

**Appendix 4 - Apigee Edge Microgateway**

Apigee Edge Microgateway is a secure, HTTP-based message processor for APIs. Its main job is to process requests and responses to and from backend services securely while asynchronously pushing valuable API execution data/meta data to and from Apigee Edge.

Typically, Edge Microgateway is installed within a trusted network in close proximity to backend target services; often, the μ-gateway will be co-located on the same OS image as the target service. μGwy provides enterprise-grade security, and some key plugin features such as spike arrest, quotas, and so on. The μ-gateway leverages an Apigee Edge Public Cloud instance, or an Apigee Edge private cloud (on premises) installation for other aspects of API Management like analytics, and developer management. You can install Edge Microgateway in the same data center or even on the same machine as your backend services.

_edge_micro_architecture.png

### Key features and benefits

* **Traffic management:** APIs proxied through Edge Microgateway never need to leave the perimeter of your corporate network. You get the Analytics and security capabilities of Apigee Edge public cloud, without sending your transaction data over public networks.
* **Security:** Edge Microgateway authenticates requests with a signed bearer token or API key issued to each client app by Apigee Edge. This means you can secure your internal-to-internal APIs without writing new server-side code.
* **Rapid deployment:** Unlike a full deployment of Apigee Edge, you can deploy and run an instance of Edge Microgateway within a matter of minutes.
* **Network proximity:** You can install and manage Edge Microgateway in the same machine, subnet, or data center as the backend target APIs with which Edge Microgateway interacts. Same-machine proxy deployment means that proxied traffic does not incur additional network capacity, and does not require an additional VM. Super low footprint.
* **Analytics:** Edge Microgateway asynchronously delivers API execution data to Apigee Edge, where it is processed by the Edge Analytics system. You can use the full suite of Edge Analytics metrics, dashboards, and APIs.
* **Reduced latency:** All proxy activity is done on the local datacenter network, meaning the overhead of the proxy is very very low. All communication with Apigee Edge is asynchronous and does not happen as part of the client request pipeline. This allows Edge Microgateway to collect API data and send it to Apigee Edge without affecting latency of the runtime transactions.

## Objectives

In this lab you will go through configuring, get working Edge Microgateway installation capable of processing an API. You'll make several secure, test API calls through Edge Microgateway to the API's backend service and see how Apigee Edge processes analytics data from Edge Microgateway.

## Prerequisites

*   Edge Micro ZIP File is downloaded to local folder. download from [here](https://s3.amazonaws.com/apigee-sdks/edgemicrogateway/latest/apigee-edge-micro.zip)
*   Node 4.2.2 or later is installed

node -v v4.2.2

*   Have access to Edge Org
*  Have openssl installed and is in path
*  curl

## Estimated Time: 60 mins

### Configure Edge Micro

* Unzip the file unzip apigee-edge-micro-1.1.0.zip
* Go to the bin folder cd apigee-edge-micro-1.1.0/cli/bin
* Test the installation by executing the following command. If it returns CLI help output, then the installation was successful.

Linux/Mac: ./edgemicro -h

Windows: node edgemicro –h

Usage: edgemicro [options] [command]

Commands:

agent <action> agent commands, see: "edgemicro agent -h"

cert <action> certificate commands, see: "edgemicro cert -h"

token <action> token commands, see: "edgemicro token -h"

private <action> private commands, see: "edgemicro private -h"

configure [options] automated, one-time setup for a new edgemicro instance

deploy-edge-service [options] deploy edge micro support server to Apigee

genkeys [options] generate authentication keys

verify [options] verify Edge Micro configuration by testing config endpoints

help [cmd] display help for [cmd]

Options:

-h, --help output usage information

* Put the cli/bin directory in your PATH variable. This way, you'll be able to execute Edge Microgateway commands from anywhere.

Linux/Mac Only:

export PATH=<Edge\_Micro\_Gateway\_Installaton\_Folder>/cli/bin:$PATH echo $PATH

* Configure the micro gateway to talk to the Edge deployment on public/private cloud

Linux/Mac: ./edgemicro configure -o <org-name> -e <env-name> -u <your Apigee email>

Windows: node edgemicro configure -o <org-name> -e <env-name> -u <your Apigee email>

checking for previously deployed proxies

preparing edgemicro-auth app to be deployed to your Edge instance

Give me a minute or two... this can take a while...

App edgemicro-auth added to your org. Now adding resources.

