SEC eDGE™
Digital Security to the Edge

SECeDGE STUDIO™

Tutorial

May 7 2024 | Version 1.2

1. TABLE OF CONTENTS

2. SECeDGE STUDIO™ OVERVIEW

SecEdge Studio is a development and test environment for SecEdge's chip-to-cloud security solution, available on Google Marketplace. SecEdge studio accelerates the integration and deployment of the SecEdge Service Platform, which provides device-level security, zero-trust networking, and secure data control and management.

With SecEdge Studio, IoT and Edge solution developers can deploy their solutions in a cloud environment, connect backend applications, and emulate edge devices. More than 80% of an IoT security solution's development and test can be done in a virtual environment by a single software engineer. IPSEC Chip to Cloud Tunnels are automatically set up through SecEdge platform, enabling the configuration/policy/KMS and dashboard management.

This document guides you through two deployments to test end-to-end the following scenarios:

First deployment:

- Verify existence of MicroEdge and CloudEdge configuration
- Verification of MicroEdge and CloudEdge connectivity
- Execution of an application using the data tunnels

Second Deployment:

- Support of multi-tunnels
- Rotation of device keys on the MicroEdge device
- Rotation of MQTT certificates on the MicroEdge device
- Test routing table

Through the guide, steps are executed in GCS, SecEdge User Interface and in the shell of the CloudEdge and MicroEdge VMs.

Please see the SecEdge Studio Getting Started Guide for steps to set up the product. Please see the User Guide for overview of SecEdge Studio architecture and capabilities. Documentation for specific device hardware deployment is supplied upon request.

2.1. SECeDGE SERVICE PLATFORM

MicroEdge™ is a middleware component which provides zero-touch security provisioning, secure end-to-end data in motion and at rest for Internet of Things and Operational Technology embedded devices with Variscite SOM modules. Implementation examples include vending machines, automotive modules, IoT gateways, set-top boxes, smart locks, perimeter security, and smart city infrastructure. A single MicroEdge instance on a device enables multi-tunnel connectivity to different CloudEdge servers enabling more secure services and/or new monetization options for the owners of the IoT/Edge devices.

The MicroEdge software is installed on devices equipped with Linux OS.

CloudEdge™ is the cloud termination endpoint for MicroEdge device tunnels. Endpoint devices can be anchored to one or more peer endpoints on an external network, but residing on the same administrative span of control as the MicroEdge endpoint. This peer endpoint is referred to as the CloudEdge. All external network flows will be securely tunneled to CloudEdge where the flows can be subjected to additional security analysis before being routed to their ultimate destination.

Customers deploy one instance of CloudEdge in their backend to connect securely all IoT/Edge devices to their backend application server.

ControlEdge™ administers all edges (IoT devices equipped with MicroEdge and CloudEdge) within the SecEdge ecosystem. ControlEdge performs all the heavy lifting functions to set, configure and manage the security of the entire deployment. All this connectivity and provisioning is managed by ControlEdge services which allow for the deployment of IPsec tunnels facilitating secure communications between instances.

ControlEdge is available as a SecEdge managed service and is accessed by customers via simple APIs.

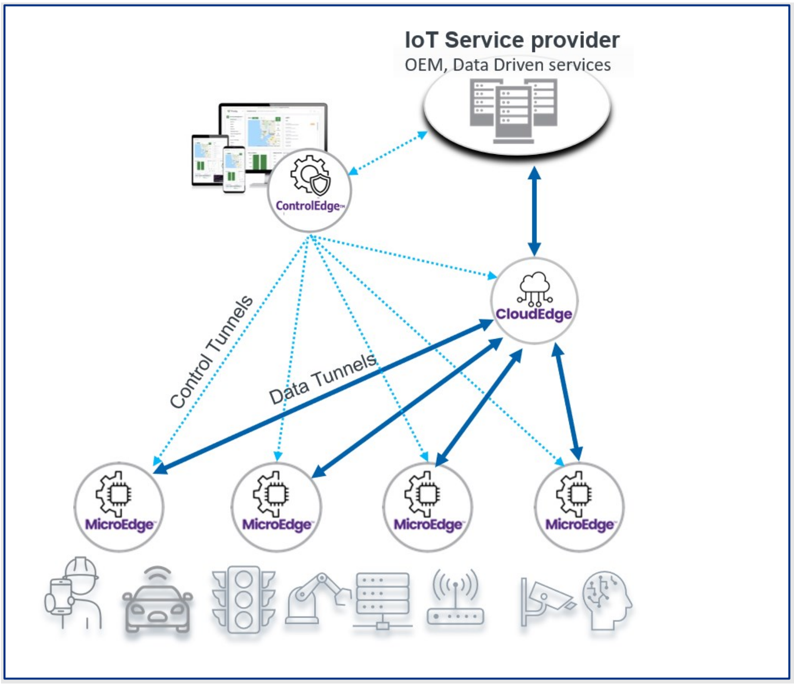


Figure 1 SecEdge Service Platform Architecture

2.2. PREREQUISITES TO USE SECeDGE STUDIO™

The following are requirements to use the SecEdge Studio:

- Google account to access Google Cloud services
- Login to Google Cloud Console, i.e. console.cloud.google.com
- The following roles assigned to the user accessing/deploying SecEdge Studio
    - Commerce Producer Viewer
    - Compute Instance Admin (v1)
    - Consumer Procurement Entitlement Manager
    - Deployment Manager Editor
    - IAP-secured Tunnel User
    - Service Account User
    - Service Management Administrator
- The following APIs enabled
    - Compute Engine API
    - Cloud Deployment Manager V2 API
    - Cloud Runtime Configuration API
- Familiarity with the following services in Google Cloud Console:
    - Compute Engine
    - VPC Network
    - Marketplace
- No hardware is required to use SecEdge Studio

3. SECeDGE STUDIO™ DEPLOYMENT TEST STEPS

This section guides you through the steps to start and test your project:

- Start with SecEdge Studio on Google Cloud Marketplace.
- Accept agreements
- Deploy SecEdge Studio VMs
- Manage MicroEdge and CloudEdge devices through SecEdge Studio User Interface.
- Customize and test with a guided example

3.1. START WITH SECeDGE STUDIO™ ON GOOGLE MARKETPLACE

The following steps get you started with SecEdge Studio on Google Cloud Marketplace:

1. Sign into your Google Cloud account.
2. Create a new Google Cloud project or use one of your existing Google Cloud projects.
3. Enable the following services for your Google Cloud project:
   - Cloud Runtime Configuration API

     https://console.cloud.google.com/apis/library/runtimeconfig.googleapis.com
   - Compute Engine, https://console.cloud.google.com/marketplace/product/google/compute.googleapis.com
   - Deployment Manager, https://console.cloud.google.com/marketplace/product/google/deploymentmanager.googleapis.com
4. Go to Marketplace section and search for **SecEdge** product.

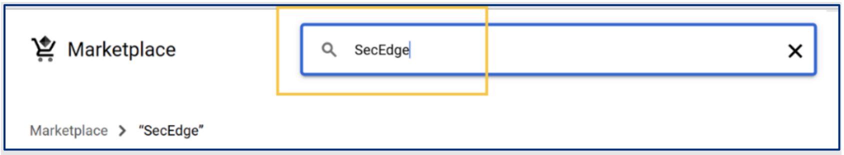


Figure 2 Marketplace Seach

5. Select **SecEdge Studio**.
6. The SecEdge Studio **Product details** page shows overview, pricing and support information, Figure 3.

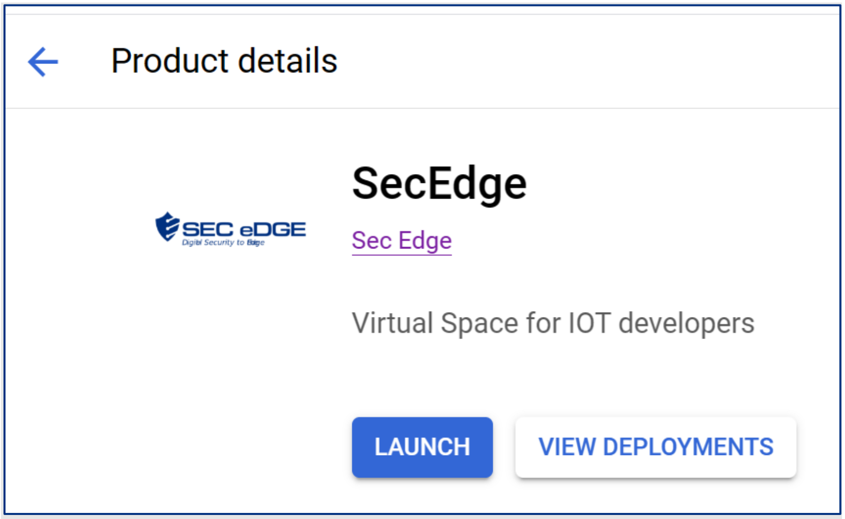


Figure 3 SecEdge Studio Product Details page

7. Click on GET STARTED to continue and access the **Agreements** page. If you already signed the agreements, click on LAUNCH and continue to the **New SecEdge Studio deployment** page.

3.2. ACCEPT PRODUCT AGREEMENTS AND TERMS OF SERVICE

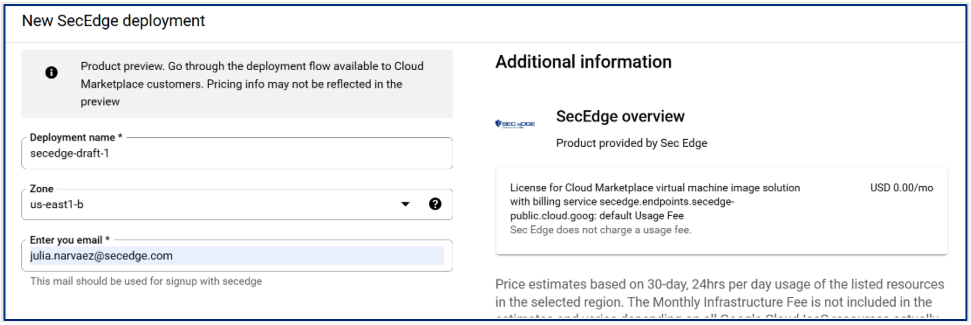
On the Google Cloud, accept agreements on the **Agreements** page, as instructed in the SecEdge Studio Getting Started Guide. After agreeing, you are redirected to the **New SecEdge Studio deployment** page to deploy your project.

4. DEPLOY FIRST SET OF SECeDGE STUDIO VMs

4.1. DEPLOY CLOUDEDGE AND MICROEDGE VMs

On the **New SecEdge Studio deployment** page, configure your deployment information and the MicroEdge and CloudEdge VMs, Figure 4, Figure 5 and Figure 6.

At the top, enter three inputs for your deployment: Deployment name, Zone, and Email.



New SecEdge deployment

Product preview. Go through the deployment flow available to Cloud Marketplace customers. Pricing info may not be reflected in the preview

Deployment name *
secedge-draft-1

Zone
us-east1-b

Enter you email *
julia.narvaez@secedge.com
This mail should be used for signup with secedge

Additional information

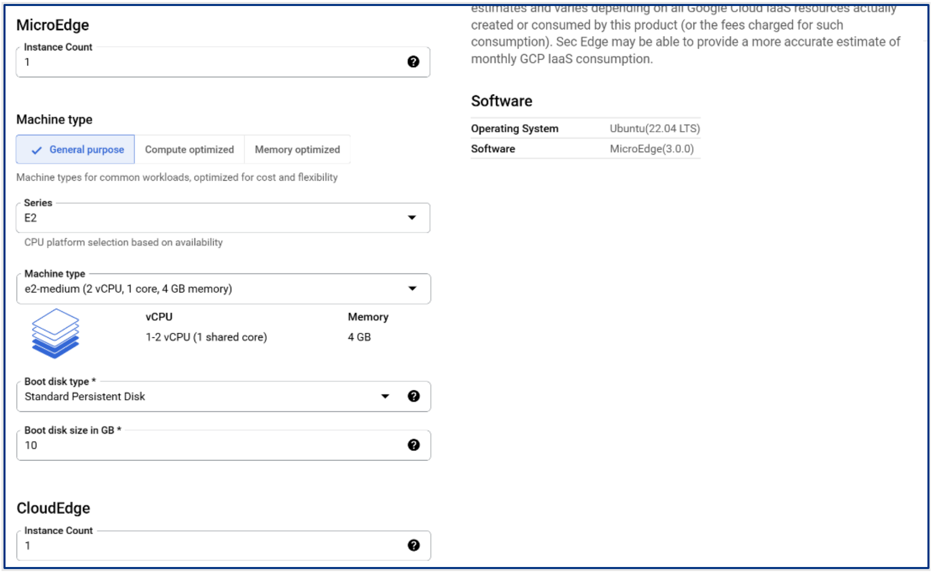
SecEdge overview
Product provided by Sec Edge

License for Cloud Marketplace virtual machine image solution with billing service secedge.endpoints.secedge-public.cloud.goog: default Usage Fee USD 0.00/mo
Sec Edge does not charge a usage fee.

Price estimates based on 30-day, 24hrs per day usage of the listed resources in the selected region. The Monthly Infrastructure Fee is not included in the

Figure 4 New SecEdge Studio Deployment Page

In the MicroEdge and CloudEdge sections, which configure the VMs, select the Series with minimum resources to save cost. Otherwise, there is no need for additional configuration.



estimates and varies depending on all Google Cloud IaaS resources actually created or consumed by this product (or the fees charged for such consumption). Sec Edge may be able to provide a more accurate estimate of monthly GCP IaaS consumption.

Software

Operating System	Ubuntu(22.04 LTS)
Software	MicroEdge(3.0.0)

MicroEdge

Instance Count: 1

Machine type

Machine types for common workloads, optimized for cost and flexibility

Series: E2

CPU platform selection based on availability

Machine type: e2-medium (2 vCPU, 1 core, 4 GB memory)

vCPU	Memory
1-2 vCPU (1 shared core)	4 GB

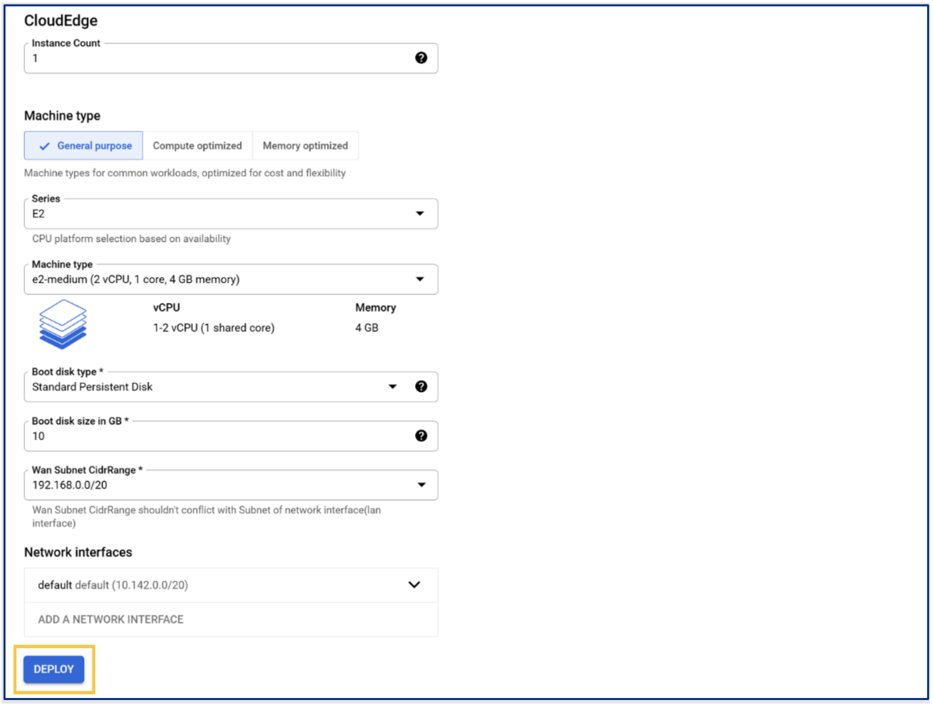
Boot disk type *: Standard Persistent Disk

Boot disk size in GB *: 10

CloudEdge

Instance Count: 1

Figure 5 New SecEdge Studio Deployment Page MicroEdge



CloudEdge

Instance Count: 1

Machine type

Machine types for common workloads, optimized for cost and flexibility

Series: E2

CPU platform selection based on availability

Machine type: e2-medium (2 vCPU, 1 core, 4 GB memory)

vCPU	Memory
1-2 vCPU (1 shared core)	4 GB

Boot disk type *: Standard Persistent Disk

Boot disk size in GB *: 10

Wan Subnet CidrRange *: 192.168.0.0/20

Wan Subnet CidrRange shouldn't conflict with Subnet of network interface(lan interface)

Network interfaces

default default (10.142.0.0/20)

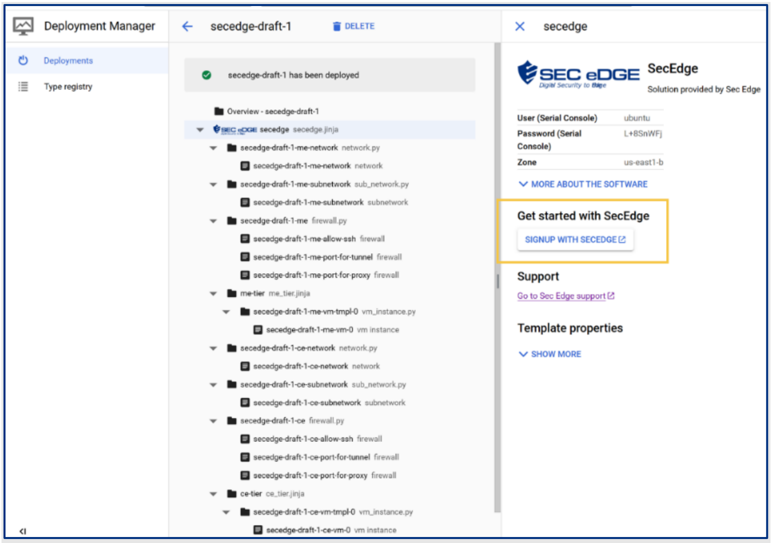
Figure 6 New SecEdge Studio Deployment Page CloudEdge

Click on DEPLOY. SecEdge Studio activates the CloudEdge and MicroEdge VMs and adds them to a default management group. Activation uses the following credentials:

- Day0 Device, an IoT/Edge device which is known to SecEdge Studio but not authenticated yet.
- Day1 Device, an IoT/Edge device which is authenticated and verified by SecEdge Studio (ControlEdge).

The deployment can take a few minutes while the following processes take place:

1. Device setting:
    - OS and MicroEdge installation in MicroEdge VM.
    - OS and CloudEdge Installation in CloudEdge VM.
    - Day0 credentials pre-installed in both VMs.
2. When the MicroEdge and CloudEdge VMs are spawned, they register themselves with ControlEdge using Day0 credentials.
    - This step is automated for SecEdge Studio customers.
3. After MicroEdge and CloudEdge are successfully registered, they receive Day1 credentials and reconnect with ControlEdge as Day1 devices.
4. ControlEdge provisions the Day1 MicroEdge and CloudEdge with secure tunnel configurations so that the MicroEdge and CloudEdge establish a secure tunnel between them.
5. On completion:
    - An email notification is sent to you, "Your SecEdge solution has been deployed on Google Cloud Platform".
    - The process redirects to the Google Cloud **Deployment Manager** for your new deployment, Figure 7.
    - On the **Deployment Manager** page, click on SIGNUP WITH SECeDGE, which redirects to the SecEdge Studio user interface where you can view and manage the connection between the VMs.



secedge-draft-1 has been deployed

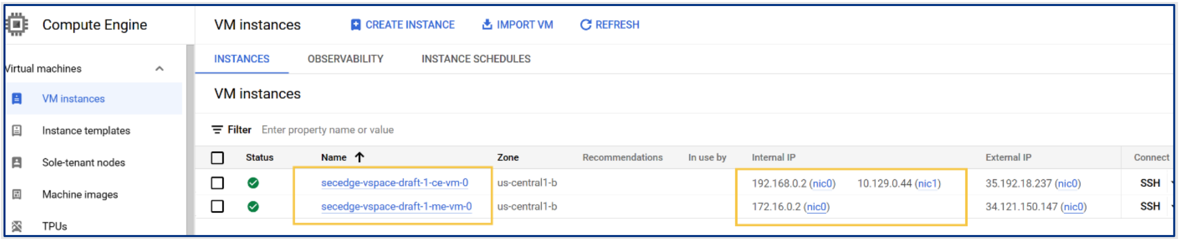
```
Overview - secedge-draft-1
▾ secedge secedge.jinja
  ▾ secedge-draft-1-me-network network.py
      secedge-draft-1-me-network network
  ▾ secedge-draft-1-me-subnetwork sub_network.py
      secedge-draft-1-me-subnetwork subnetwork
  ▾ secedge-draft-1-me firewall.py
      secedge-draft-1-me-allow-ssh firewall
      secedge-draft-1-me-port-for-tunnel firewall
      secedge-draft-1-me-port-for-proxy firewall
  ▾ me-tier me_tier.jinja
    ▾ secedge-draft-1-me-vm-tmpl-0 vm_instance.py
        secedge-draft-1-me-vm-0 vm instance
  ▾ secedge-draft-1-ce-network network.py
      secedge-draft-1-ce-network network
  ▾ secedge-draft-1-ce-subnetwork sub_network.py
      secedge-draft-1-ce-subnetwork subnetwork
  ▾ secedge-draft-1-ce firewall.py
      secedge-draft-1-ce-allow-ssh firewall
      secedge-draft-1-ce-port-for-tunnel firewall
      secedge-draft-1-ce-port-for-proxy firewall
  ▾ ce-tier ce_tier.jinja
    ▾ secedge-draft-1-ce-vm-tmpl-0 vm_instance.py
        secedge-draft-1-ce-vm-0 vm instance
```

User (Serial Console)	ubuntu
Password (Serial Console)	L+8SnWFj
Zone	us-east1-b

Figure 7 Deployment Manager Page

Google Cloud, Compute Engine, **VM instances** page lists the two deployed VMs. Note that the MicroEdge VM name contains "me" and the CloudEdge VM name contains "ce". Figure 8:

- CloudEdge VM, secedge-draft-1-ce-vm-0 has two network interfaces: LAN and WAN.
- MicroEdge VM, secedge-draft-1-me-vm-0 has one WAN network interface.



