Servers Virtual Hosts TLS Key Pairs

+ Key Value Map

test

NAME ACTION

▼ unpw Delete

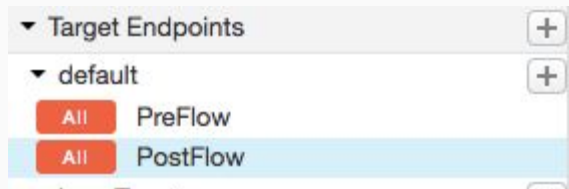
KEY	VALUE	ACTIONS
username	foundationUser	Edit Delete
password	Test1234	Edit Delete
		+ Entry

your "map name"

Click on +Key Value Map, Expand then click on +Entry.
Add 2 entries "username", "password"

Add a KVM policy

- back in the proxy, in the Develop tab
- select the default Target Endpoint / PostFlow



- click on the '+ Step' on the request flow



KVM Policy Configuration Options

- Find KeyValueCollection Operations policy in list

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<KeyValueCollection async="false"
  mapIdentifier="unpw" continueOnError="false"
  enabled="true"
  name="Key-Value-Map-Operations-1">
  <DisplayName>Key Value Map
Operations-1</DisplayName>
  <Properties/>
  <ExclusiveCache>false</ExclusiveCache>
  <ExpiryTimeInSecs>-1</ExpiryTimeInSecs>
  <Get assignTo="private.username" index="1">
    <Key><Parameter>username</Parameter></Key>
  </Get>
  <Get assignTo="private.password" index="1">
    <Key><Parameter>password</Parameter></Key>
  </Get>
  <Scope>environment</Scope>
</KeyValueCollection>
```

KVM Policy

Add Step

Policy Instance

New

Existing



Generate SAML Assertion



Validate SAML Assertion

MEDIATION



JSON to XML



XML to JSON



Raise Fault



XSL Transform



SOAP Message Validation



Assign Message



Extract Variables



Access Entity



Key Value Map Operations

KVM Policy Configuration Options

- **ExpiryTimeInSecs** - This setting is used to expire the cache not the entry
- **InitialEntries** - Allows you to pre-define values
 - We prebuilt our initial entries
- **Multiple Values** - KVM supports multiple values per name, you can access values using the index attribute of the Get tag

Create Basic Authentication Policy

- Same flow, click on Add Step ["+"] button; Find Basic Authentication policy in list
 - Can Encode two variables into a basic Authorization header
 - Can Decode a basic Authorization header into two variables

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BasicAuthentication async="false" continueOnError="false"
enabled="true" name="Basic-Authentication-1">
  <DisplayName>Basic Authentication-1</DisplayName>
  <Operation>Encode</Operation>
  <IgnoreUnresolvedVariables>false</IgnoreUnresolvedVariables>
  <User ref="private.username"/>
  <Password ref="private.password"/>
  <AssignTo
createNew="true">request.header.Authorization</AssignTo>
  <Source>request.header.Authorization</Source>
</BasicAuthentication>
```

Add Step

Policy Instance

New

Existing

SECURITY

- Basic Authentication
- XML Threat Protection
- JSON Threat Protection
- Regular Expression Protection
- OAuth v2.0
- Get OAuth v2.0 Info
- Set OAuth v2.0 Info
- Delete OAuth v2.0 Info
- OAuth v1.0a
- Get OAuth v1.0a Info
- Delete OAuth v1.0 Info
- Verify API Key

Basic Auth Policy

Test your proxy

- Test again with the /chefs resource to:

<http://<your-orgname>-test.apigee.net/v1/apieatery-<yr-intls>/chefs>

THANK YOU