App edgemicro-auth deployed.

checking org for existing vault

vault already exists in your org

configuring host edgemicroservices-us-east-1.apigee.net for region us-east-1

updating agent configuration

vault info:

-----BEGIN CERTIFICATE-----

MIICpDCCAYwCCQDyRBB4weplRDANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQDEwls

b2NhbGhvc3QwHhcNMTUwODA1MTczODQxWhcNMTUwODA2MTczODQxWjAUMRIwEAYD

VQQDEwlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDt

Zv2nTCpTCrlkilQbT4yArCJ1vRNd4RWLzpuGGhofDO7Bk92tktqcEJALGnaDOnlb

FbeG473U/z19dpfgg+otZmf+z1ovEmT5mIx9Ktzj2Ykf32lnj94cD0vIY1W9DViP

pYit1AgwHKnDJZNio4EuxCno66jsrS3lzReEolQO55t1HH1Yzs9JdVev67wHAvf4

FbTeUeni0WBmFhp7XqYxXcM2WAe4EC6wHq1BlPjKuf+U+G55N/aJ7unPY5V2NP0L

l9n69EDbe29qe6zI/mP3MwYpHmwxKc+KPA4uI4E+4xZywWIt4v4tje5XQiLma0ht

LvxRRWadyuKf/q70SzUDAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAClXGNdjRsYi

HEhwh9TbaPMkF0A58NIi9S+QJgjE8eHQ/wX0AX5wov3A8OnSFkWJMxEJN5Y+d0bR

5lmOEQnudHEJu4JdH1bwzstgBRnZxkzqre48WjCM1G3RwYbqalePpAkhD44ro36i

SkTaQuQmgTQp3MchKNO/wVpoMvVdsX8gccZGU3pJXgxw97kCUY7kZYy8pI/3Gbcx

RCoQdM2tK7LCF4wrbf8PuPvX8UEaLF4FFkHDNtgvqCXn6L7Z5Hs3Y22AFFf9K3eq

sW8CccuDBYghmmo4Bn3LtKf97BpyQjW48FgBFZkhsbjiFKtfoyq+VS22Yu8HU4Kr

Nt/SqU1JKaU=

-----END CERTIFICATE-----

The following credentials are required to start edge micro

key: xxxxx

secret: xxxx

edgemicro configuration complete!

* **Copy the** Key, Secret and vault info, for later parts of the exercise.
* Using the key and secret you just viewed; verify that the edge micro is configured correctly with the Edge Cloud org.

./edgemicro verify -o <org-name> -e <env-name> -k <key> -s <secret>

You should see happy messages. If not, you'll need to stop, and diagnose.

### Start the Edge Micro agent

* Before continuing, open a separate terminal window. This is where the agent server will run.
* cd to the agent directory.  cd ../../agent
* Execute this command to start the server:  npm start  You will see an output from that command:

> edgemicro-agent@1.1.1 start C:\Users\nanda\Documents\apigee-edge-micro-1.1.1\agent