☐	Status	Name ↑	Zone	Recommendations	In use by	Internal IP		External IP	Connect
☐	✓	secedge-vspace-draft-1-ce-vm-0	us-central1-b			192.168.0.2 (nic0)	10.129.0.44 (nic1)	35.192.18.237 (nic0)	SSH
☐	✓	secedge-vspace-draft-1-me-vm-0	us-central1-b			172.16.0.2 (nic0)		34.121.150.147 (nic0)	SSH

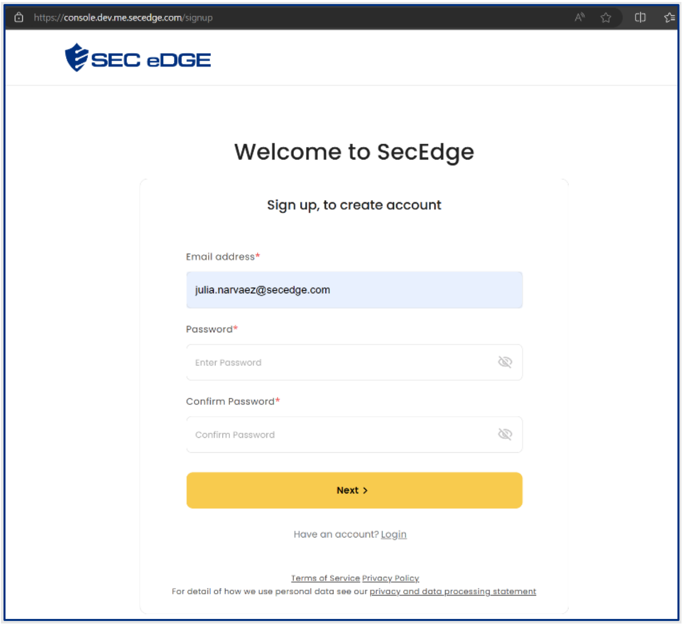
Figure 8 VM Instances page after deploying SecEdge Studio VMs

4.2. MANAGE MICROEDGE AND CLOUDEDGE INSTANCES THROUGH SECeDGE STUDIO™ USER INTERFACE

On the SecEdge Studio User Interface you can manage and configure MicroEdge and CloudEdge device groups, devices and their connectivity.

1. Sign Up into SecEdge Studio™ User Interface

- On the **Deployment Manager** page, clicking on the SIGNUP WITH SECeDGE link redirects you to the SecEdge Studio user interface, Figure 9 and Figure 10.
- Sign up on the **Welcome to SecEdge** page of the user interface. The password requires at least an upper-case letter and special character.



Welcome to SecEdge

Sign up, to create account

Email address*

julia.narvaez@secedge.com

Password*

Enter Password

Confirm Password*

Confirm Password

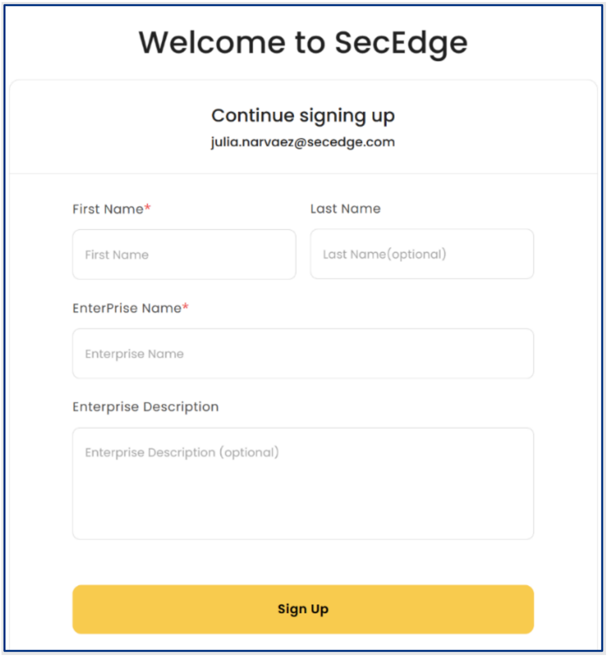
Next >

Have an account? Login

Terms of Service Privacy Policy

For detail of how we use personal data see our privacy and data processing statement

Figure 9 SecEdge Studio Create Account



Welcome to SecEdge

Continue signing up

julia.narvaez@secedge.com

First Name*

First Name

Last Name

Last Name(optional)

EnterPrise Name*

Enterprise Name

Enterprise Description

Enterprise Description (optional)

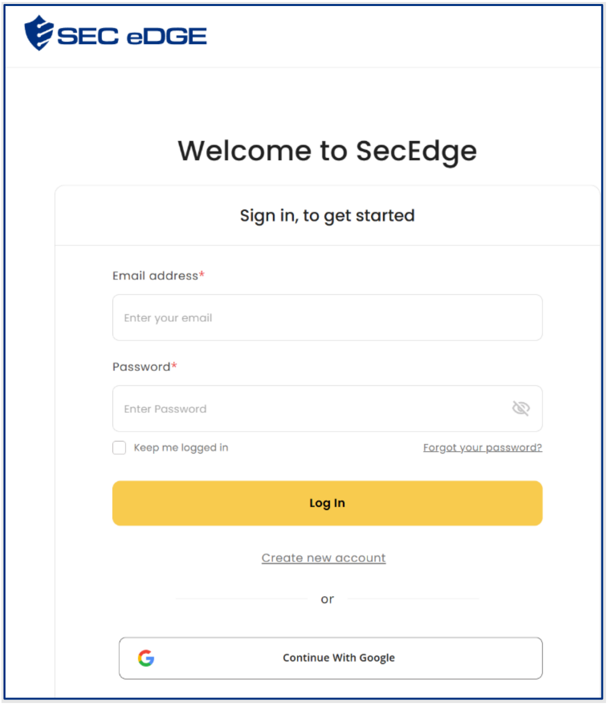
Sign Up

Figure 10 SecEdge Studio Sign up

2. Sign into SecEdge Studio™ User Interface to manage your deployment, Figure 11.

   + To access directly after you have signed up:

     https://console.me.secedge.com



SEC eDGE

Welcome to SecEdge

Sign in, to get started

Email address*

Enter your email

Password*

Enter Password

□ Keep me logged in

Forgot your password?

Log In

Create new account

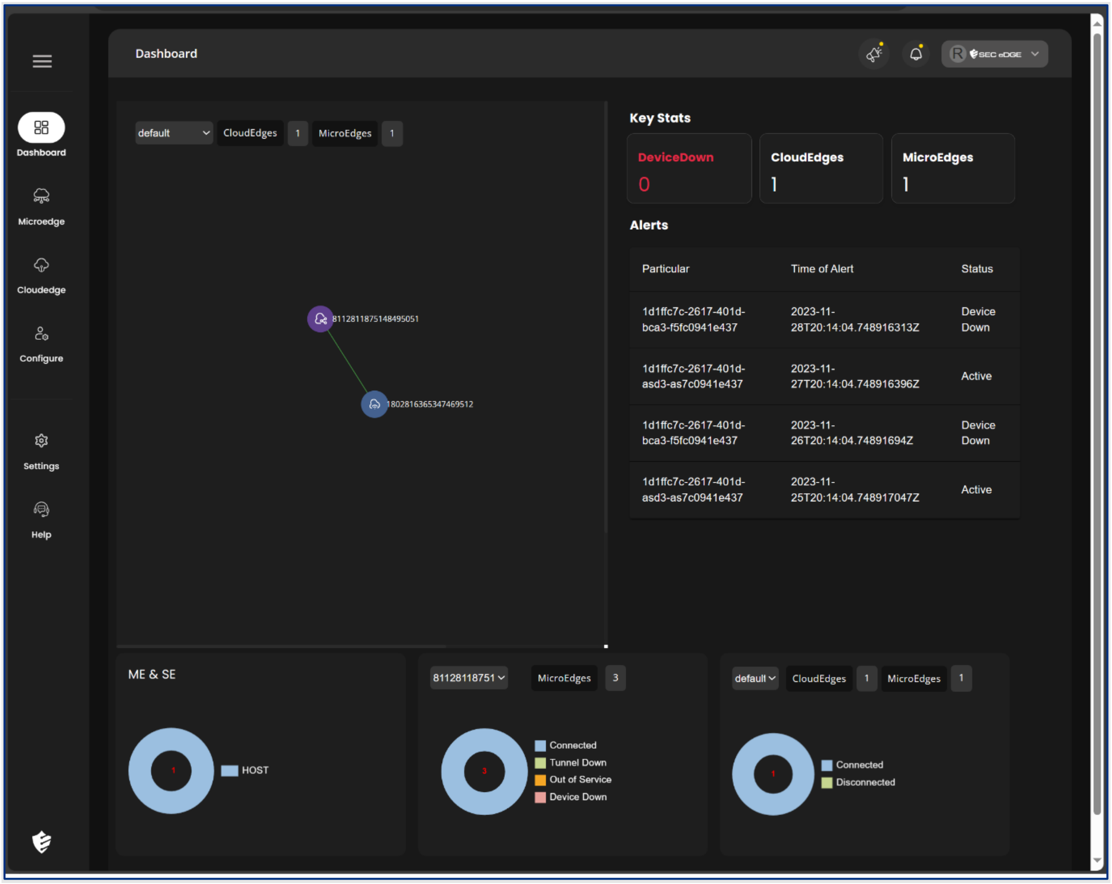
or

Continue With Google

Figure 11 SecEdge Studio Sign In

4.3. SECeDGE STUDIO™ USER INTERFACE DASHBOARD

The dashboard, Figure 12, shows the secure tunnel established between MicroEdge and CloudEdge, their connection state and key stats. The left side options enable management of MicroEdge and CloudEdge groups, devices, profile configuration and user settings.



Dashboard

Key Stats

DeviceDown	CloudEdges	MicroEdges
0	1	1

Alerts

Particular	Time of Alert	Status
1d1ffc7c-2617-401d-bca3-f5fc0941e437	2023-11-28T20:14:04.748916313Z	Device Down
1d1ffc7c-2617-401d-asd3-as7c0941e437	2023-11-27T20:14:04.748916396Z	Active
1d1ffc7c-2617-401d-bca3-f5fc0941e437	2023-11-26T20:14:04.74891694Z	Device Down
1d1ffc7c-2617-401d-asd3-as7c0941e437	2023-11-25T20:14:04.748917047Z	Active

Figure 12 SecEdge Studio Dashboard

5. VERIFY CONFIGURATION AND CREDENTIAL EXISTENCE

During deployment, MicroEdge is configured on the MicroEdge and CloudEdge VMs. The verification of the existence of expected configuration file and credentials is done in the operating system of each VM.

MicroEdge VM

1. Access the terminal of the VM. Section 12.1.1 Guide to Connect to MicroEdge VM Serial Console instructs how to connect to the serial console.

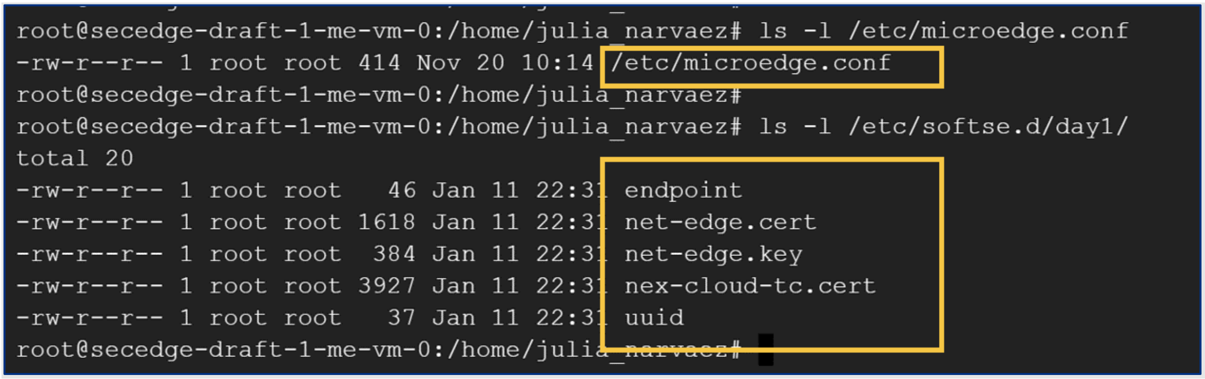
2. Run the following commands. The output is shown in Figure 13:

   + Verify the existence of the configuration file.

```
ls -l /etc/microedge.conf "
```

   + Verify the existence of day1 ControlEdge credentials.

```
ls -l /etc/softse.d/day1/
```



```
root@secedge-draft-1-me-vm-0:/home/julia_narvaez# ls -l /etc/microedge.conf
-rw-r--r-- 1 root root 414 Nov 20 10:14 /etc/microedge.conf
root@secedge-draft-1-me-vm-0:/home/julia_narvaez#
root@secedge-draft-1-me-vm-0:/home/julia_narvaez# ls -l /etc/softse.d/day1/
total 20
-rw-r--r-- 1 root root   46 Jan 11 22:31 endpoint
-rw-r--r-- 1 root root 1618 Jan 11 22:31 net-edge.cert
-rw-r--r-- 1 root root  384 Jan 11 22:31 net-edge.key
-rw-r--r-- 1 root root 3927 Jan 11 22:31 nex-cloud-tc.cert
-rw-r--r-- 1 root root   37 Jan 11 22:31 uuid
root@secedge-draft-1-me-vm-0:/home/julia_narvaez#
```

Figure 13 MicroEdge Configuration and Credentials

CloudEdge VM

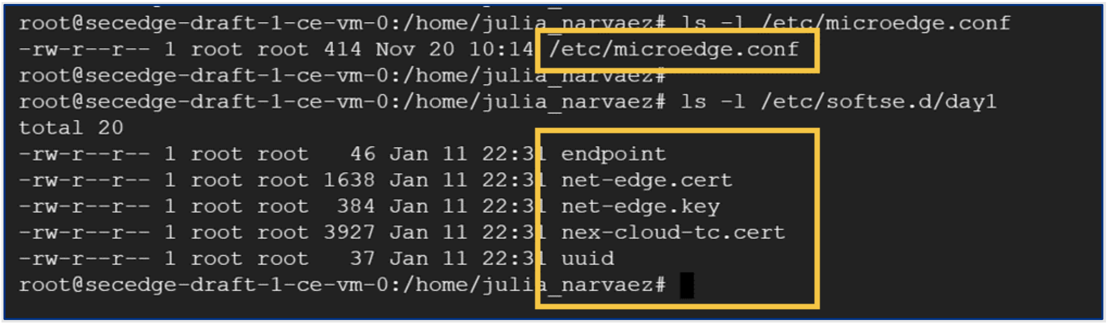
1. SSH to the VM.
2. Run the following commands. The output is shown in Figure 14:

   + Verify the existence of the configuration file.

```
ls -l /etc/microedge.conf "
```

   + Verify the existence of day1 ControlEdge credentials.

```
ls -l /etc/softse.d/day1/
```



```
root@secedge-draft-1-ce-vm-0:/home/julia_narvaez# ls -l /etc/microedge.conf
-rw-r--r-- 1 root root 414 Nov 20 10:14 /etc/microedge.conf
root@secedge-draft-1-ce-vm-0:/home/julia_narvaez#
root@secedge-draft-1-ce-vm-0:/home/julia_narvaez# ls -l /etc/softse.d/day1
total 20
-rw-r--r-- 1 root root   46 Jan 11 22:31 endpoint
-rw-r--r-- 1 root root 1638 Jan 11 22:31 net-edge.cert
-rw-r--r-- 1 root root  384 Jan 11 22:31 net-edge.key
-rw-r--r-- 1 root root 3927 Jan 11 22:31 nex-cloud-tc.cert
-rw-r--r-- 1 root root   37 Jan 11 22:31 uuid
root@secedge-draft-1-ce-vm-0:/home/julia_narvaez#
```

Figure 14 CloudEdge Configuration and Credentials

6. VERIFY CONNECTIVITY BETWEEN MICROEDGE™ AND CLOUDEDGE™

This test verifies the existence of the virtual interface and the connectivity between the MicroEdge and CloudEdge VMs. Also, it refers to the SecEdge User Interface where the last connection time is recorded.

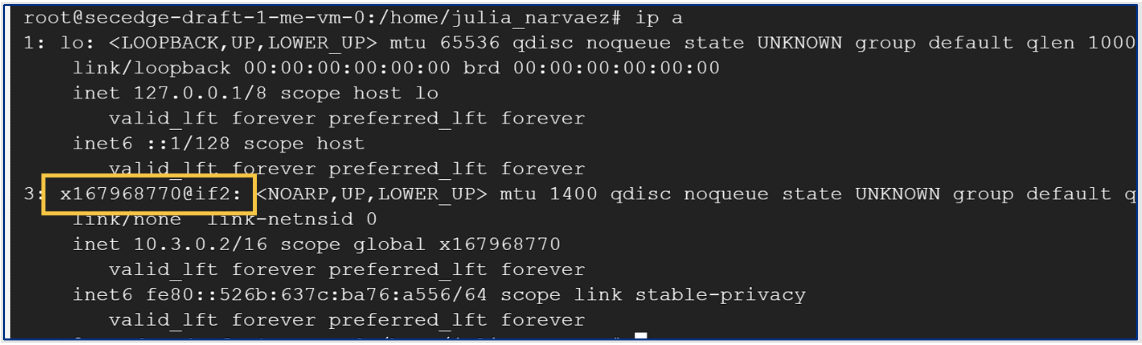
6.1. VERIFY EXISTENCE OF VIRTUAL INTERFACE

MicroEdge VM

1. Access the VM serial console, please see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.
2. Run the following command. The output is shown in Figure 15:

```
ip a
```

3. Verify the existence of virtual interface, starts with **x**. Sample output shown in Figure 15



```
root@secedge-draft-1-me-vm-0:/home/julia_narvaez# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: x167968770@if2: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default q
    link/none  link-netnsid 0
    inet 10.3.0.2/16 scope global x167968770
       valid_lft forever preferred_lft forever
    inet6 fe80::526b:637c:ba76:a556/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

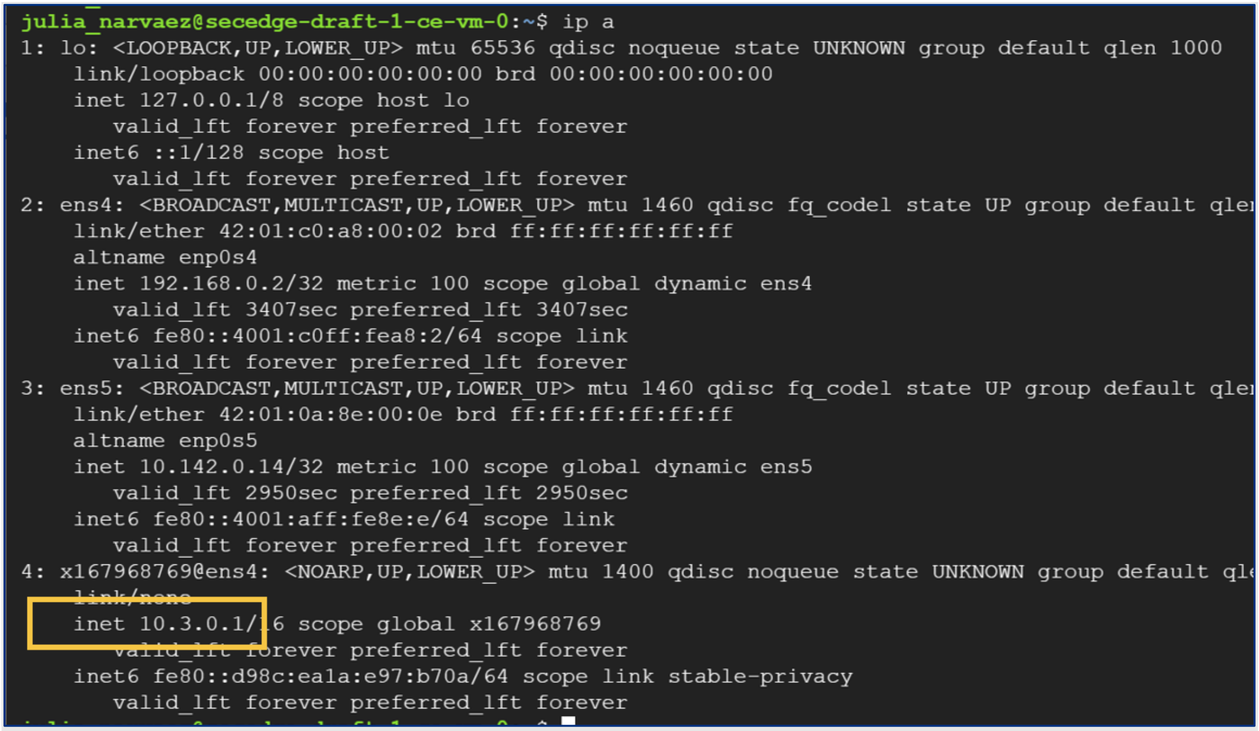
Figure 15 MicroEdge Virtual Interface

CloudEdge VM

1. SSH to the VM.
2. Run the following command. The output is shown in Figure 16:

