apigee

Aug, 2015

Create and Manage APIs

Connectivity and Resource Management

Building Target Authentication

- Problem Statement

While attempting to make a request to a target through Apigee I am asked for basic authentication credentials.

- Basic Authentication

  - Base 64 Encrypted Username and Password (username:password)

- Where do I store the username in password?

  - Hard Coded in a policy

  - Build time properties replacement

  - Key Value Map

The Key Value Map Authentication Solution

- Step 1: Seed your map with credentials

- Step 2: Attach a keyvaluemap policy to retrieve said credentials

- Step 3: Attach a Basic Authentication Policy to put them in your Authentication header
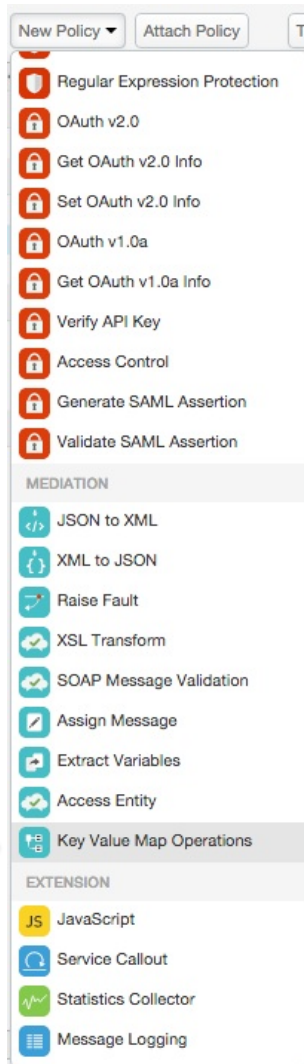
Step 1: Seeding your map with Curl:

```
curl "https://api.enterprise.apigee.com/v1/o/{organization}/keyvaluemaps" -H "Content-Type:application/json" -u {username} -d @credsKVM.json -v
```

credsKVM.json

```
{
  "name":"credentials",
  "entry":[
    {
      "name":"username",
      "value":"usernameForTarget"
    }, {
      "name":"password",
      "value":"passwordForTarget"
    }
  ]
}
```

The KVM Auth Solution Part 2

Attach KVM Policy

Name and Select the Target Endpoint (Preflow) from the flows, then press Add

New Policy ▾ | Attach Policy

- Regular Expression Protection
- OAuth v2.0
- Get OAuth v2.0 Info
- Set OAuth v2.0 Info
- OAuth v1.0a
- Get OAuth v1.0a Info
- Verify API Key
- Access Control
- 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**

EXTENSION

- JavaScript
- Service Callout
- Statistics Collector
- Message Logging

New Policy: 🔳 Key Value Map Operations   ✕

Policy Display Name   kvm_get_credentials

Policy Name   kvm_get_credentials

Attach Policy   ☑

Flow   Flow PreFlow, Target Endpoint default ⇕

Segment   ◉ Request   ○ Response

                                    Cancel   **Add**

Modify the content to retrieve the credentials

```
Code: kvm_get_credentials
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <KeyValueMapOperations name="kvm_get_credentials" mapIdentifier="credentials">
3      <DisplayName>kvm_get_credentials</DisplayName>
4      <ExpiryTimeInSecs>-1</ExpiryTimeInSecs>
5      <Get assignTo="username" index="1">
6          <Key>
7              <Parameter>username</Parameter>
8          </Key>
9      </Get>
10     <Get assignTo="password" index="1">
11         <Key>
12             <Parameter>password</Parameter>
13         </Key>
14     </Get>
15     <Scope>organization</Scope>
16 </KeyValueMapOperations>
```

KVM Options

- **Attributes**

  - mapIdentifier – References a defined kvm

- **Elements**

  - Scope – Where and when you can access data contained within the Map

  - ExpiryTimeInSecs – Specifies when the data will expire (note -1 = no expiration)

  - Initial Entries – Allows you to pre-load data on the first run of the policy

  - Put – Allows you to add data to the map dynamically (Warning: adding too much data can cause system degradation)

  - Get – Allows you to get data from the map

  - Delete – Allows you to remove data from the map

  - For More Help: http://apigee.com/docs/api-services/content/key-value-map-operations-policy

Attach Basic Authentication Policy

Attach Basic Authentication Policy

Name and Select the Target Endpoint (Preflow) from the flows, then press Add

New Policy: Basic Authentication

Policy Display Name	basic_authentication
Policy Name	basic_authentication
Attach Policy	☑
Flow	Flow PreFlow, Target Endpoint default
Segment	◉ Request ○ Response

Cancel   Add

Modify the content to build the Authentication Header

```
Code: basic_authentication
1  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2  <BasicAuthentication name="basic_authentication">
3      <DisplayName>basic_authentication</DisplayName>
4      <Operation>Encode</Operation>
5      <IgnoreUnresolvedVariables>false</IgnoreUnresolvedVariables>
6      <User ref="username" />
7      <Password ref="password" />
8      <AssignTo createNew="false">request.header.Authorization</AssignTo>
9      <Source>request.header.Authorization</Source>
10 </BasicAuthentication>
```

Basic Authentication Options

- Outbound Configuration

  - Operation – Encode

  - User – Attr:ref = location of username in a variable

  - Password – Attr:ref= location of the password in a variable

  - AssignTo

    - Attr:createNew = true / false

    - Reference to the authentication location (commonly request.header.Authentication)

- Inbound Configuration

  - Operation – Decode

  - User – Attr:ref = location to put decoded username

  - Password – Attr:ref= location to put decoded password

  - Source – variable location where the policy will find the Base64 encoded variables (commonly request.header.Authentication)

Trace – Lets Validate With Trace

Day 1 – Lab 5 Basic KVM

- Build KVM to Store credentials for target server

  - Create Key-Value-Map at the environment level using **POSTMAN**

    - POST https://api.enterprise.apigee.com/v1/o/orgName/keyvaluemaps/

    - Post data:

      <KeyValueMap name="credentials">

        <Entry name="username">foundationUser</Entry>

        <Entry name="password">Test1234</Entry>

      </KeyValueMap>

    - Create Key-value-map policy in preflow of default Target Endpoint to retrieve username and password

    - Create BasicAuthentication Policy to build Authorization header with base64 encription of userid / password

    - Test using Postman and start the Trace in Apigee to check flow variables.

Thank you

apigee

March 2014