> node build/src/index.js

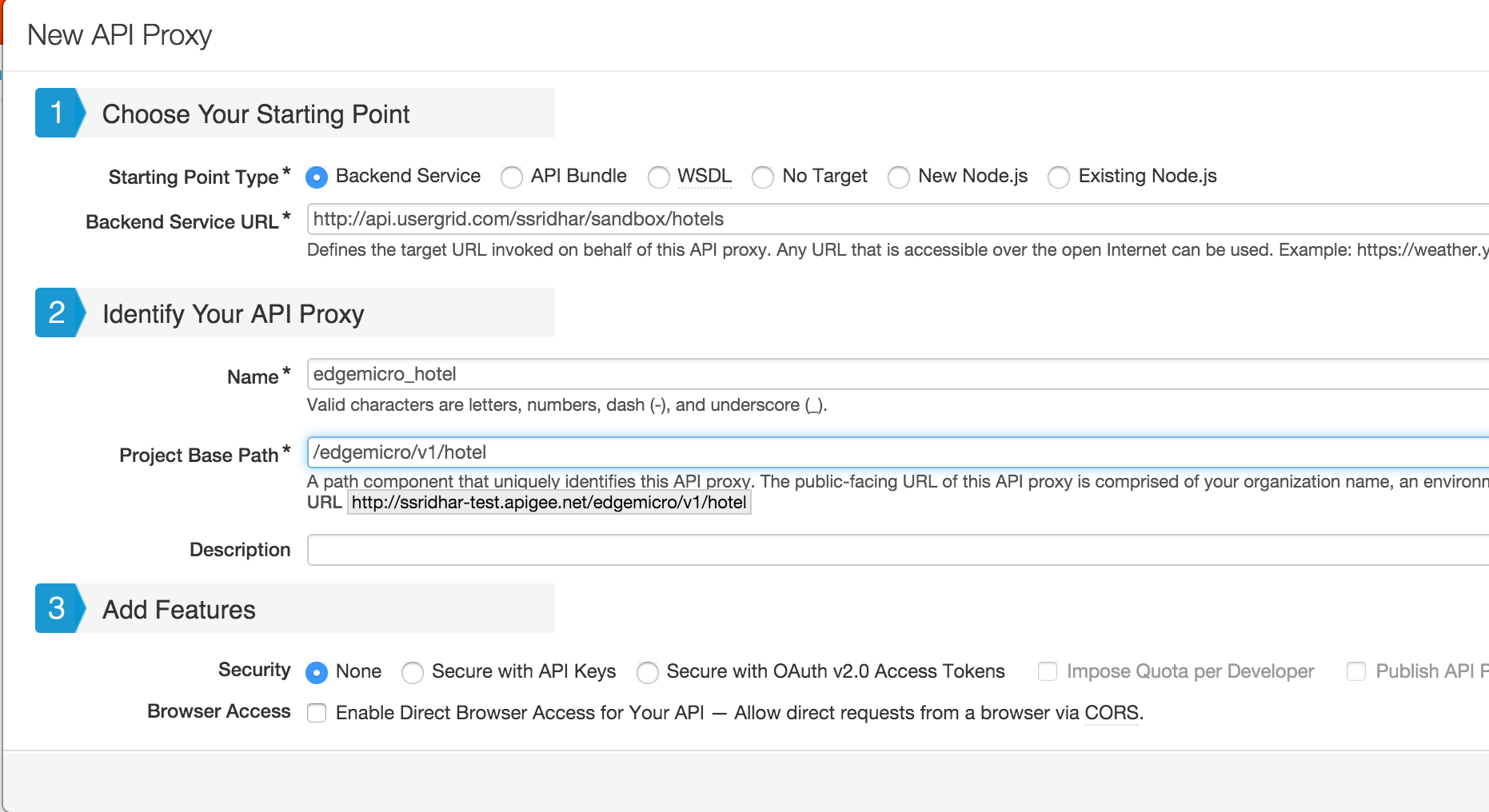
i edge micro agent listening on 9000

The configuration done so far allows Edge Microgateway to bootstrap itself to Apigee Edge. The Edge Microgateway agent manages this bootstrapping process, which kicks off whenever you start or restart Edge Microgateway. After the bootstrapping succeeds, Edge Microgateway retrieves a payload of additional configuration information from Apigee Edge.

### Create a passthrough API Proxy

Log in to your organization on Apigee Edge.

* Select APIs > API Proxies from the top menu.
* In the API Proxies page, click + API Proxy.
* In the dialog, configure the proxy as follows: _api_create.png
  + Starting Point Type: **Backend Service**
  + Backend Service URL: http://api.usergrid.com/{org-name}/sandbox/hotels
  + Name: edgemicro\_{your\_initials}\_hotels
  + Project Base Path: /{your-initials}/v1/mghotels
  + Description: Edge Micro Proxy that will run locally to the node.js service
  + Features: None



**Note:** Edge μ-gateway-aware proxy names must always begin with the prefix **edgemicro\_**.

* Click on Build to build and deploy the proxy
* Once the proxy has been deployed, click on the Close button_update_target_endpoint.png
* Click on the Save button to save and deploy the changes to the hotels API Proxy
* We have created an API Proxy that will be fetched by Edge Micro gateway, when it starts locally
* Add the API Proxy you created edgemicro\_<your initials>\_mghotels to the API Product <your initials> Hospitality Basic Product
  + From the Apigee Edge Management UI, go to Publish → API Products
  + Select the API Product: <your initials> Hospitality Basic Product
  + Click on Edit Button on the top right
  + Click on + API Proxy button and API Proxy edgemicro\_<your initials>\_mghotels _update_api_proxy.png

### Start Edge Microgateway

* Open a new terminal window (not the one where the agent is running) and print out help info for the agentproc command. We're going to use the -c, -k, and -s options to start Edge Microgateway.

Linux/Mac: ./edgemicro agent proc –h

Windows: node edgemicro agent proc -h

**Note:** The tutorial assumes that the cli/bin directory is in your PATH. If you do not put it in your PATH, then you need to execute CLI commands from the cli/bin directory (cd ../cli/bin and run ./edgemicro agent proc -h).

* Start Edge Microgateway by executing the following command, providing the key and secret values with the -k and -s parameters, respectively.