```
ip a
```

3. Verify the existence of virtual interface, starts with x, and take note of the IP address.

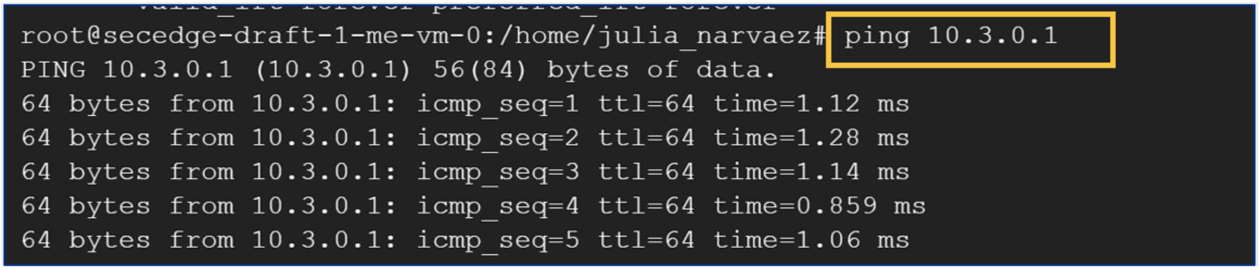


```
julia_narvaez@secedge-draft-1-ce-vm-0:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc fq_codel state UP group default qle
    link/ether 42:01:c0:a8:00:02 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 192.168.0.2/32 metric 100 scope global dynamic ens4
       valid_lft 3407sec preferred_lft 3407sec
    inet6 fe80::4001:c0ff:fea8:2/64 scope link
       valid_lft forever preferred_lft forever
3: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc fq_codel state UP group default qle
    link/ether 42:01:0a:8e:00:0e brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet 10.142.0.14/32 metric 100 scope global dynamic ens5
       valid_lft 2950sec preferred_lft 2950sec
    inet6 fe80::4001:aff:fe8e:e/64 scope link
       valid_lft forever preferred_lft forever
4: x167968769@ens4: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default ql
    link/none
    inet 10.3.0.1/16 scope global x167968769
       valid_lft forever preferred_lft forever
    inet6 fe80::d98c:ea1a:e97:b70a/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Figure 16 CloudEdge Virtual Interface

6.2. EXECUTE ping COMMAND

On the MicroEdge VM, execute the ping command to the CloudEdge VM virtual interface address, e.g. ping 10.3.0.1. Figure 17 shows sample output.



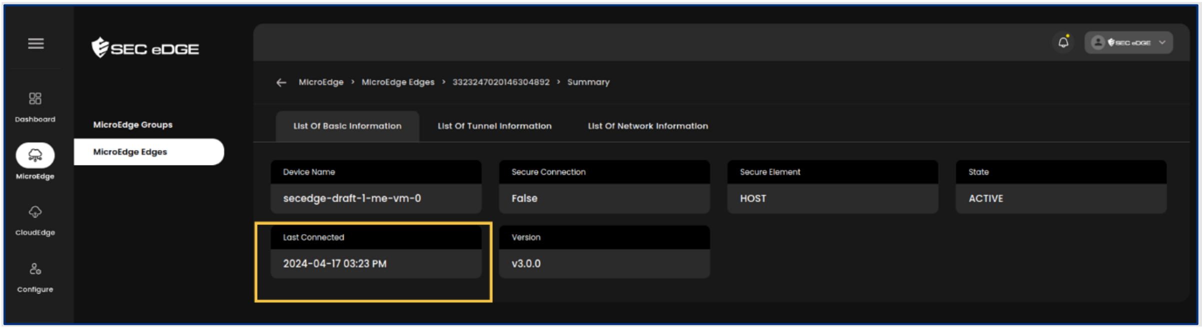
```
    valid_lft forever preferred_lft forever
root@secedge-draft-1-me-vm-0:/home/julia_narvaez# ping 10.3.0.1
PING 10.3.0.1 (10.3.0.1) 56(84) bytes of data.
64 bytes from 10.3.0.1: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 10.3.0.1: icmp_seq=2 ttl=64 time=1.28 ms
64 bytes from 10.3.0.1: icmp_seq=3 ttl=64 time=1.14 ms
64 bytes from 10.3.0.1: icmp_seq=4 ttl=64 time=0.859 ms
64 bytes from 10.3.0.1: icmp_seq=5 ttl=64 time=1.06 ms
```

Figure 17 Command ping execution

6.3. VERIFY CONNECTIVITY IN THE SECeDGE USER INTERFACE

On the SecEdge User Interface, select MicroEdge option on the left and then Edges, Figure 18, and verify that:

- STATE is ACTIVE
- Last Connected timestamp should be close to current time.


SEC eDGE
Dashboard
MicroEdge
CloudEdge
Configure
MicroEdge Groups
MicroEdge Edges
MicroEdge › MicroEdge Edges › 3323247020146304892 › Summary
List Of Basic Information
List Of Tunnel Information
List Of Network Information

Device Name: secedge-draft-1-me-vm-0
Secure Connection: False
Secure Element: HOST
State: ACTIVE
Last Connected: 2024-04-17 03:23 PM
Version: v3.0.0

Figure 18 MicroEdge List of Basic Information

7. DEMO IOT APP

This is simple client-server application. The demo application is available at github repo: https://github.com/secedgedev/me_solution_demo_app_1. The source code is provided for demonstration purpose only. During the test, you clone the repo and build the application.

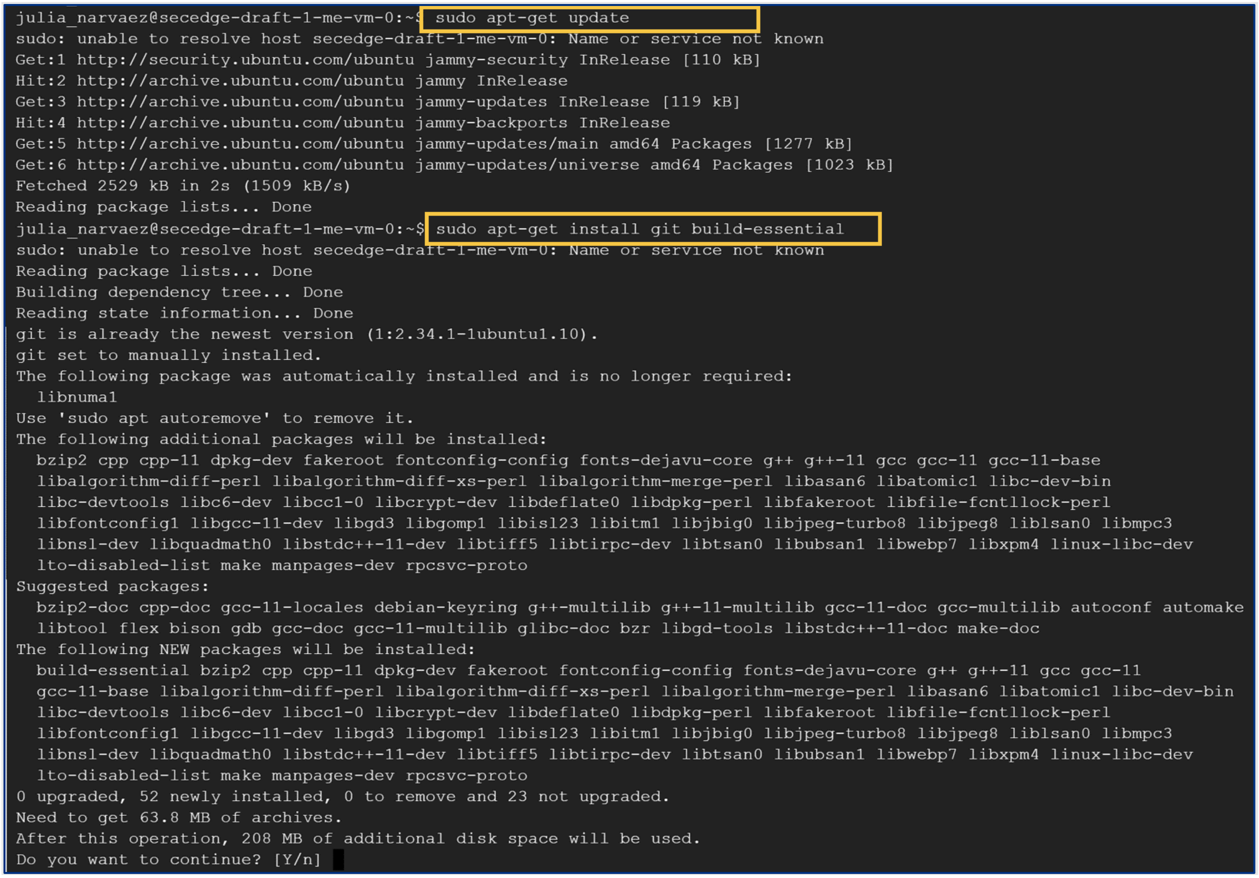
7.1. INSTALL DEMO APP IOT APPLICATION IN MICROEDGE VM

The application on the MicroEdge VM instance will run in client mode. You can enter the message on terminal and send it to server application.

1. Connect to the MicroEdge VM instance, see 12.1.1 Guide to Connect to MicroEdge VM Serial Console..
2. Install git and g++ compiler:

```
$ sudo apt-get update
$ sudo apt-get install git build-essential
```

Figure 19 shows sample commands and output.



```
julia_narvaez@secedge-draft-1-me-vm-0:~$ sudo apt-get update
sudo: unable to resolve host secedge-draft-1-me-vm-0: Name or service not known
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1277 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1023 kB]
Fetched 2529 kB in 2s (1509 kB/s)
Reading package lists... Done
julia_narvaez@secedge-draft-1-me-vm-0:~$ sudo apt-get install git build-essential
sudo: unable to resolve host secedge-draft-1-me-vm-0: Name or service not known
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.34.1-1ubuntu1.10).
git set to manually installed.
The following package was automatically installed and is no longer required:
  libnuma1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  bzip2 cpp cpp-11 dpkg-dev fakeroot fontconfig-config fonts-dejavu-core g++ g++-11 gcc gcc-11 gcc-11-base
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan6 libatomic1 libc-dev-bin
  libc-devtools libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl
  libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 liblsan0 libmpc3
  libnsl-dev libquadmath0 libstdc++-11-dev libtiff5 libtirpc-dev libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev
  lto-disabled-list make manpages-dev rpcsvc-proto
Suggested packages:
  bzip2-doc cpp-doc gcc-11-locales debian-keyring g++-multilib g++-11-multilib gcc-11-doc gcc-multilib autoconf automake
  libtool flex bison gdb gcc-doc gcc-11-multilib glibc-doc bzr libgd-tools libstdc++-11-doc make-doc
The following NEW packages will be installed:
  build-essential bzip2 cpp cpp-11 dpkg-dev fakeroot fontconfig-config fonts-dejavu-core g++ g++-11 gcc gcc-11
  gcc-11-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan6 libatomic1 libc-dev-bin
  libc-devtools libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl
  libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 liblsan0 libmpc3
  libnsl-dev libquadmath0 libstdc++-11-dev libtiff5 libtirpc-dev libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev
  lto-disabled-list make manpages-dev rpcsvc-proto
0 upgraded, 52 newly installed, 0 to remove and 23 not upgraded.
Need to get 63.8 MB of archives.
After this operation, 208 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 19 MicroEdge Instance Software Installation

3. Clone demo app source code to this VM.

```
$ git clone https://github.com/secedgedev/me_solution_demo_app_1
```

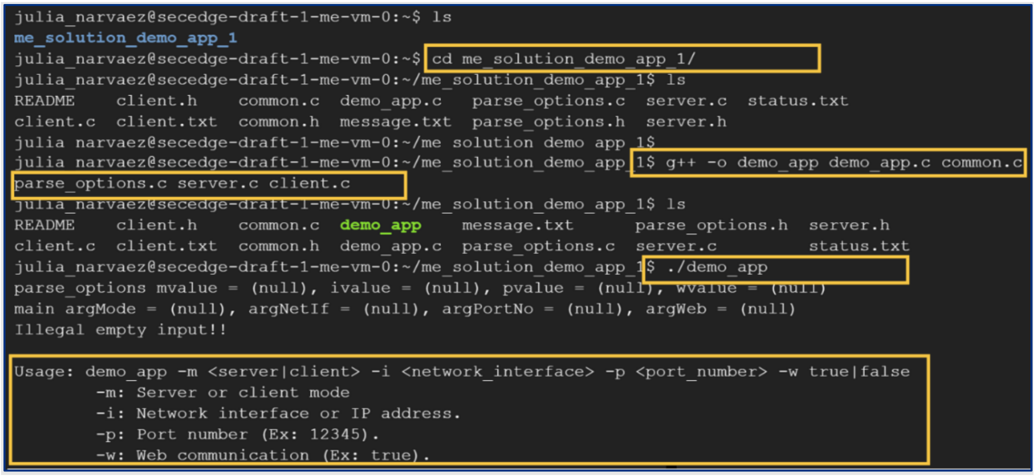
4. Compile the source code:

```
$ cd me_solution_demo_app_1

$ g++ -o demo_app demo_app.c common.c parse_options.c server.c client.c
```

5. Check the usage help text:

```
$ ./demo_app
```

Figure 20 shows sample commands and output.



```
julia_narvaez@secedge-draft-1-me-vm-0:~$ ls
me_solution_demo_app_1
julia_narvaez@secedge-draft-1-me-vm-0:~$ cd me_solution_demo_app_1/
julia_narvaez@secedge-draft-1-me-vm-0:~/me_solution_demo_app_1$ ls
README     client.h     common.c  demo_app.c   parse_options.c  server.c  status.txt
client.c   client.txt   common.h  message.txt  parse_options.h  server.h
julia_narvaez@secedge-draft-1-me-vm-0:~/me_solution_demo_app_1$
julia_narvaez@secedge-draft-1-me-vm-0:~/me_solution_demo_app_1$ g++ -o demo_app demo_app.c common.c
parse_options.c server.c client.c
julia_narvaez@secedge-draft-1-me-vm-0:~/me_solution_demo_app_1$ ls
README     client.h     common.c  demo_app     message.txt      parse_options.h  server.h
client.c   client.txt   common.h  demo_app.c   parse_options.c  server.c         status.txt
julia_narvaez@secedge-draft-1-me-vm-0:~/me_solution_demo_app_1$ ./demo_app
parse_options mvalue = (null), ivalue = (null), pvalue = (null), wvalue = (null)
main argMode = (null), argNetIf = (null), argPortNo = (null), argWeb = (null)
Illegal empty input!!

Usage: demo_app -m <server|client> -i <network_interface> -p <port_number> -w true|false
        -m: Server or client mode
        -i: Network interface or IP address.
        -p: Port number (Ex: 12345).
        -w: Web communication (Ex: true).
```

Figure 20 MicroEdge Instance Demo App Build

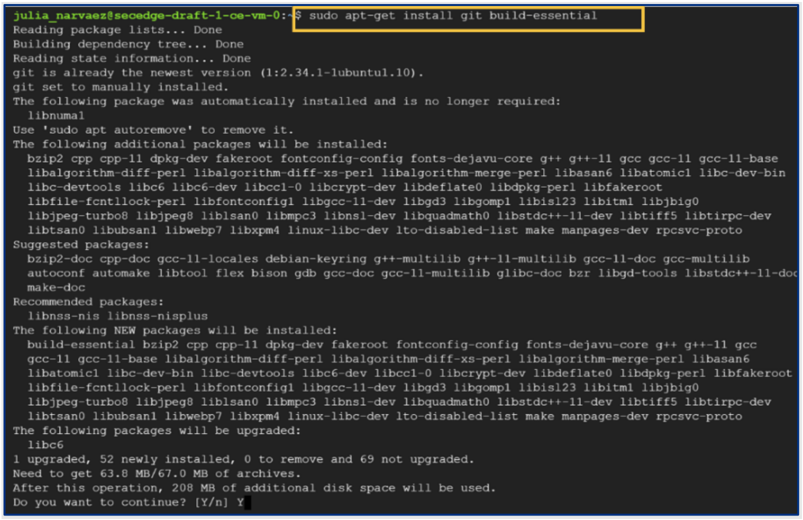
7.2. INTEGRATE/CONNECT BACKEND APPLICATION IN MICROEDGE VM INSTANCE WITH CLOUDEDGE VM

Deploy the same application on CloudEdge, which will run with server mode. The server application waits for messages from client application.

1. Connect to MicroEdge VM instance, see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.

2. Install git and g++ compiler:

```
$ sudo apt-get update

$ sudo apt-get install git build-essential
```



```
julia_narvaez@secedge-draft-1-ce-vm-0:~$ sudo apt-get install git build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.34.1-1ubuntu1.10).
git set to manually installed.
The following package was automatically installed and is no longer required:
  libnuma1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  bzip2 cpp cpp-11 dpkg-dev fakeroot fontconfig-config fonts-dejavu-core g++ g++-11 gcc gcc-11 gcc-11-base
  libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan6 libatomic1 libc-dev-bin
  libc-devtools libc6 libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfakeroot
  libfile-fcntllock-perl libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0
  libjpeg-turbo8 libjpeg8 liblsan0 libmpc3 libnsl-dev libquadmath0 libstdc++-11-dev libtiff5 libtirpc-dev
  libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev rpcsvc-proto
Suggested packages:
  bzip2-doc cpp-doc gcc-11-locales debian-keyring g++-multilib g++-11-multilib gcc-11-doc gcc-multilib
  autoconf automake libtool flex bison gdb gcc-doc gcc-11-multilib glibc-doc bzr libgd-tools libstdc++-11-doc
  make-doc
Recommended packages:
  libnss-nis libnss-nisplus
The following NEW packages will be installed:
  build-essential bzip2 cpp cpp-11 dpkg-dev fakeroot fontconfig-config fonts-dejavu-core g++ g++-11 gcc
  gcc-11 gcc-11-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan6
  libatomic1 libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfakeroot
  libfile-fcntllock-perl libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0
  libjpeg-turbo8 libjpeg8 liblsan0 libmpc3 libnsl-dev libquadmath0 libstdc++-11-dev libtiff5 libtirpc-dev
  libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev rpcsvc-proto
The following packages will be upgraded:
  libc6
1 upgraded, 52 newly installed, 0 to remove and 69 not upgraded.
Need to get 63.8 MB/67.0 MB of archives.
After this operation, 208 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Figure 21 CloudEdge Instance Software Installation

3. Clone demo app source code to this VM.

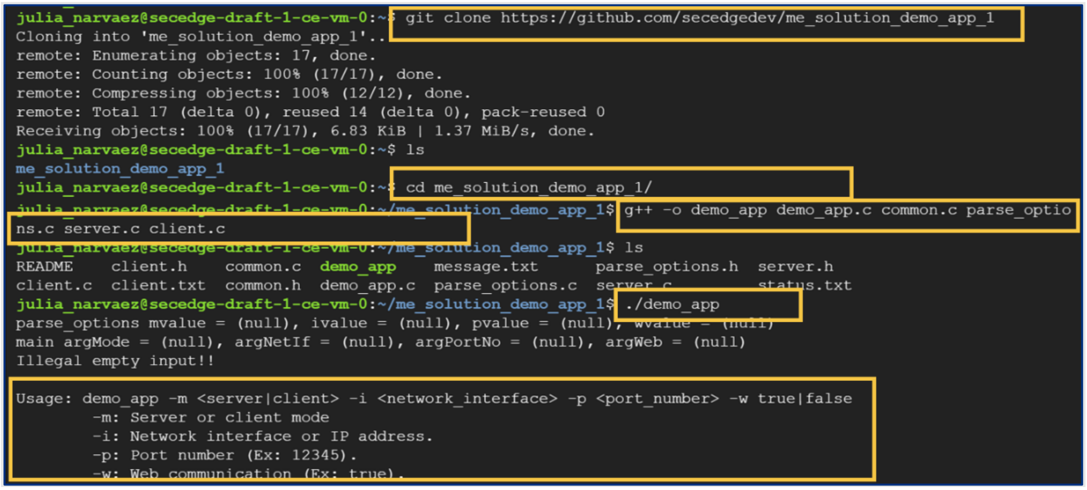
```
$ git clone https://github.com/secedgedev/me_solution_demo_app_1
```

4. Compile the source code:

```
$ cd me_solution_demo_app_1

$ g++ -o demo_app demo_app.c common.c parse_options.c server.c client.c
```

5. Check the usage help text:

```
$ ./demo_app
```



```
julia_narvaez@secedge-draft-1-ce-vm-0:~$ git clone https://github.com/secedgedev/me_solution_demo_app_1
Cloning into 'me_solution_demo_app_1'...
remote: Enumerating objects: 17, done.
remote: Counting objects: 100% (17/17), done.
remote: Compressing objects: 100% (12/12), done.
remote: Total 17 (delta 0), reused 14 (delta 0), pack-reused 0
Receiving objects: 100% (17/17), 6.83 KiB | 1.37 MiB/s, done.
julia_narvaez@secedge-draft-1-ce-vm-0:~$ ls
me_solution_demo_app_1
julia_narvaez@secedge-draft-1-ce-vm-0:~$ cd me_solution_demo_app_1/
julia_narvaez@secedge-draft-1-ce-vm-0:~/me_solution_demo_app_1$ g++ -o demo_app demo_app.c common.c parse_optio
ns.c server.c client.c
julia_narvaez@secedge-draft-1-ce-vm-0:~/me_solution_demo_app_1$ ls
README    client.h    common.c  demo_app    message.txt      parse_options.h  server.h
client.c  client.txt  common.h  demo_app.c  parse_options.c  server.c         status.txt
julia_narvaez@secedge-draft-1-ce-vm-0:~/me_solution_demo_app_1$ ./demo_app
parse_options mvalue = (null), ivalue = (null), pvalue = (null), wvalue = (null)
main argMode = (null), argNetIf = (null), argPortNo = (null), argWeb = (null)
Illegal empty input!!

Usage: demo_app -m <server|client> -i <network_interface> -p <port_number> -w true|false
        -m: Server or client mode
        -i: Network interface or IP address.
        -p: Port number (Ex: 12345).
        -w: Web communication (Ex: true).
```

Figure 22 CloudEdge Instance Demo App Build

7.3. PERFORM COMPLETE END TO END TESTING

Test the secure tunnel with data from the MicroEdge VM instance to the CloudEdge VM instance using the client-server application installed in the previous section.

1. SSH to the **CloudEdge** VM instance.

2. In the CloudEdge VM, identify the IP address of the XFRM interface. The interface starts with the x letter. In this example the IP is 10.3.0.1.

3. Start demo_app in server mode, listening on secure tunnel IP and port number

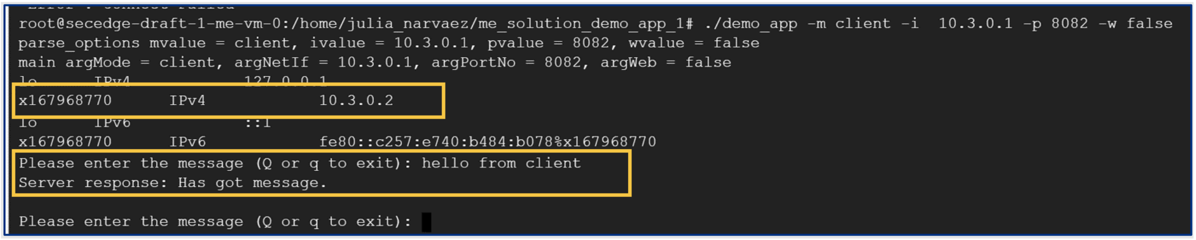
```
$ cd me_solution_demo_app_1

$ ./demo_app -m server -i  10.3.0.1 -p 8082 -w false
```

4. Connect to the **MicroEdge** VM, please see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.

5. In the MicroEdge VM, start demo_app in client mode to connect to the CloudEdge VM via secure tunnel IP and port number

```
$ cd me_solution_demo_app_1

$ ./demo_app -m client -i  10.3.0.1 -p 8082 -w false
```

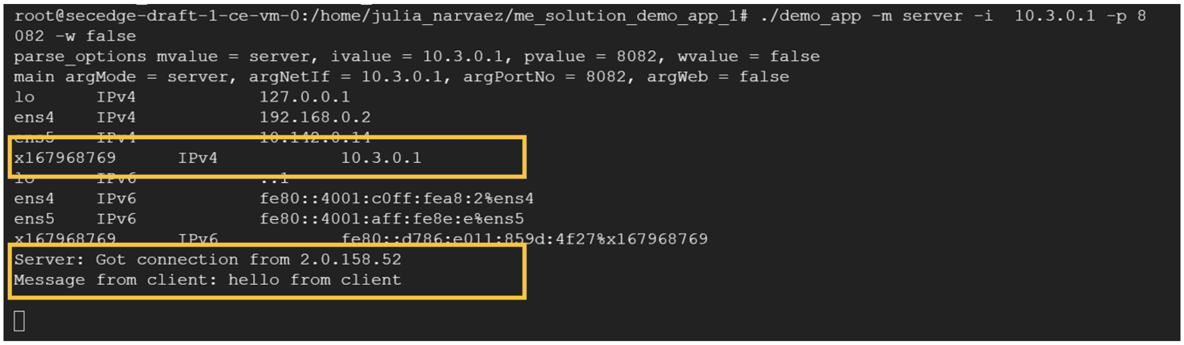
6. In the MicroEdge VM terminal, type a message and press Enter to send the message to the server, e.g. Figure 23.



```
root@secedge-draft-1-me-vm-0:/home/julia_narvaez/me_solution_demo_app_1# ./demo_app -m client -i  10.3.0.1 -p 8082 -w false
parse_options mvalue = client, ivalue = 10.3.0.1, pvalue = 8082, wvalue = false
main argMode = client, argNetIf = 10.3.0.1, argPortNo = 8082, argWeb = false
lo      IPv4            127.0.0.1
x167968770      IPv4            10.3.0.2
lo      IPv6            ::1
x167968770      IPv6            fe80::c257:e740:b484:b078%x167968770
Please enter the message (Q or q to exit): hello from client
Server response: Has got message.

Please enter the message (Q or q to exit): 
```

Figure 23 MicroEdge demo_app execution

7. Observe message displayed on CloudEdge VM console, e.g. Figure 24.



```
root@secedge-draft-1-ce-vm-0:/home/julia_narvaez/me_solution_demo_app_1# ./demo_app -m server -i  10.3.0.1 -p 8
082 -w false
parse_options mvalue = server, ivalue = 10.3.0.1, pvalue = 8082, wvalue = false
main argMode = server, argNetIf = 10.3.0.1, argPortNo = 8082, argWeb = false
lo      IPv4            127.0.0.1
ens4    IPv4            192.168.0.2
ens5    IPv4            10.142.0.14
x167968769      IPv4            10.3.0.1
lo      IPv6            ::1
ens4    IPv6            fe80::4001:c0ff:fea8:2%ens4
ens5    IPv6            fe80::4001:aff:fe8e:e%ens5
x167968769      IPv6            fe80::d786:e011:859d:4f27%x167968769
Server: Got connection from 2.0.158.52
Message from client: hello from client

```

Figure 24 CloudEdge demo_app execution

8. TEST MULTI TUNNELS: CREATE MULTI TUNNELS FROM MICROEDGE™ TO CLOUDEDGES™

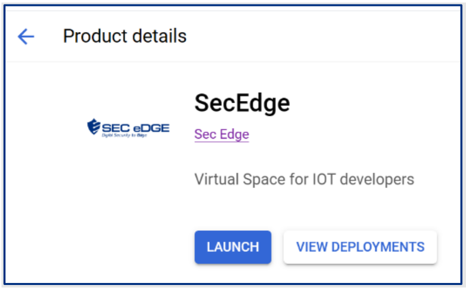
A single MicroEdge instance on a device enables multi-tunnel connectivity to different CloudEdge servers. You can setup multiple configuration profiles and assign them to different groups. This test includes the following main steps:

- In Google Cloud, launch a new deployment with two CloudEdge VMs and one MicroEdge VM.
- In Google Cloud, deploy two additional VM instances that are used as web application servers.
- In the SecEdge User Interface, set up two CloudEdge Groups for defining multi-tunnel profiles and configure the MicroEdge.
- In the VMs terminal, execute the test.

8.1. DEPLOY CLOUDEDGE AND MICROEDGE VMs

In the step, you make new deployment with one MicroEdge VM and two CloudEdge VMs:

- Start in Google Cloud, SecEdge Studio **Product details** page, as described in section 3 Secedge Studio™ Deployment Test Steps, step 6.



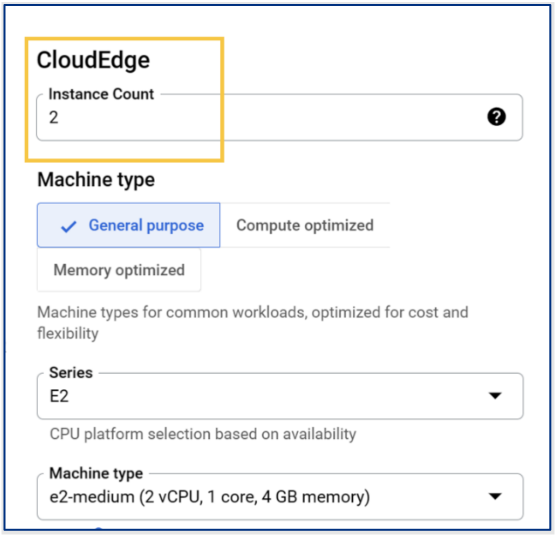
Product details

SecEdge

Sec Edge

Virtual Space for IOT developers

- Click on Launch.
- On deployment input form, CloudEdge **Instance Count**, increase the number to **2**. Then click on Deploy at the bottom of the page.



CloudEdge

Instance Count: 2

Machine type

Machine types for common workloads, optimized for cost and flexibility

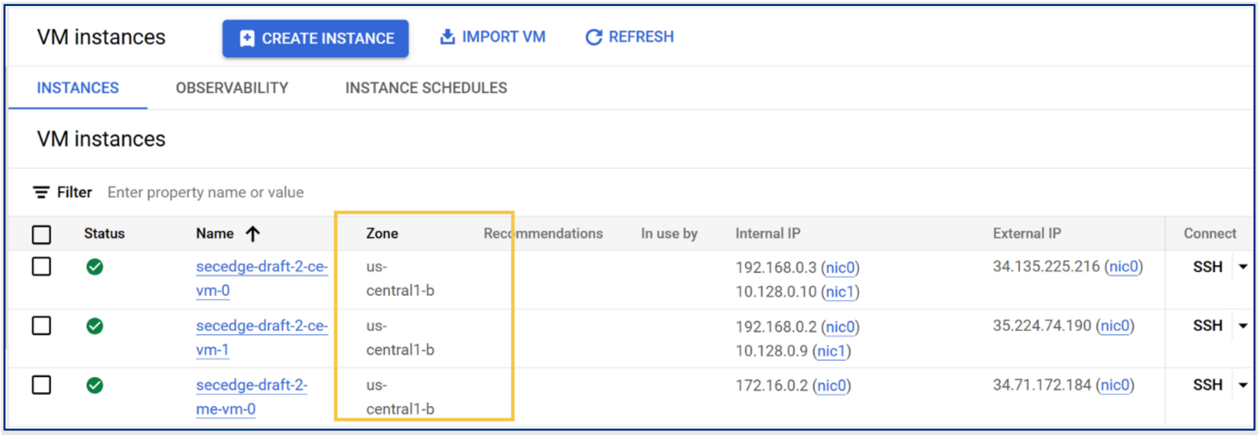
Series: E2

CPU platform selection based on availability

Machine type: e2-medium (2 vCPU, 1 core, 4 GB memory)

Figure 25 Google Cloud, New SecEdge Deployment Page Configuration

After deploying successfully, in the VM instances list, there are three new VMs, such as in Figure 26.



□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
□	✓	secedge-draft-2-ce-vm-0	us-central1-b			192.168.0.3 (nic0) 10.128.0.10 (nic1)	34.135.225.216 (nic0)	SSH ▾
□	✓	secedge-draft-2-ce-vm-1	us-central1-b			192.168.0.2 (nic0) 10.128.0.9 (nic1)	35.224.74.190 (nic0)	SSH ▾
□	✓	secedge-draft-2-me-vm-0	us-central1-b			172.16.0.2 (nic0)	34.71.172.184 (nic0)	SSH ▾

Figure 26 Google Cloud, VM Instances, New Test Deployment VMs

In this deployment, the MicroEdge instance has a tunnel stablished with only one CloudEdge. If you see the SecEdge User Interface Dashboard, it shows a standalone CloudEdge.

8.2. CREATE TWO WEB SERVERS

In Google Cloud, **VM Instances** page, create two VMs, app-web-server and app-web-server-1, shown in Figure 27:

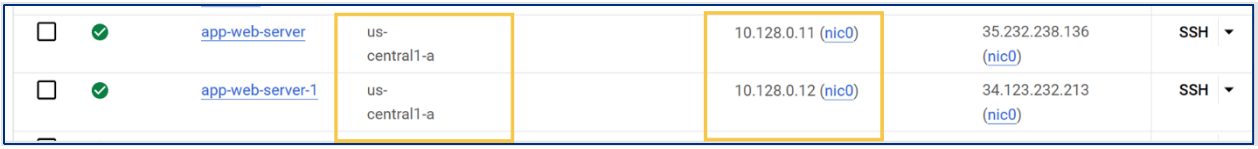
1. Click on the CREATE INSTANCE button.

2. Name the first instance app-web-server.

3. The Region must be same as the CloudEdge and MicroEdge VMs deployed in the previous section. In this example, Region is us-central1. Zone can be different. Accordingly, the selection here is also us-central1. Zone can be a, b, c, f.

4. Repeat steps 1 through 3 to create a new VM instance, app-web-server-1.

5. Notice the Internal IP address of app-web-server and app-web-server-1.



☐	✓	app-web-server	us-central1-a	10.128.0.11 (nic0)	35.232.238.136 (nic0)	SSH ▾
☐	✓	app-web-server-1	us-central1-a	10.128.0.12 (nic0)	34.123.232.213 (nic0)	SSH ▾

Figure 27 Google Cloud, VM Instances, App Web Server VM Instances

8.3. CONFIGURE CLOUDEDGE GROUPS

Both CloudEdge devices created in 8.1 belong to the CloudEdge Default group. This section guides you through the steps to create two groups, Group1 and Group2, and assign each CloudEdge to a different group.

8.3.1. ADD CLOUDEDGE GROUP1

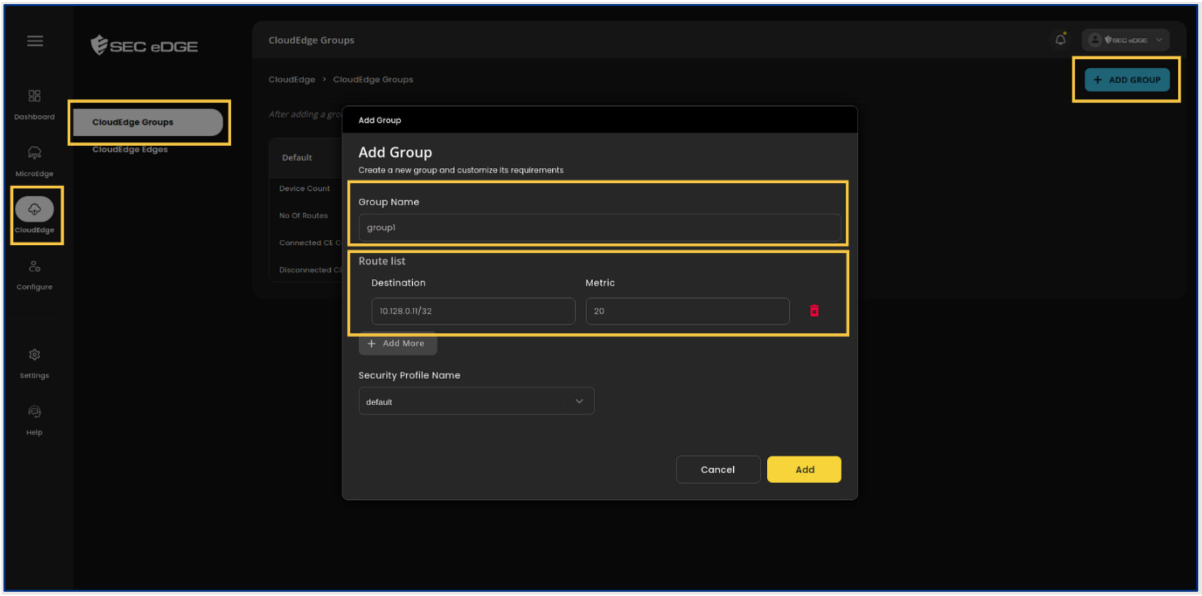
In the SecEdge User Interface, add CloudEdge Group1

+ Select CloudEdge and Groups on the page left side and click on Add Group.

+ Enter the Group Name, in the example is Group1.

The Destination is the IP address in CIDR subnet notation of the app-web-server VM added in 8.2

+ Enter additional data and click on the Add button, shown in Figure 28.



Add Group

Create a new group and customize its requirements

Group Name: group1

Route list

Destination	Metric
10.128.0.11/32	20

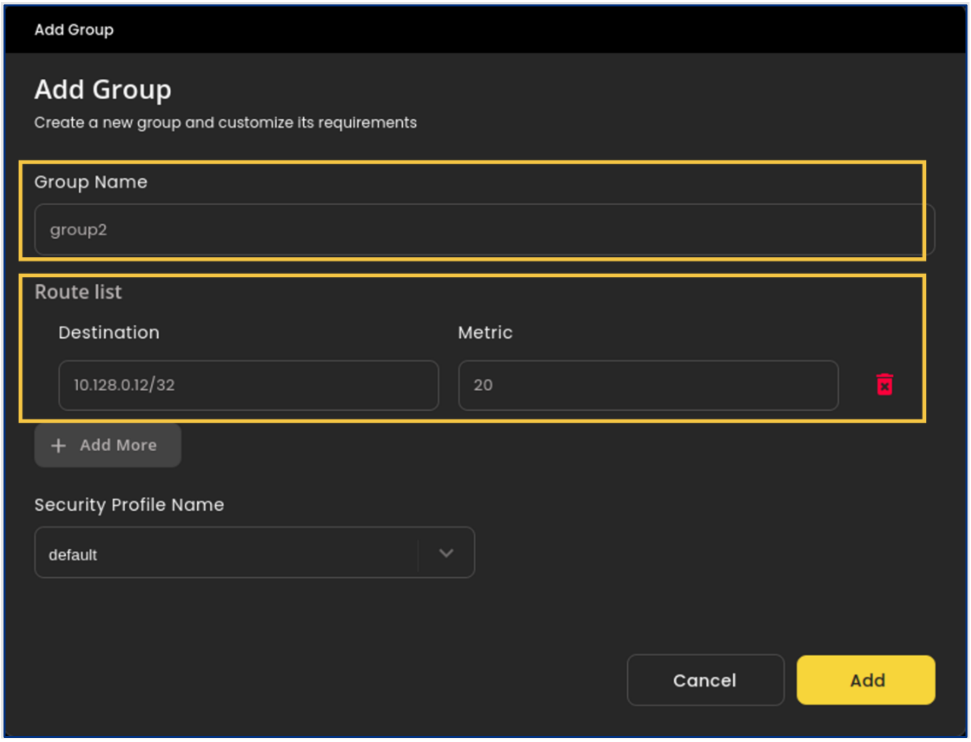
Security Profile Name: default

Figure 28 SecEdge Studio User Interface, Add CloudEdge Group1

- Manually refresh the page to see the new CloudEdge listed in the group.

8.3.2. ADD CLOUDEDGE GROUP2

- Repeat the steps in 1, but change Group Name to Group2.
- The Destination is the internal IP of app-web-server-1 in CIDR format, always with "/32".