Linux/Mac: ./edgemicro agent proc -c start -k <key> -s <secret>

Windows: node edgemicro agent proc –c start –k <key> -s <secret>

* If the micro gateway is started successfully, you will see something like the following console output:

{ "pid": 9104, "uid": "MTQ0NzQ1MjU4Nzk0MQ", "running": "true", "restarts": 0, "since": "2015-11-13T22: 09: 47.959Z" }

**Note:** The **UID** is the unique id for this instance of Edge Microgateway. You use this ID when retrieving log and monitoring information about Edge Microgateway. See the *Edge Microgateway Administrator*'s Guide for more information.

**Agent output:** In the terminal where the agent is running, you'll see output like this. You may have to scroll up through the terminal output to see some of the messages.

info: config download from https://edgemicroservices-us-east-1.apigee.net/edgemicro/bootstrap/organization/amer-partner1/environment/test returned 200 OK info: products download from https://amer-partner1-test.apigee.net/edgemicro-auth/products returned 200 OK info: jwt\_public\_key download from https://amer-partner1-test.apigee.net/edgemicro-auth/publicKey returned 200 OK warning: no edge micro proxies found in org warning: no products found in org downloaded jwt\_public\_key '\*\*\*\*\*' installed plugin from /Users/SandeepM/Apigee/Products/EdgeMicro/apigee-edge-micro-1.1.0/plugins/analytics installed plugin from /Users/SandeepM/Apigee/Products/EdgeMicro/apigee-edge-micro-1.1.0/plugins/oauth MTQ0NzQ0NjgwNzkxOQ edge micro listening on port 8000

At this point, the agent retrieves a payload of Edge Microgateway configuration information from Apigee Edge. This information includes:

* +   The public key we created and stored previously in the Apigee vault.
  +   A JSON representation of all Edge Microgatewayaware proxies that exist in the organization/environment. These are all proxies that are named with the prefix edgemicro\_.
  +   A JSON representation of all of the API products that exist in the organization.

With this information, Edge Microgateway knows which proxies and proxy paths are allowed. If/when configured, it uses the product information to enforce security (in the same way as any API proxy does on Apigee Edge, where developer app keys have an association with products). We'll go through the steps to secure Edge Microgateway shortly.

* To test our API Proxy, call the

curl -i http://localhost:8000//{your-initials}/v1/mghotels

* If you will see an authorization error, your Micro Gateway is listening for the API you have configured in the previous step

{"error":"missing\_authorization","error\_description":"Missing Authorization header"}

* Run the following command to get the JWT Token

curl -i -X POST "http://<org name>-test.apigee.net/edgemicro-auth/token" \ -H "Content-Type:application/json" \ -d '{ "grant\_type": "client\_credentials", "client\_id":"...CLIENT\_ID\_HERE...", "client\_secret": "...CLIENT\_SECRET\_HERE..." }'

The response you see will have a very long string, looking something like so:

"eyJ0eXAiOiJKV1QiLc9.eyJhcHBsaWNhdGlvbl9u....kkBnE40jk\_2trmZkP6uf4-mcgUw91-qKofaw"

* Make the API Call with a bearer token you received in the step above

curl -i -H "Authorization:Bearer VERY\_LONG\_JWT\_TOKEN\_HERE" http://localhost:8000/{your-initials}/v1/weather/forecast?zipcode=95113

* You should see the response json:

|  |  |
| --- | --- |
|  | { |
|  | "action" : "get", |
|  | "application" : "5d4057c0-3ace-11e5-9fd6-0dff5edbe5ab", |
|  | "params" : { }, |
|  | "path" : "/hotels", |
|  | "uri" : "https://api.usergrid.com/ssridhar/sandbox/hotels", |
|  | "entities" : [ { |
|  | "uuid" : "7d20227a-5c82-11e5-a131-a7fee2bde904", |
|  | "type" : "hotel", |
|  | "name" : "MotifÃ‚ Seattle", |
|  | "created" : 1442415121943, |
|  | "modified" : 1442415121943, |
|  | "address1" : "1415 5th Ave", |
|  | "airportCode" : "SEA", |
|  | "amenityMask" : 7798786, |

……

You have used the credentials you received from your Edge org on cloud and you have used them on your local Micro Gateway. You are able to manage your APIs centrally, while the enforcement is happening locally.

## Summary

That completes this hands-on lesson. In this lesson you learned about setting up an Edge Micro Gateway, creating an API Proxy and corresponding life cycle on your Edge org. You now have a fully functioning and secure Edge Microgateway that can run your APIs locally, picking up the security credentials from your Edge org.