Group Name: group2

Route list

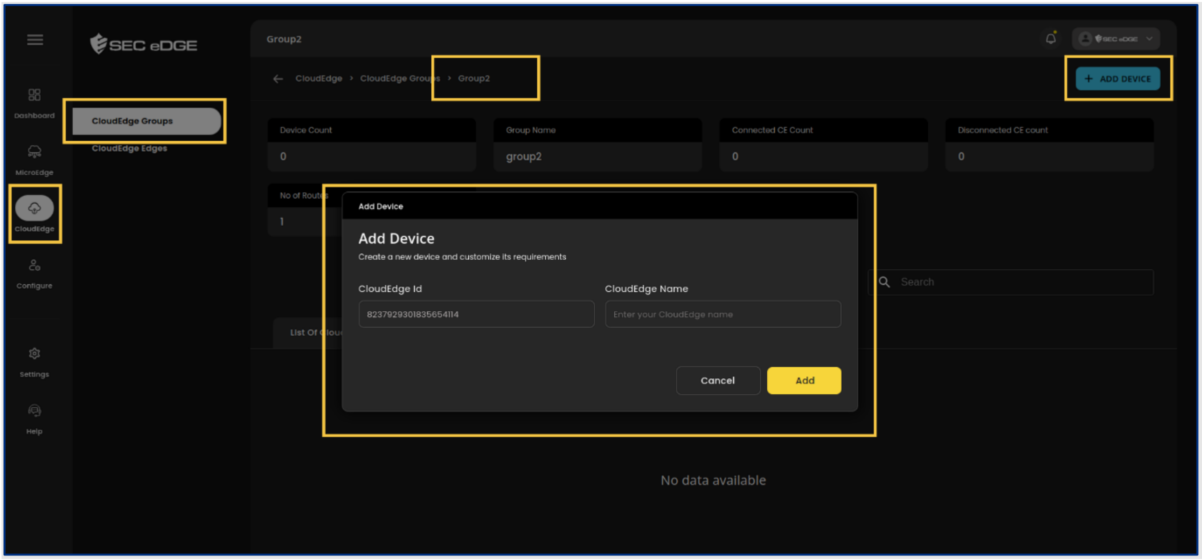
Destination	Metric
10.128.0.12/32	20

Security Profile Name: default

Figure 29 SecEdge Studio User Interface, Add CloudEdge Group2

8.3.3. ADD ONE OF THE CLOUDEDGE VMS TO CLOUDEDGE GROUP1

1. Select CloudEdge and Groups on the page left side.
2. Click on Group1.
3. Click on Add Device.



Device Count	Group Name	Connected CE Count	Disconnected CE count
0	group2	0	0

No of Routes: 1

Add Device

Add Device

Create a new device and customize its requirements

CloudEdge Id: 8237929301835654114

CloudEdge Name: Enter your CloudEdge name

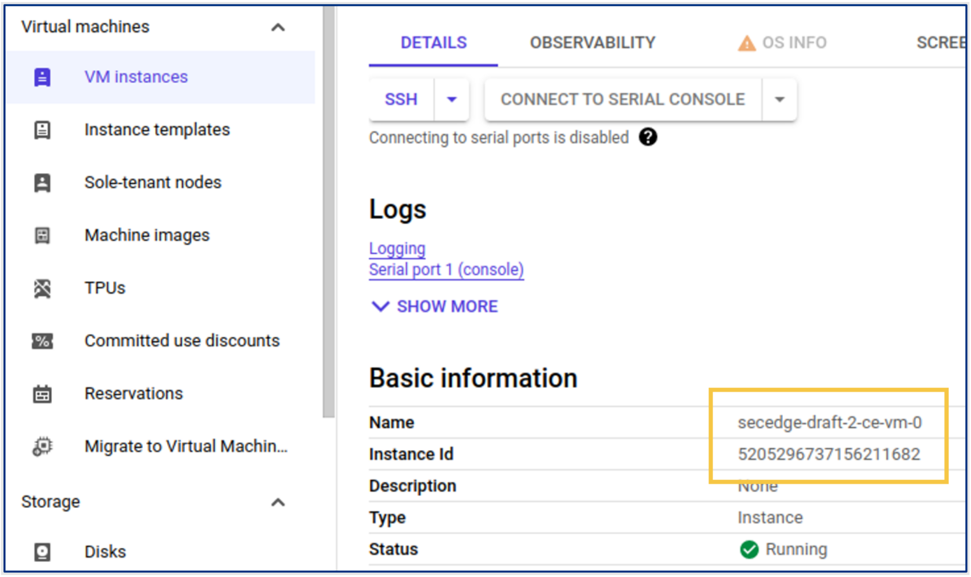
Cancel Add

Figure 30 SecEdge Studio User Interface, Add Device to CloudEdge Group1

4. To enter CloudEdge Id, first identify the Instance Id of one of the CloudEdge VMs deployed in 8.1 Deploy CloudEdge and MicroEdge VMs.

   + For example, in Google Cloud, **VM Instances**, click on the VM name whose name ends in “ce-vm-0”.

   + On the **Details**, **Basic Information** page, identify and copy in the clipboard the Instance Id, illustrated in Figure 31.



Basic information

Name	secedge-draft-2-ce-vm-0
Instance Id	5205296737156211682
Description	None
Type	Instance
Status	Running

Figure 31 Google Cloud, VM Instances, CloudEdge VM Instance Basic Information Page

5. On the SecEdge User Interface, Add Device page:

   + CloudEdge Id: paste the Instance Id from the clipboard.

8.3.4. ADD THE OTHER CLOUDEDGE VM TO CLOUDEDGE GROUP2

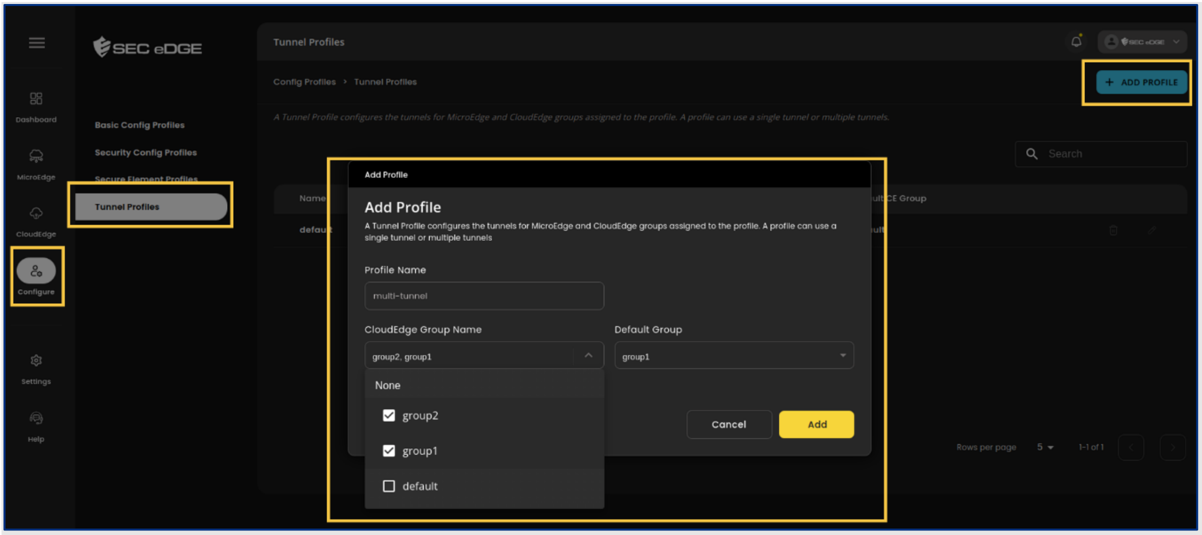
Repeat the steps described in 8.3.3 with the following changes:

- Select CloudEdge Group2.
- To add the device, in Google Cloud, **VM Instances**, look at the details of the CloudEdge VM whose name ends in "ce-vm-1".

8.4. CREATE A MULTI-TUNNEL PROFILE

Create a multi-tunnel profile which links to CloudEdge Group1 and CloudEdge Group2.

- Select Configure and Tunnel Profiles on the page left side and click on Add Profile.
- Enter the Profile Name, in the example is multi-tunnel.
- In CloudEdge Group Name select group1 and group2.
- Select a Default Group.
- Click on the Add button.



A Tunnel Profile configures the tunnels for MicroEdge and CloudEdge groups assigned to the profile. A profile can use a single tunnel or multiple tunnels.

Add Profile

Add Profile

A Tunnel Profile configures the tunnels for MicroEdge and CloudEdge groups assigned to the profile. A profile can use a single tunnel or multiple tunnels

Profile Name: multi-tunnel

CloudEdge Group Name: group2, group1

None
☑ group2
☑ group1
☐ default

Default Group: group1

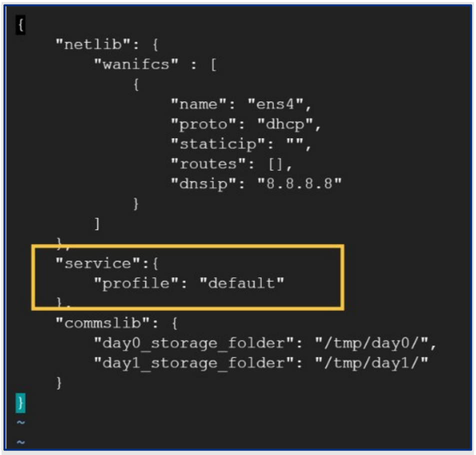
Figure 32 SecEdge Studio User Interface, Add Tunnel Profile

8.5. ASSIGN MULTI-TUNNEL CONFIGURATION TO MICROEDGE

Assign the multi-tunnel profile to the MicroEdge by changing profile in configuration file /etc/microedge.conf of MicroEdge VM.

1. Connect to the MicroEdge VM created in 8.1 Deploy CloudEdge and MicroEdge VMs. Please see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.
2. Edit the MicroEdge configuration file /etc/microedge.conf as follows:

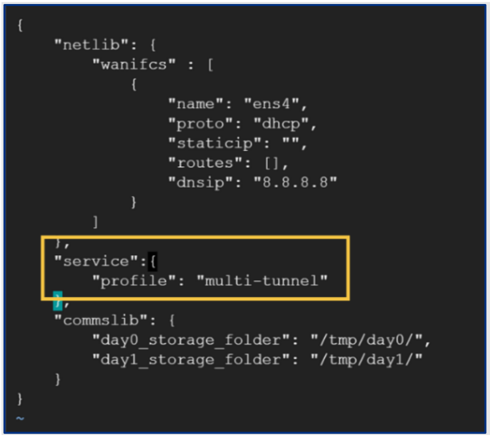
- Figure 33 shows the default tunnel configuration assigned during deployment.



```
{
    "netlib": {
        "wanifcs" : [
            {
                "name": "ens4",
                "proto": "dhcp",
                "staticip": "",
                "routes": [],
                "dnsip": "8.8.8.8"
            }
        ]
    },
    "service":{
        "profile": "default"
    },
    "commslib": {
        "day0_storage_folder": "/tmp/day0/",
        "day1_storage_folder": "/tmp/day1/"
    }
}
~
~
```

Figure 33 MicroEdge Original Configuration with Default Tunnel Profile

- Change the service profile to the one created in 8.4. Figure 34 shows the multi-tunnel tunnel configuration.



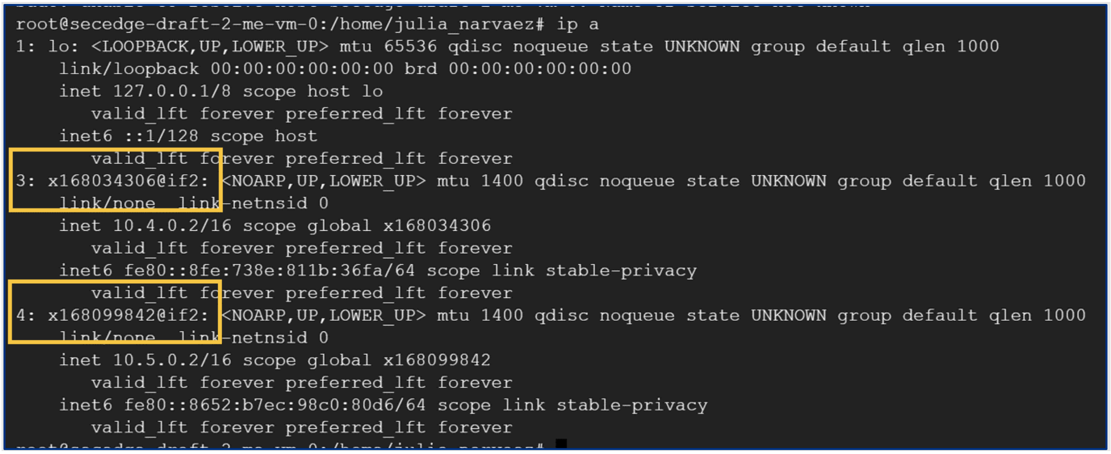
```
{
    "netlib": {
        "wanifcs" : [
            {
                "name": "ens4",
                "proto": "dhcp",
                "staticip": "",
                "routes": [],
                "dnsip": "8.8.8.8"
            }
        ]
    },
    "service":{
        "profile": "multi-tunnel"
    },
    "commslib": {
        "day0_storage_folder": "/tmp/day0/",
        "day1_storage_folder": "/tmp/day1/"
    }
}
~
```

Figure 34 MicroEdge Original Configuration after Changing to multi-tunnel Profile

3. Restart MicroEdge so that ControlEdge can re-setup the tunnels. Check how the multi-tunnel works. The following command can be used:

```
sudo systemctl restart microedge.service
```

4. Execute ip a or “ifconfig. Figure 35 shows the MicroEdge terminal with two tunnels



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: x168034306@if2: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none  link-netnsid 0
    inet 10.4.0.2/16 scope global x168034306
       valid_lft forever preferred_lft forever
    inet6 fe80::8fe:738e:811b:36fa/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
4: x168099842@if2: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none  link-netnsid 0
    inet 10.5.0.2/16 scope global x168099842
       valid_lft forever preferred_lft forever
    inet6 fe80::8652:b7ec:98c0:80d6/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

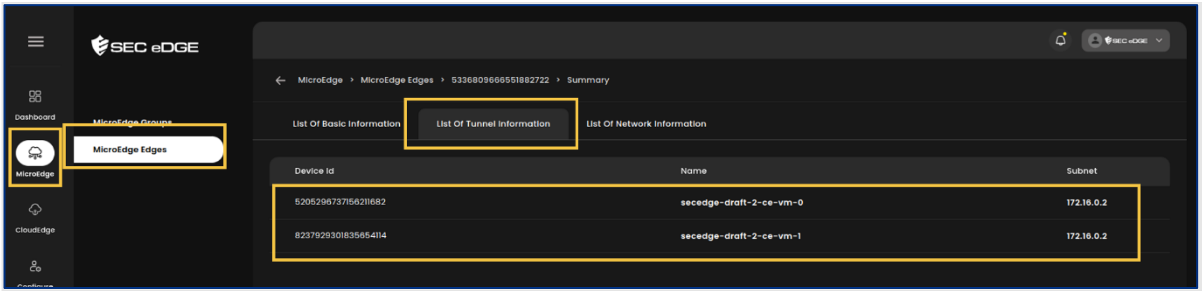
Figure 35 MicroEdge Terminal Listing Two Tunnels

5. On the SecEdge Studio User Interface, see the MicroEdge with multiple tunnels.

   + Select MicroEdge and Edges on the page left side.

   + Select the MicroEdge instance that you configured.

   + Click on List of Tunnel Information and notice the two routes, shown in Figure 36.


SEC eDGE
Dashboard
MicroEdge
CloudEdge
Configure
MicroEdge Groups
MicroEdge Edges
MicroEdge › MicroEdge Edges › 5336809666551882722 › Summary
List Of Basic Information
List Of Tunnel Information
List Of Network Information

Device Id	Name	Subnet
5205296737156211682	secedge-draft-2-ce-vm-0	172.16.0.2
8237929301835654114	secedge-draft-2-ce-vm-1	172.16.0.2

Figure 36 MicroEdge List of Tunnel Information

8.6. START WEB APPLICATION SERVERS

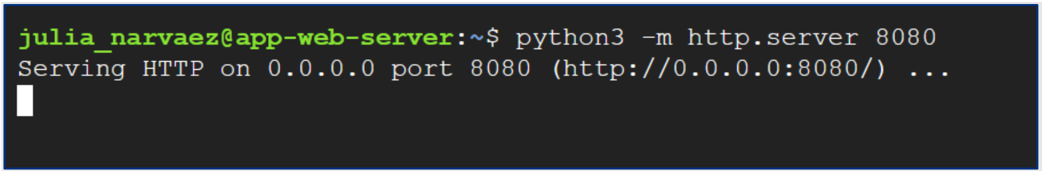
Start web server application in app-web-server and app-web-server-1.

app-web-server VM

1. SSH to the app-web-server VM created in 8.2 Create Two Web Servers.

2. Execute command to run the server, shown in Figure 37.

```
python3 -m http.server 8080
```



```
julia_narvaez@app-web-server:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

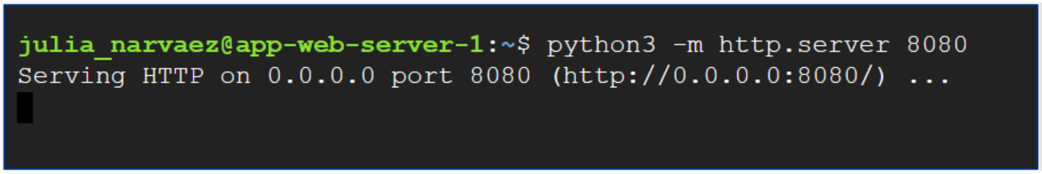
Figure 37 http server on app-web-server

app-web-server VM-1

3. SSH to the app-web-server-1 VM

4. Execute command to run the server, shown in Figure 38.

```
python3 -m http.server 8080
```



```
julia_narvaez@app-web-server-1:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

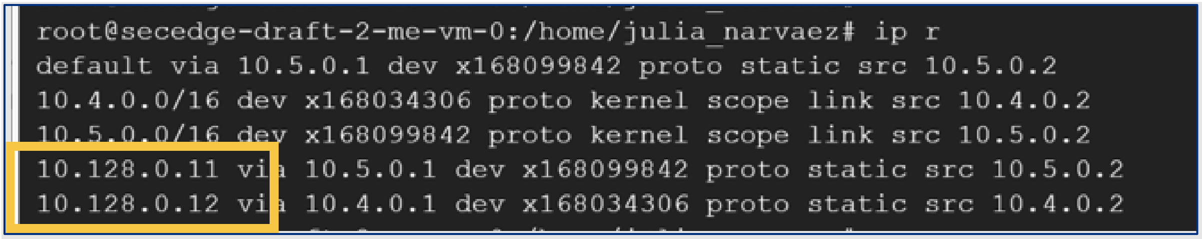
Figure 38 http server on app-web-server -1

8.7. SEND REQUESTS TO APP WEB SERVERS FROM MICROEDGE VM

From the MicroEdge VM, send requests to both app web servers.

1. Connect to the MicroEdge VM, see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.

2. Run ip r commands to confirm that the Internal IP of app-web-server-1 is added to the routing table. Figure 39 shows app-web-server and app-web-server-1 Internal IP addresses.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# ip r
default via 10.5.0.1 dev x168099842 proto static src 10.5.0.2
10.4.0.0/16 dev x168034306 proto kernel scope link src 10.4.0.2
10.5.0.0/16 dev x168099842 proto kernel scope link src 10.5.0.2
10.128.0.11 via 10.5.0.1 dev x168099842 proto static src 10.5.0.2
10.128.0.12 via 10.4.0.1 dev x168034306 proto static src 10.4.0.2
```

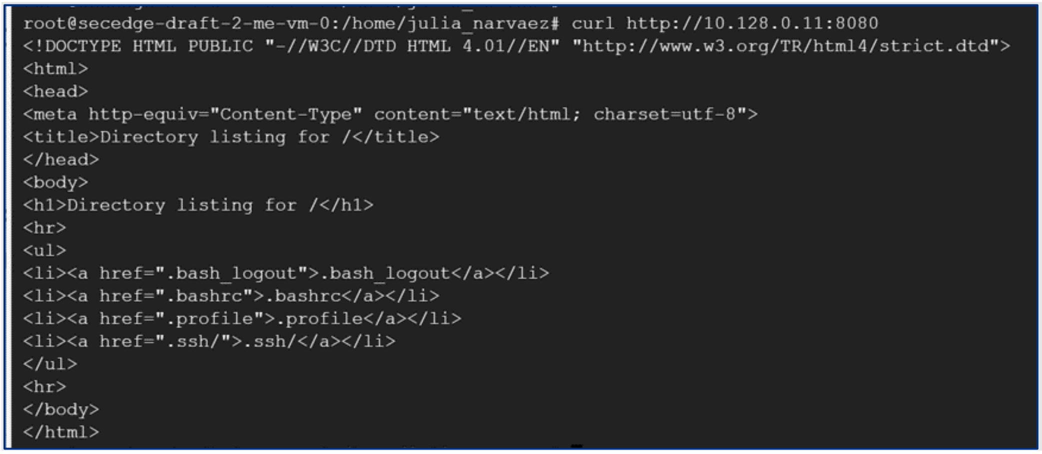
Figure 39 MicroEdge Multiple Tunnels

3. Send requests to the app-web-server.

   + Run the curl command

```
curl http://< Internal IP of app-web-server>:8080
```

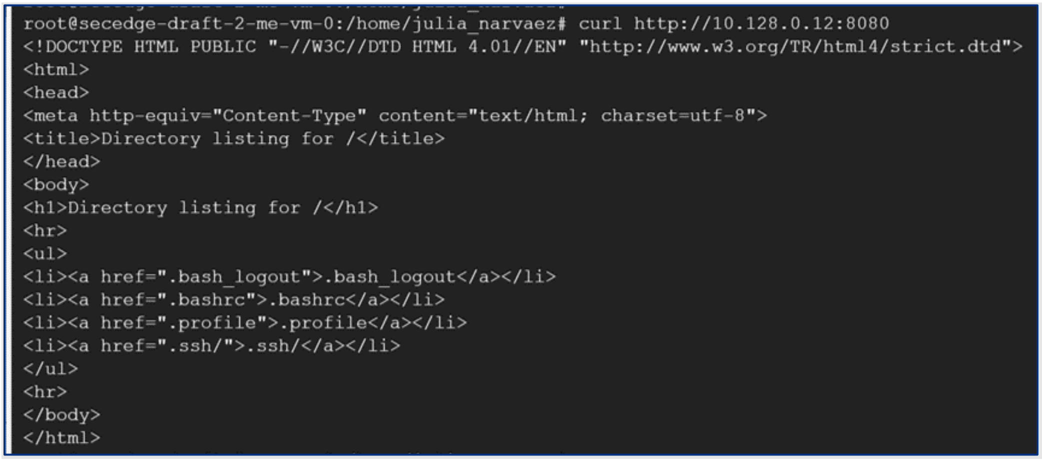
- The MicroEdge VM receives in return the directory listing, via the first tunnel.
- Figure 40 illustrates the execution of curl http://10.128.0.11:8080, where 10.128.0.11 is the internal IP of app-web-server, as shown in Figure 27 Google Cloud, VM Instances, App Web Server VM Instances.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# curl http://10.128.0.11:8080
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bashrc">.bashrc</a></li>
<li><a href=".profile">.profile</a></li>
<li><a href=".ssh/">.ssh/</a></li>
</ul>
<hr>
</body>
</html>
```

Figure 40 MicroEdge Request to app-web-server

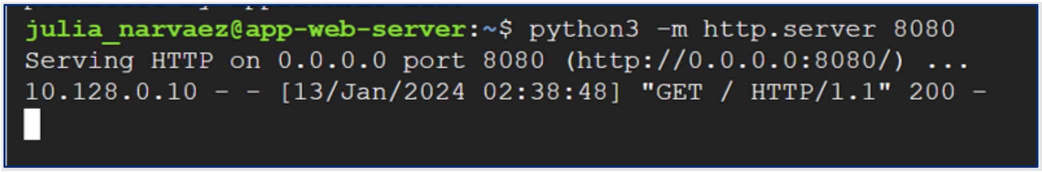
4. Send requests to the app-web-server-1.
   - Run the curl command
   - The MicroEdge VM receives in return the directory listing, via the second tunnel.
   - Figure 41 illustrates the execution of curl http://10.128.0.12:8080, where 10.128.0.12 is the internal IP of app-web-server-1, as shown in Figure 27 Google Cloud, VM Instances, App Web Server VM Instances



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# curl http://10.128.0.12:8080
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bashrc">.bashrc</a></li>
<li><a href=".profile">.profile</a></li>
<li><a href=".ssh/">.ssh/</a></li>
</ul>
<hr>
</body>
</html>
```

Figure 41 MicroEdge Request to app-web-server-1

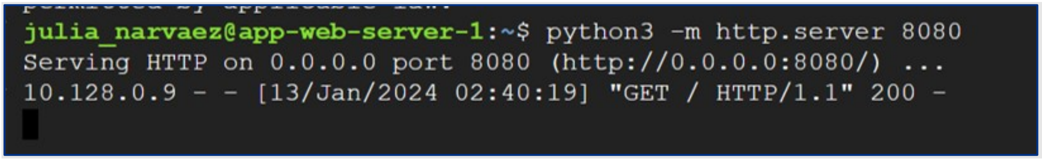
5. Verify that app-web-server and app-web-server-1 received requests from two different CloudEdge devices.
   - Figure 42 shows request from one CloudEdge.



```
julia_narvaez@app-web-server:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.128.0.10 - - [13/Jan/2024 02:38:48] "GET / HTTP/1.1" 200 -
```

Figure 42 app-web-server Received Request

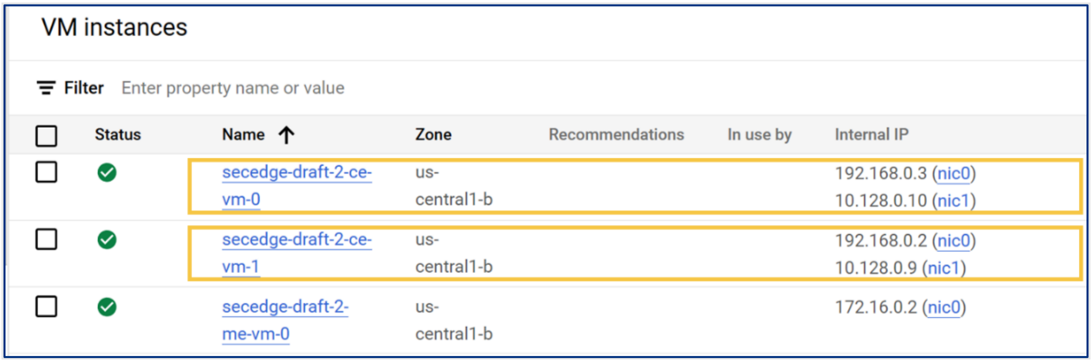
- Figure 43 shows request from the other CloudEdge.



```
julia_narvaez@app-web-server-1:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.128.0.9 - - [13/Jan/2024 02:40:19] "GET / HTTP/1.1" 200 -
```

Figure 43 app-web-server-1 Received Request

- Figure 44 shows that the address in the requests received by the app web servers correspond to the Internal Ip addresses of the CloudEdge VMs.



VM instances

Filter Enter property name or value

□	Status	Name ↑	Zone	Recommendations	In use by	Internal IP
□	✓	secedge-draft-2-ce-vm-0	us-central1-b			192.168.0.3 (nic0) 10.128.0.10 (nic1)
□	✓	secedge-draft-2-ce-vm-1	us-central1-b			192.168.0.2 (nic0) 10.128.0.9 (nic1)
□	✓	secedge-draft-2-me-vm-0	us-central1-b			172.16.0.2 (nic0)

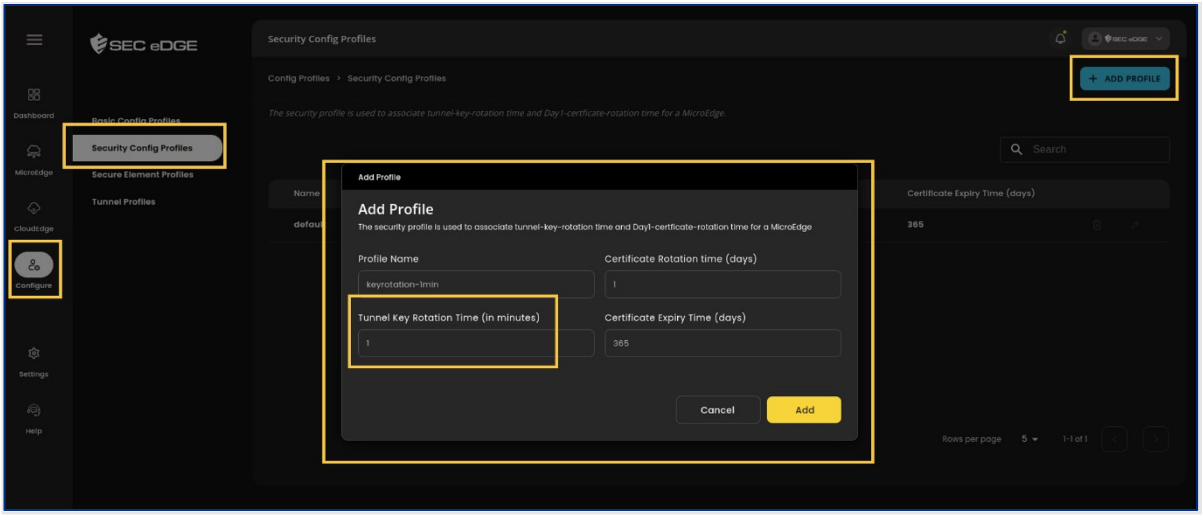
Figure 44 Google Cloud, VM Instances, CloudEdge VMs Deployed in 8.1

9. TEST TUNNEL KEY ROTATION

9.1. CREATE A NEW SECURITY CONFIG PROFILE

In the SecEdge User Interface, create new Security Config Profiles in which the Tunnel Key Rotation Time is set to 1.

- Select Configure and Security Config Profiles on the page left side and click on Add Profile.
- Enter the Profile Name, in the example is keyRotation-1Min.
- Enter Tunnel Key Rotation Time: 1
- Enter additional data and click on the Add button, shown in Figure 45.



Security Config Profiles

Config Profiles > Security Config Profiles

The security profile is used to associate tunnel-key-rotation time and Day1-certficate-rotation time for a MicroEdge.

Name	Certificate Expiry Time (days)
defau	365

Add Profile

Add Profile

The security profile is used to associate tunnel-key-rotation time and Day1-certficate-rotation time for a MicroEdge

Profile Name: keyrotation-1min

Certificate Rotation time (days): 1

Tunnel Key Rotation Time (in minutes): 1

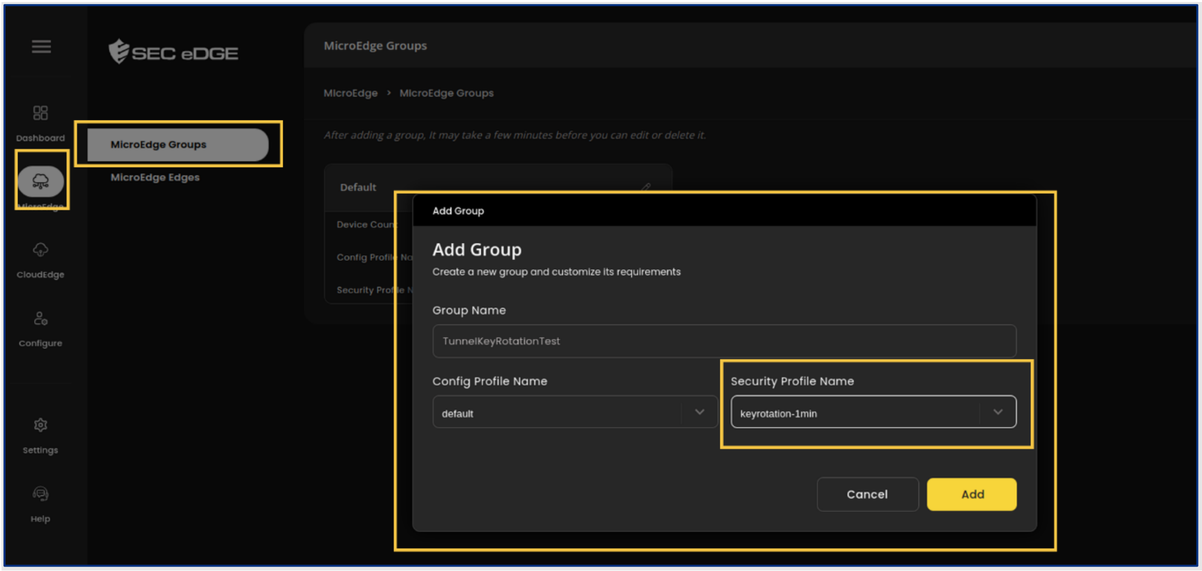
Certificate Expiry Time (days): 365

Figure 45 SecEdge User Interface Add Security Config Profile

9.2. CREATE A NEW MICROEDGE GROUP

In the SecEdge User Interface, create a new MicroEdge Group which has assigned the Security Profile with one minute key rotation time created in the previous step.

- Select MicroEdge and Groups on the page left side and click on Add Group.
- Enter the Group Name, in the example is TunnelKeyRotationTest.
- Select keyRotation-1Min in the Security Profile Name drop down.
- Enter additional data and click on the Add button, shown in Figure 46.



MicroEdge Groups

MicroEdge > MicroEdge Groups

After adding a group, It may take a few minutes before you can edit or delete it.

Add Group

Add Group

Create a new group and customize its requirements

Group Name: TunnelKeyRotationTest

Config Profile Name: default

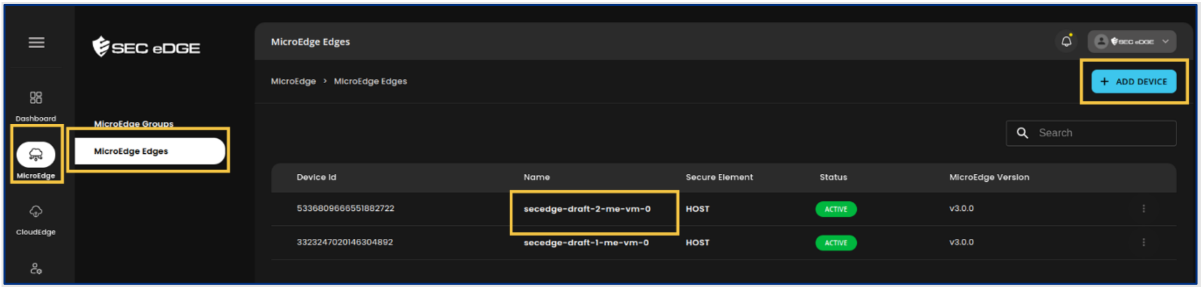
Security Profile Name: keyrotation-1min

Figure 46 SecEdge User Interface Add MicroEdge Group

9.3. ADD A MICROEDGE DEVICE TO A GROUP

1. Select a MicroEdge

   - Select MicroEdge and Edges on the page left side.
   - From the list, choose a device, which becomes the MicroEdge instance under test.
   - Copy or take note of the device Name and Id.

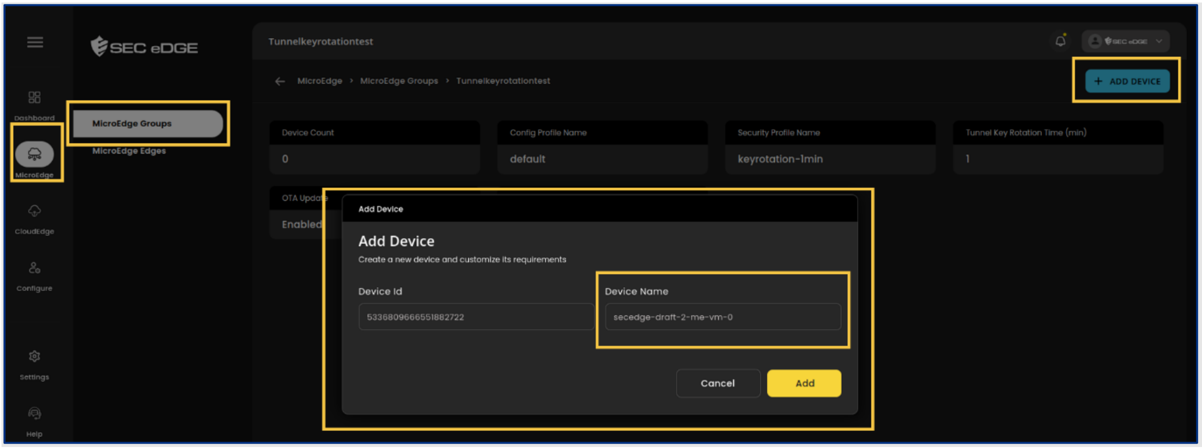


Device Id	Name	Secure Element	Status	MicroEdge Version
5336809666551882722	secedge-draft-2-me-vm-0	HOST	ACTIVE	v3.0.0
3323247020146304892	secedge-draft-1-me-vm-0	HOST	ACTIVE	v3.0.0

Figure 47 SecEdge User Interface Select Device

2. Add the MicroEdge instance under test to the TunnelKeyRotationTest MicroEdge Group.

   - Select MicroEdge and Groups on the page left side.
   - Select TunnelKeyRotationTest MicroEdge Group and click on Add Device.
   - Enter or paste the Device Name copied in the previous step.
   - Enter or paste Device Id.



Device Count: 0
Config Profile Name: default
Security Profile Name: keyrotation-1min
Tunnel Key Rotation Time (min): 1
OTA Update: Enabled

Add Device
Create a new device and customize its requirements
Device Id: 5336809666551882722
Device Name: secedge-draft-2-me-vm-0

Figure 48 SecEdge User Interface Add MicroEdge Device to Group

9.4. VIEW TUNNEL KEY ROTATION

Execute the following steps in the MicroEdge terminal.

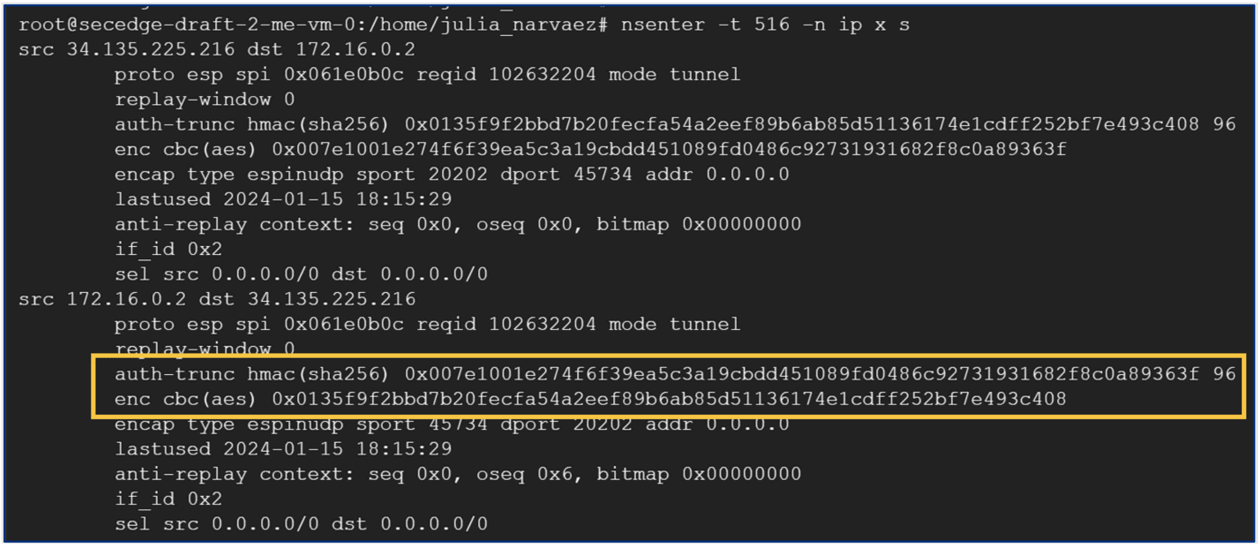
1. Access to the MicroEdge VM you selected for the test, see 12.1.1 Guide to Connect to MicroEdge VM Serial Console.
2. Identify the MicroEdge process id and execute the nsenter command as superuser:

```
ps aux | grep microedge

nsenter -t <microedge_pid> -n ip x s
```

3. Wait for 1 minute, run the same commands again.
4. Verify that the tunnel keys have been changed.

The following screenshots show the sequence.

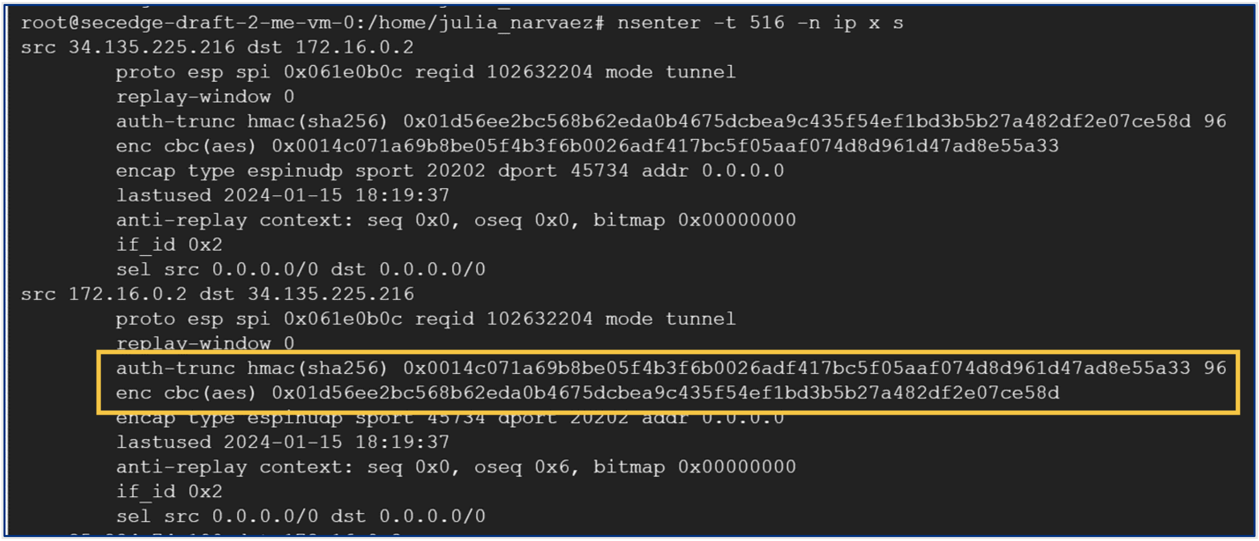
Figure 49 shows the keys at one point in time.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# nsenter -t 516 -n ip x s
src 34.135.225.216 dst 172.16.0.2
        proto esp spi 0x061e0b0c reqid 102632204 mode tunnel
        replay-window 0
        auth-trunc hmac(sha256) 0x0135f9f2bbd7b20fecfa54a2eef89b6ab85d51136174e1cdff252bf7e493c408 96
        enc cbc(aes) 0x007e1001e274f6f39ea5c3a19cbdd451089fd0486c92731931682f8c0a89363f
        encap type espinudp sport 20202 dport 45734 addr 0.0.0.0
        lastused 2024-01-15 18:15:29
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        if_id 0x2
        sel src 0.0.0.0/0 dst 0.0.0.0/0
src 172.16.0.2 dst 34.135.225.216
        proto esp spi 0x061e0b0c reqid 102632204 mode tunnel
        replay-window 0
        auth-trunc hmac(sha256) 0x007e1001e274f6f39ea5c3a19cbdd451089fd0486c92731931682f8c0a89363f 96
        enc cbc(aes) 0x0135f9f2bbd7b20fecfa54a2eef89b6ab85d51136174e1cdff252bf7e493c408
        encap type espinudp sport 45734 dport 20202 addr 0.0.0.0
        lastused 2024-01-15 18:15:29
        anti-replay context: seq 0x0, oseq 0x6, bitmap 0x00000000
        if_id 0x2
        sel src 0.0.0.0/0 dst 0.0.0.0/0
```

Figure 49 MicroEdge Terminal at an Initial Point in Time

Figure 50 shows the keys have changed after waiting for one minute.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# nsenter -t 516 -n ip x s
src 34.135.225.216 dst 172.16.0.2
        proto esp spi 0x061e0b0c reqid 102632204 mode tunnel
        replay-window 0
        auth-trunc hmac(sha256) 0x01d56ee2bc568b62eda0b4675dcbea9c435f54ef1bd3b5b27a482df2e07ce58d 96
        enc cbc(aes) 0x0014c071a69b8be05f4b3f6b0026adf417bc5f05aaf074d8d961d47ad8e55a33
        encap type espinudp sport 20202 dport 45734 addr 0.0.0.0
        lastused 2024-01-15 18:19:37
        anti-replay context: seq 0x0, oseq 0x0, bitmap 0x00000000
        if_id 0x2
        sel src 0.0.0.0/0 dst 0.0.0.0/0
src 172.16.0.2 dst 34.135.225.216
        proto esp spi 0x061e0b0c reqid 102632204 mode tunnel
        replay-window 0
        auth-trunc hmac(sha256) 0x0014c071a69b8be05f4b3f6b0026adf417bc5f05aaf074d8d961d47ad8e55a33 96
        enc cbc(aes) 0x01d56ee2bc568b62eda0b4675dcbea9c435f54ef1bd3b5b27a482df2e07ce58d
        encap type espinudp sport 45734 dport 20202 addr 0.0.0.0
        lastused 2024-01-15 18:19:37
        anti-replay context: seq 0x0, oseq 0x6, bitmap 0x00000000
        if_id 0x2
        sel src 0.0.0.0/0 dst 0.0.0.0/0
```

Figure 50 MicroEdge Terminal One Minute after the Initial Point in Time

10. TEST MQTT CERTIFICATE ROTATION

In the SecEdge User Interface, the Security Config Profile allows you to set the MicroEdge and CloudEdge device certificate rotation time. You can also rotate the device certificate by selecting Rotate Certs in the list options of MicroEdge Edges. For this test, you can force the rotation of a MicroEdge certificate by changing the MicroEdge Group.

1. Select a MicroEdge for testing.

2. Connect to the MicroEdge VM you selected for the test, see 12.1.1 Guide to Connect to MicroEdge VM Serial Console..

3. In the MicroEdge terminal:

   + Use the IPSec command to view current tunnel keys. If you executed it before, there is no need to run it again.

List the day1 certificate and take note the timestamp and look at its content.

```
ls -l /etc/softse.d/day1/net-edge.cert

cat /etc/softse.d/day1/net-edge.cert
```

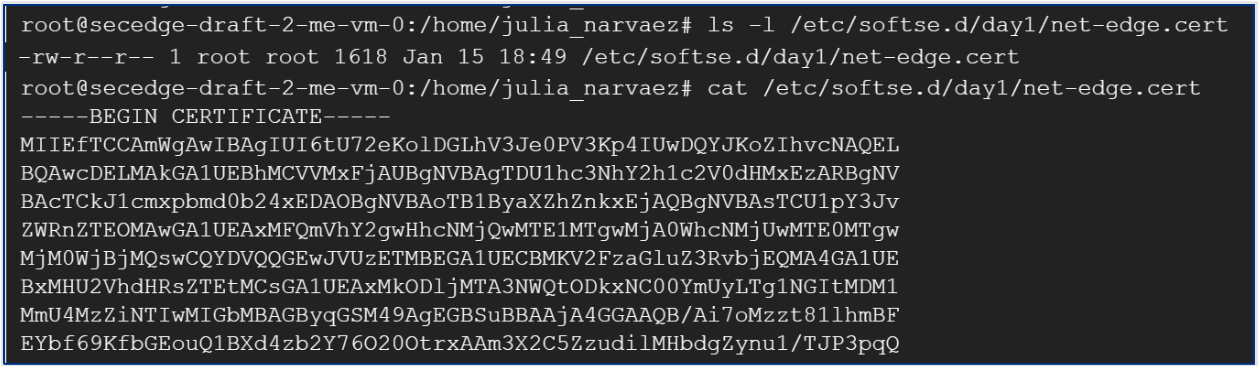
4. Force certificate rotation by changing MicroEdge Group.

   + In the SecEdge User Interface, follow the same steps as in 9.3 Add a MicroEdge Device to a Group to add the selected MicroEdge to a different group.

5. Verify in the MicroEdge terminal the certificate change.

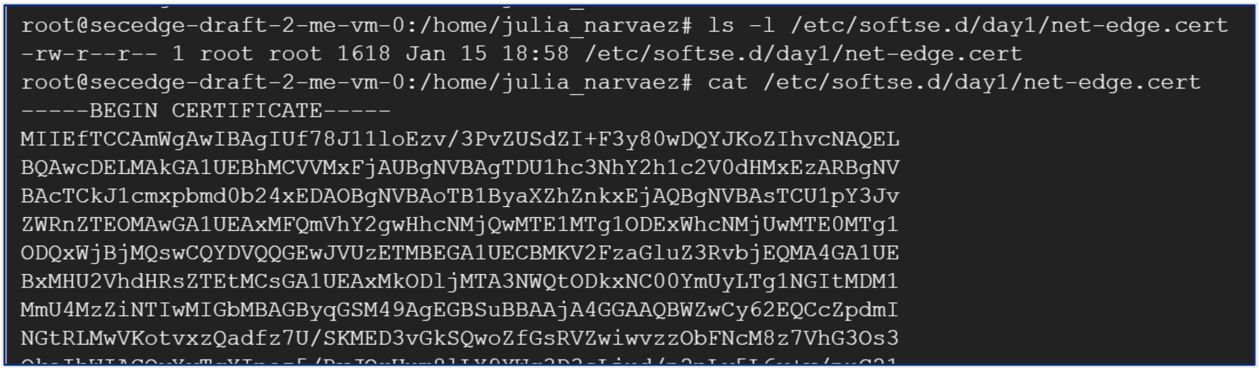
- In the terminal, run the same commands to view the Day1 certificate.
- Verify that the certificate timestamp and its content have changed.

Figure 51 shows the Day1 certificate before the MicroEdge Group change. Figure 52 shows the Day1 certificate after the MicroEdge Group update. See that the certificate timestamp and content have changed.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# ls -l /etc/softse.d/day1/net-edge.cert
-rw-r--r-- 1 root root 1618 Jan 15 18:49 /etc/softse.d/day1/net-edge.cert
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# cat /etc/softse.d/day1/net-edge.cert
-----BEGIN CERTIFICATE-----
MIIEfTCCAmWgAwIBAgIUI6tU72eKolDGLhV3Je0PV3Kp4IUwDQYJKoZIhvcNAQEL
BQAwcDELMAkGA1UEBhMCVVMxFjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEzARBgNV
BAcTCkJ1cmxpbmd0b24xEDAOBgNVBAoTB1ByaXZhZnkxEjAQBgNVBAsTCU1pY3Jv
ZWRnZTEOMAwGA1UEAxMFQmVhY2gwHhcNMjQwMTE1MTgwMjA0WhcNMjUwMTE0MTgw
MjM0WjBjMQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UE
BxMHU2VhdHRsZTEtMCsGA1UEAxMkODljMTA3NWQtODkxNC00YmUyLTg1NGItMDM1
MmU4MzZiNTIwMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQB/Ai7oMzzt81lhmBF
EYbf69KfbGEouQ1BXd4zb2Y76O20OtrxAAm3X2C5ZzudilMHbdgZynu1/TJP3pqQ
```

Figure 51 MicroEdge Day1 Certificate Before Group Change

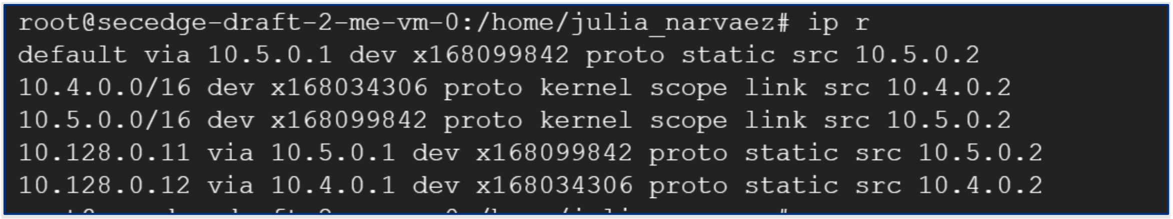


```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# ls -l /etc/softse.d/day1/net-edge.cert
-rw-r--r-- 1 root root 1618 Jan 15 18:58 /etc/softse.d/day1/net-edge.cert
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# cat /etc/softse.d/day1/net-edge.cert
-----BEGIN CERTIFICATE-----
MIIEfTCCAmWgAwIBAgIUf78J11loEzv/3PvZUSdZI+F3y80wDQYJKoZIhvcNAQEL
BQAwcDELMAkGA1UEBhMCVVMxFjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxEzARBgNV
BAcTCkJ1cmxpbmd0b24xEDAOBgNVBAoTB1ByaXZhZnkxEjAQBgNVBAsTCU1pY3Jv
ZWRnZTEOMAwGA1UEAxMFQmVhY2gwHhcNMjQwMTE1MTg1ODExWhcNMjUwMTE0MTg1
ODQxWjBjMQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UE
BxMHU2VhdHRsZTEtMCsGA1UEAxMkODljMTA3NWQtODkxNC00YmUyLTg1NGItMDM1
MmU4MzZiNTIwMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBWZwCy62EQCcZpdmI
NGtRLMwVKotvxzQadfz7U/SKMED3vGkSQwoZfGsRVZwiwvzzObFNcM8z7VhG3Os3
```

Figure 52 MicroEdge Day1 Certificate After Group Change

11. TEST ROUTING TABLE

1. Connect to a MicroEdge VM you selected for the test, 12.1.1 Guide to Connect to MicroEdge VM Serial Console.
2. Execute commands such as
    - ip r
    - route
3. Verify that all routings to external are via XFRM interfaces. Figure 53 shows the existing interfaces.



```
root@secedge-draft-2-me-vm-0:/home/julia_narvaez# ip r
default via 10.5.0.1 dev x168099842 proto static src 10.5.0.2
10.4.0.0/16 dev x168034306 proto kernel scope link src 10.4.0.2
10.5.0.0/16 dev x168099842 proto kernel scope link src 10.5.0.2
10.128.0.11 via 10.5.0.1 dev x168099842 proto static src 10.5.0.2
10.128.0.12 via 10.4.0.1 dev x168034306 proto static src 10.4.0.2
```

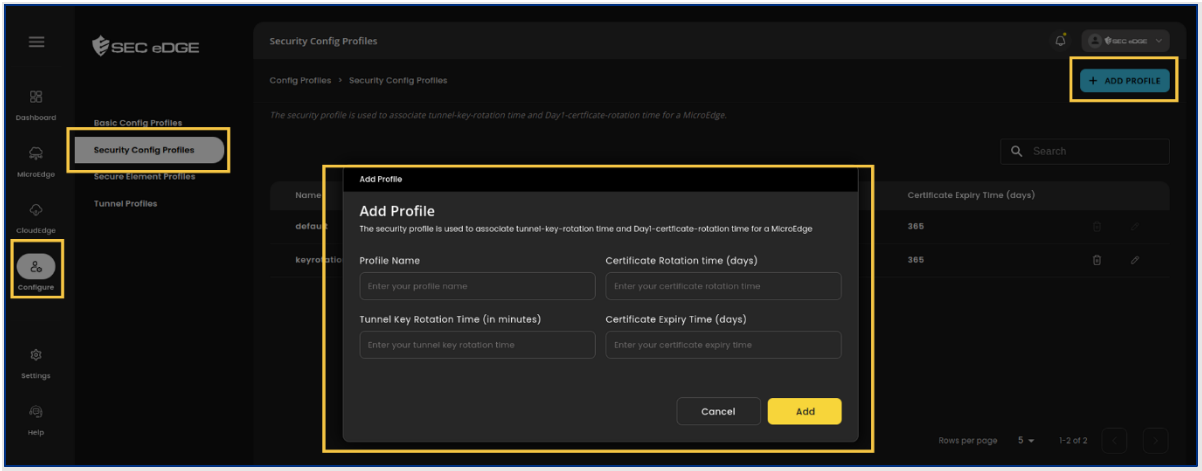
Figure 53 MicroEdge Routing

12. TEST ADDITIONAL SECURITY PARAMETERS

Configure MicroEdge And CloudEdge security parameters. Refer to the SecEdge User Guide to configure security profiles such as:

- Tunnel Key Rotation Time
- Certificate Expiry Time

Open SecEdge User Interface and tunnel security parameters to change the behavior. Note that the default profile is not editable. To test, for example, create a new security profile, new MicroEdge group and add MicroEdge instance to that group. Change the tunnel key rotation and certificate rotation time. Figure 54 shows the page to add a security configuration profile.



The security profile is used to associate tunnel-key-rotation time and Day1-certficate-rotation time for a MicroEdge.

Name	Certificate Expiry Time (days)
defau	365
keyrotatio	365

Rows per page 5 1-2 of 2

Add Profile

Add Profile

The security profile is used to associate tunnel-key-rotation time and Day1-certficate-rotation time for a MicroEdge

Profile Name: Enter your profile name

Certificate Rotation time (days): Enter your certificate rotation time

Tunnel Key Rotation Time (in minutes): Enter your tunnel key rotation time

Certificate Expiry Time (days): Enter your certificate expiry time

Figure 54 SecEdge User Interface Add Security Configuration Profile

12.1.1. GUIDE TO CONNECT TO MICROEDGE VM SERIAL CONSOLE

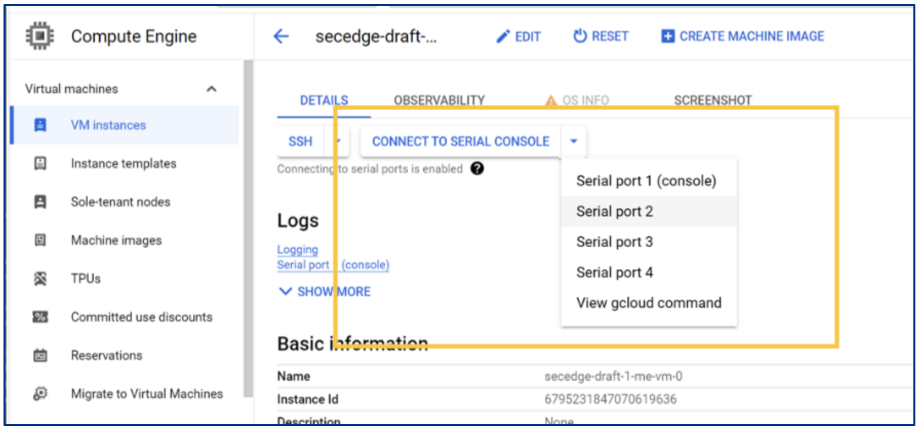
Using the MicroEdge VM serial console is the recommended connection in this tutorial. When accessing the MicroEdge VM through its serial console, the system is in the init namespace and the virtual interfaces are available. This section explains how to connect using the browser or the gcloud cli shell, and how to find credentials to access the MicroEdge VM serial console.

CONNECT FROM BROWSER

In the Google Cloud **VM instances** section, **DETAILS** page, Serial port 2 or View gcloud command are the recommended options to access the MicroEdge VM. MicroEdge is running on the foreground with the highest logging level. Serial port 1 console prints the log messages and it is not suitable for interacting and running shell commands.

To access from the browser, In the Google Cloud **VM instances** section, **DETAILS** page, do the following:

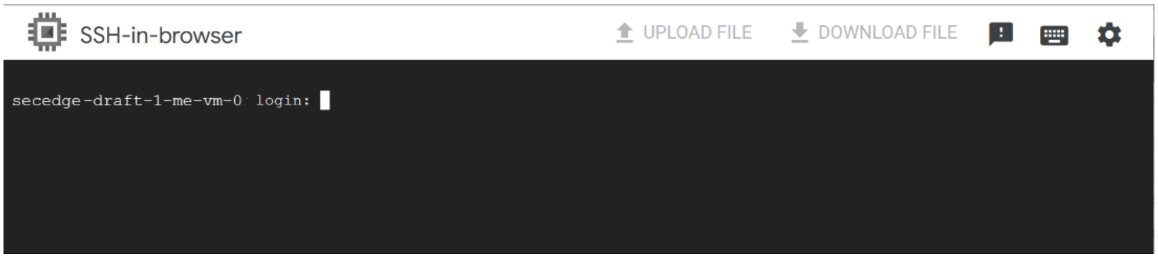
1. Click on the CONNECT TO SERIAL CONSOLE drop down menu, Figure 55.



Name secedge-draft-1-me-vm-0
Instance Id 6795231847070619636
Description None

Figure 55 Google Cloud, VM Instances, CONNECT TO SERIAL CONSOLE Options

2. If using the browser with serial port 2, click on the Serial port 2 option, authorize Cloud Shell if needed, and press enter on the browser window to see the login prompt, Figure 56.



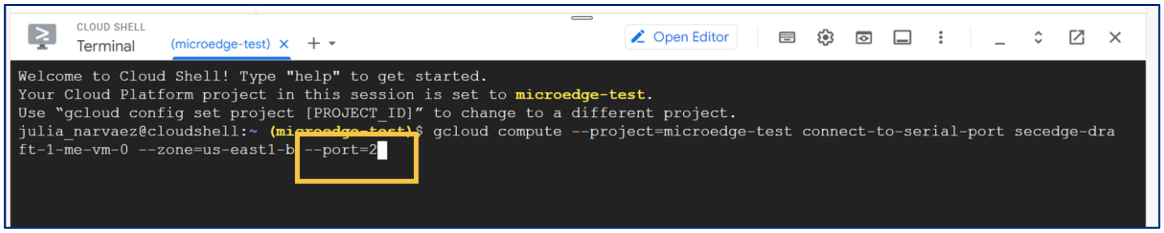
```
secedge-draft-1-me-vm-0 login:
```

Figure 56 MicroEdge Serial Console Login

3. Continue to **Log into Ubuntu** steps listed later in this section.

Alternatively, if using View gcloud command:

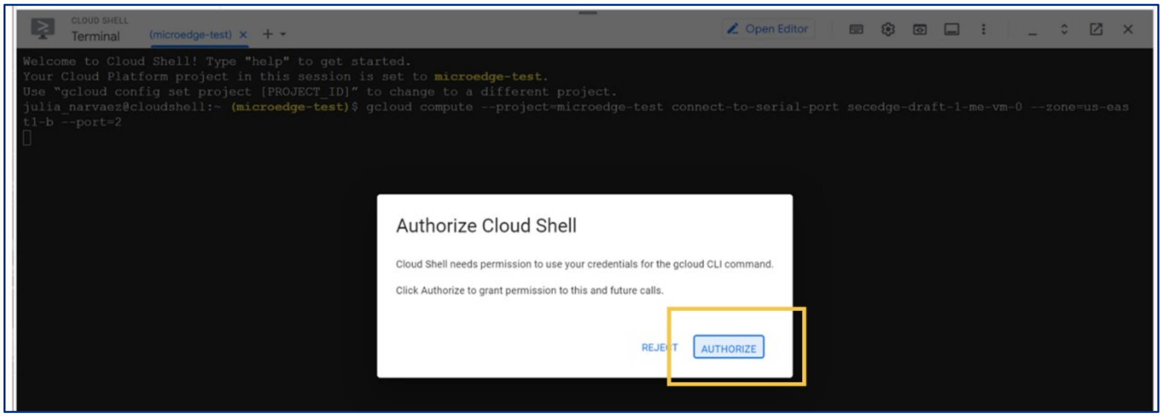
+ click on View gcloud command, copy the command, paste it in the terminal and add the **--port=2** flag, Figure 57.



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to microedge-test.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud compute --project=microedge-test connect-to-serial-port secedge-dra
ft-1-me-vm-0 --zone=us-east1-b --port=2
```

Figure 57 Cloud Shell Terminal Connect To Serial Port Command

- Press Enter when the new side bar opens and authorize Cloud Shell to use your credentials for the gcloud CLI command, Figure 58.



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to microedge-test.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud compute --project=microedge-test connect-to-serial-port secedge-draft-1-me-vm-0 --zone=us-eas
t1-b --port=2
```

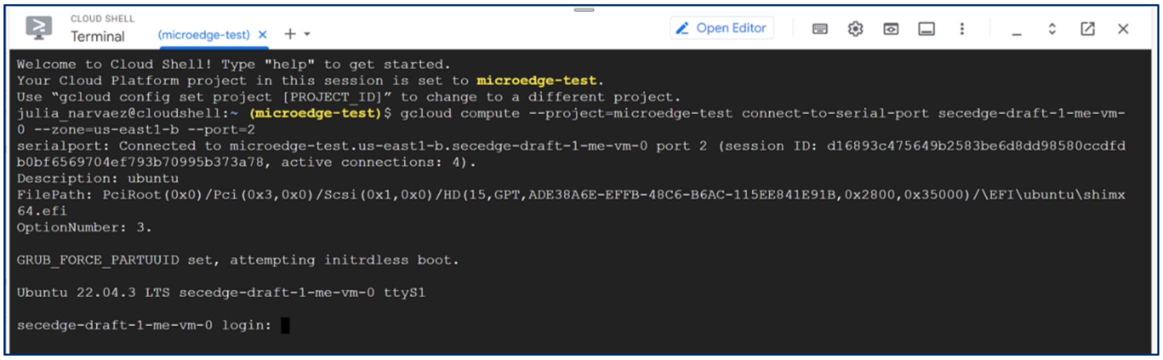
Authorize Cloud Shell

Cloud Shell needs permission to use your credentials for the gcloud CLI command.

Click Authorize to grant permission to this and future calls.

Figure 58 Cloud Shell Authorization

- When the command succeeds, the login information is requested, Figure 59.



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to microedge-test.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud compute --project=microedge-test connect-to-serial-port secedge-draft-1-me-vm-
0 --zone=us-east1-b --port=2
serialport: Connected to microedge-test.us-east1-b.secedge-draft-1-me-vm-0 port 2 (session ID: d16893c475649b2583be6d8dd98580ccdfd
b0bf6569704ef793b70995b373a78, active connections: 4).
Description: ubuntu
FilePath: PciRoot(0x0)/Pci(0x3,0x0)/Scsi(0x1,0x0)/HD(15,GPT,ADE38A6E-EFFB-48C6-B6AC-115EE841E91B,0x2800,0x35000)/\EFI\ubuntu\shimx
64.efi
OptionNumber: 3.

GRUB_FORCE_PARTUUID set, attempting initrdless boot.

Ubuntu 22.04.3 LTS secedge-draft-1-me-vm-0 ttyS1

secedge-draft-1-me-vm-0 login:
```

Figure 59 Cloud Shell Success and Login Prompt

If you encounter errors because your gcloud user account, please see 14 Accessing Serial Terminal Troubleshooting in this document for troubleshooting ideas.

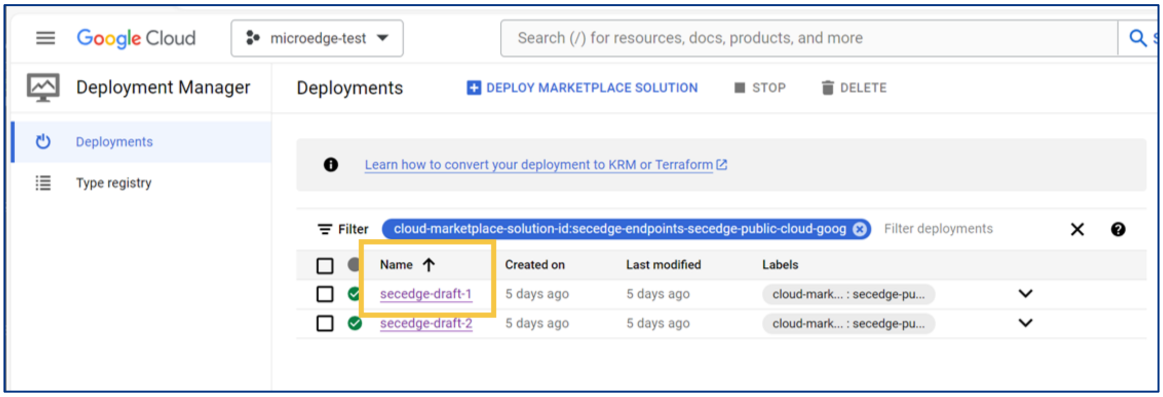
LOG INTO UBUNTU

The username and password are on the **Deployment Manager**, **Deployments** page. The password is also on the **VM instances DETAILS** page. The username is the same across deployments, ubuntu. The password is unique for every deployment.

PLEASE NOTE THAT SECeDGE™ RESERVES THE RIGHT TO CHANGE THE CONTENT OF THE DOCUMENT AS FEATURES EVOLVE OR NEW IMPROVEMENTS ARE ADDED

4. Identify the serial console password on one of the two following locations.

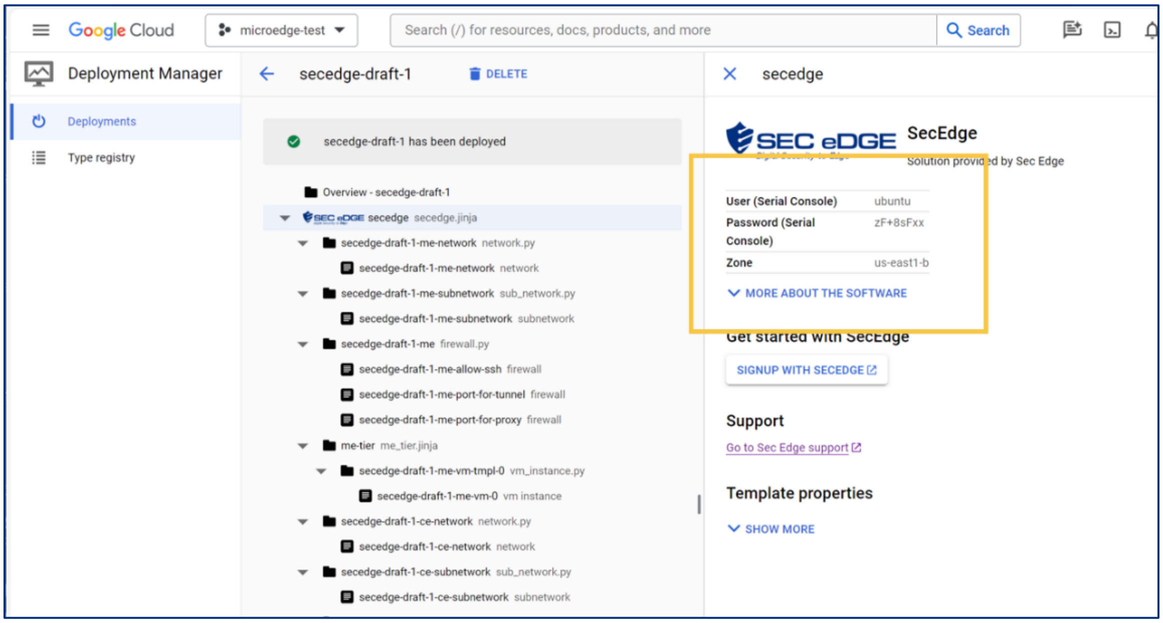
   - From the **Deployment Manager** section, Figure 60, click on the deployment name to which the MicroEdge VM belongs.


Google Cloud
microedge-test
Search (/) for resources, docs, products, and more
Deployment Manager
Deployments
DEPLOY MARKETPLACE SOLUTION
STOP
DELETE
Deployments
Type registry
Learn how to convert your deployment to KRM or Terraform
Filter
cloud-marketplace-solution-id:secedge-endpoints-secedge-public-cloud-goog
Filter deployments

Name ↑	Created on	Last modified	Labels
secedge-draft-1	5 days ago	5 days ago	cloud-mark... : secedge-pu...
secedge-draft-2	5 days ago	5 days ago	cloud-mark... : secedge-pu...

Figure 60 Google Cloud, Deployments Manager, Deployments page

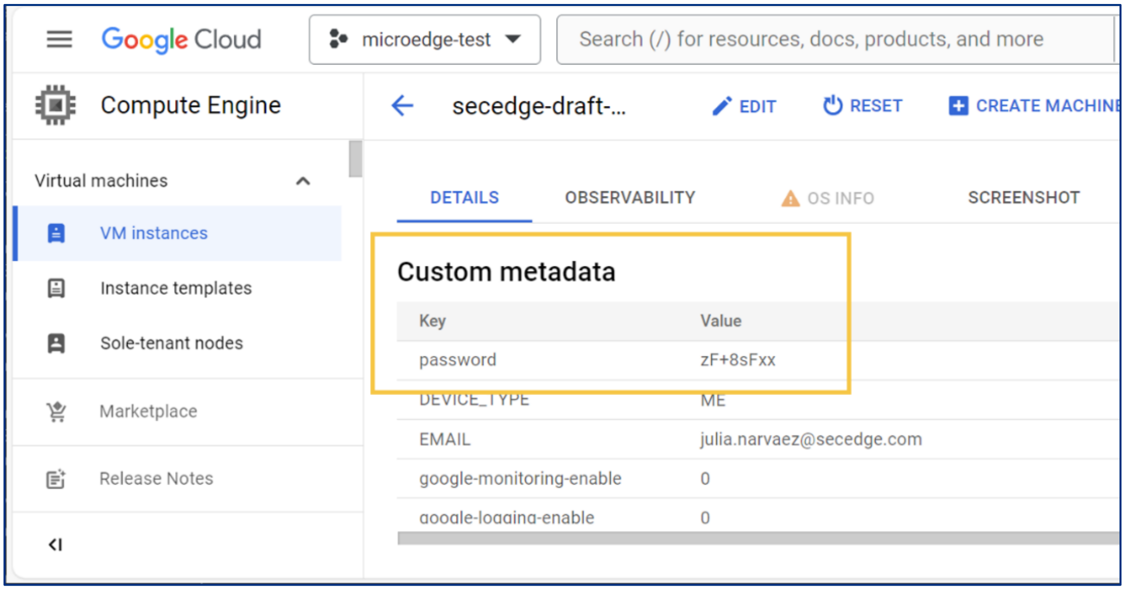
Note that the user is ubuntu. Take note of the password, shown in Figure 61.


Google Cloud
microedge-test
Search (/) for resources, docs, products, and more
Search
Deployment Manager
secedge-draft-1
DELETE
Deployments
Type registry
secedge-draft-1 has been deployed
Overview - secedge-draft-1
secedge secedge.jinja
secedge-draft-1-me-network network.py
secedge-draft-1-me-network network
secedge-draft-1-me-subnetwork sub_network.py
secedge-draft-1-me-subnetwork subnetwork
secedge-draft-1-me firewall.py
secedge-draft-1-me-allow-ssh firewall
secedge-draft-1-me-port-for-tunnel firewall
secedge-draft-1-me-port-for-proxy firewall
me-tier me_tier.jinja
secedge-draft-1-me-vm-tmpl-0 vm_instance.py
secedge-draft-1-me-vm-0 vm instance
secedge-draft-1-ce-network network.py
secedge-draft-1-ce-network network
secedge-draft-1-ce-subnetwork sub_network.py
secedge-draft-1-ce-subnetwork subnetwork
secedge
SecEdge
Solution provided by Sec Edge
MORE ABOUT THE SOFTWARE
Get started with SecEdge
SIGNUP WITH SECEDGE
Support
Go to Sec Edge support
Template properties
SHOW MORE

User (Serial Console)	ubuntu
Password (Serial Console)	zF+8sFxx
Zone	us-east1-b

Figure 61 Google Cloud, Deployments Manager, Selected Deployment page

   - Alternatively, on the **VM instances DETAILS** page, scroll down to the Custom metadata section by the bottom of the page where the VM password is displayed, Figure 62.

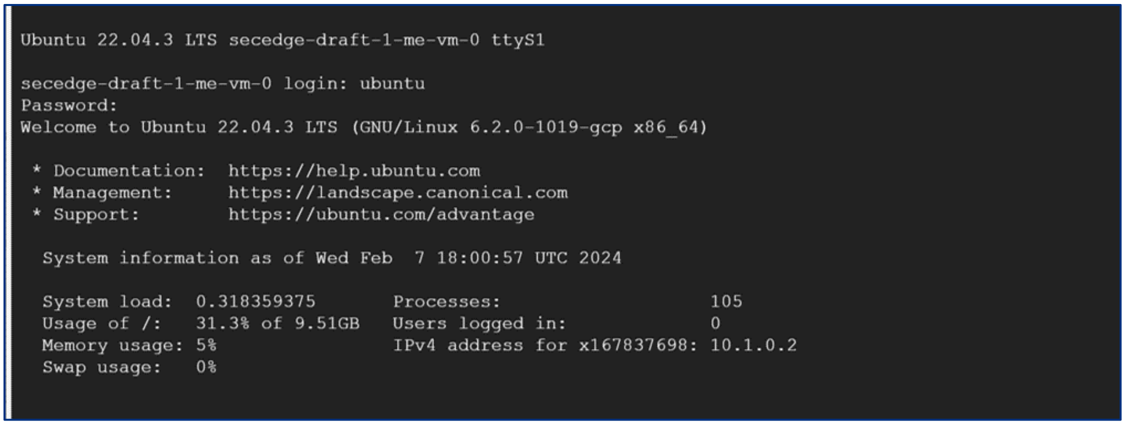


Custom metadata

Key	Value
password	zF+8sFxx
DEVICE_TYPE	ME
EMAIL	julia.narvaez@secedge.com
google-monitoring-enable	0
google-logging-enable	0

Figure 62 Google Cloud, VM instances, Details, Custom metadata

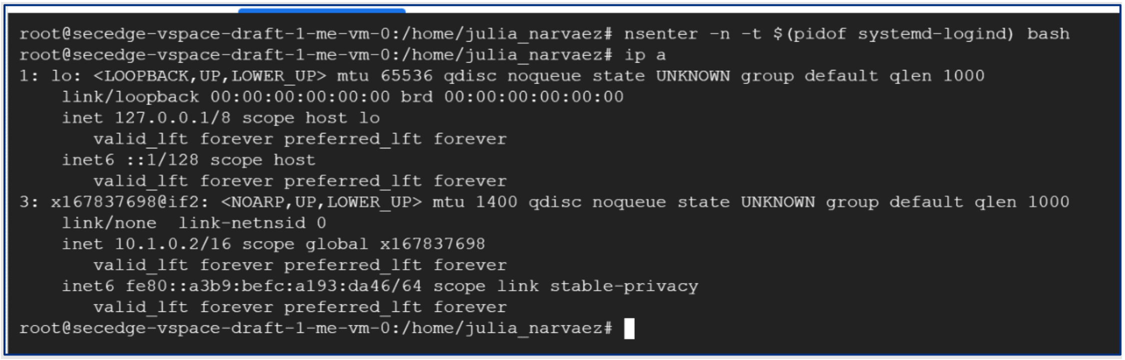
5. Enter the login and password when prompted, Figure 63.



```
Ubuntu 22.04.3 LTS secedge-draft-1-me-vm-0 ttyS1

secedge-draft-1-me-vm-0 login: ubuntu
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1019-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Feb  7 18:00:57 UTC 2024

  System load:  0.318359375       Processes:                105
  Usage of /:   31.3% of 9.51GB   Users logged in:          0
  Memory usage: 5%                IPv4 address for x167837698: 10.1.0.2
  Swap usage:   0%
```

Figure 63 Ubuntu Login

6. Execute ip a and notice the xfrm interface created by MicroEdge, Figure 64.



```
root@secedge-vspace-draft-1-me-vm-0:/home/julia_narvaez# nsenter -n -t $(pidof systemd-logind) bash
root@secedge-vspace-draft-1-me-vm-0:/home/julia_narvaez# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: x167837698@if2: <NOARP,UP,LOWER_UP> mtu 1400 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none  link-netnsid 0
    inet 10.1.0.2/16 scope global x167837698
       valid_lft forever preferred_lft forever
    inet6 fe80::a3b9:befc:a193:da46/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
root@secedge-vspace-draft-1-me-vm-0:/home/julia_narvaez# 
```

Figure 64 MicroEdge Terminal Window xfrm Interface

CONNECT FROM TERMINAL

This is an alternative way to access the serial terminal instead of connecting from browser.

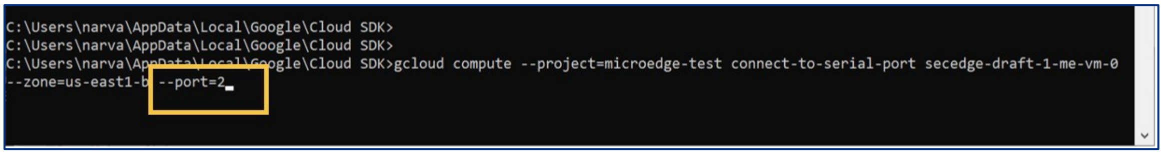
- Install gcloud cli in system https://cloud.google.com/sdk/docs/install.

  Execute the following command

```
gcloud compute --project=SecEdge-public connect-to-serial-port SecEdge-vspace-draft-1-me-vm-0 --zone=us-central1-b --port=2
```

Where "us-central1-b" is the selected zone, "SecEdge-vspace-draft-1-me-vm-0" is the VM instance name and "SecEdge-public" is the project name in Google Cloud.

Where “SecEdge-public“ is the project name in Google Cloud, "secedge-draft-1-me-vm-0" is the VM instance name, “connect-to-serial-port” connects to the serial port of the instance, "us-central1-b" is the deployment selected zone, and “--port=2” connects to the serial port 2 to reduce the VM logs printed on the console, e.g. Figure 65.



```
C:\Users\narva\AppData\Local\Google\Cloud SDK>
C:\Users\narva\AppData\Local\Google\Cloud SDK>
C:\Users\narva\AppData\Local\Google\Cloud SDK>gcloud compute --project=microedge-test connect-to-serial-port secedge-draft-1-me-vm-0
--zone=us-east1-b --port=2
```

Figure 65 Accessing Serial Console from gcloud cli shell

Continue with the steps described above to log in to Ubuntu.

13. SSH TO CLOUDEDGE VM INSTANCE AND OTHER VMS

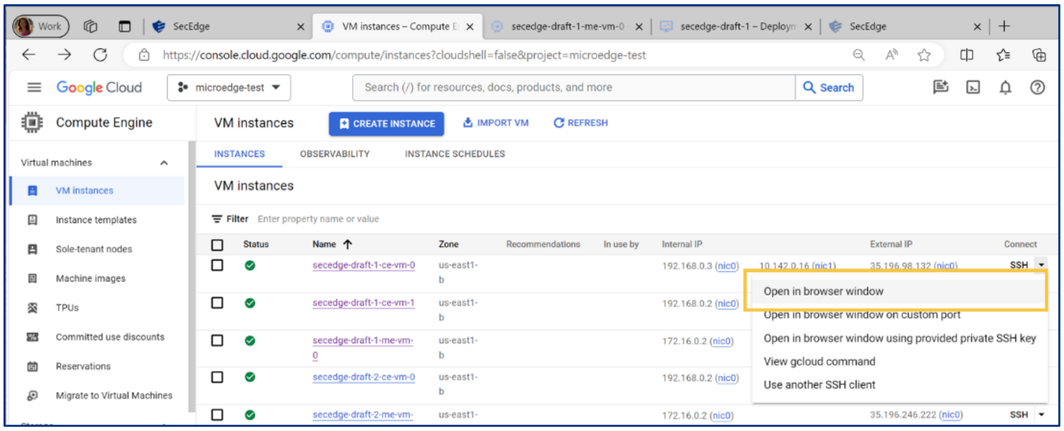
Accessing the VMs via SSH differs for CloudEdge and MicroEdge VMs. When accessing a CloudEdge VM via ssh, the system is in the init user name space and the virtual interfaces are available. This section is intended to describe SSH access to CloudEdge VMs.

When accessing a MicroEdge VM via ssh, the system is in the default user name space which requires the use of the nsenter command to switch to the init namespace with the virtual interfaces. SSH access is not recommended for accessing MicroEdge VMs as it can show unexpected behavior.

The following steps are a way to ssh to a CloudEdge VM or other VMs using during testing, except for MicroEdge VMs which process is described in the previous section. On the **VM instances** page, for the VM, use one of the SSH connection options.

From browser

- Click on drop down button beside SSH.
- Click on Open in browser window, Figure 66.



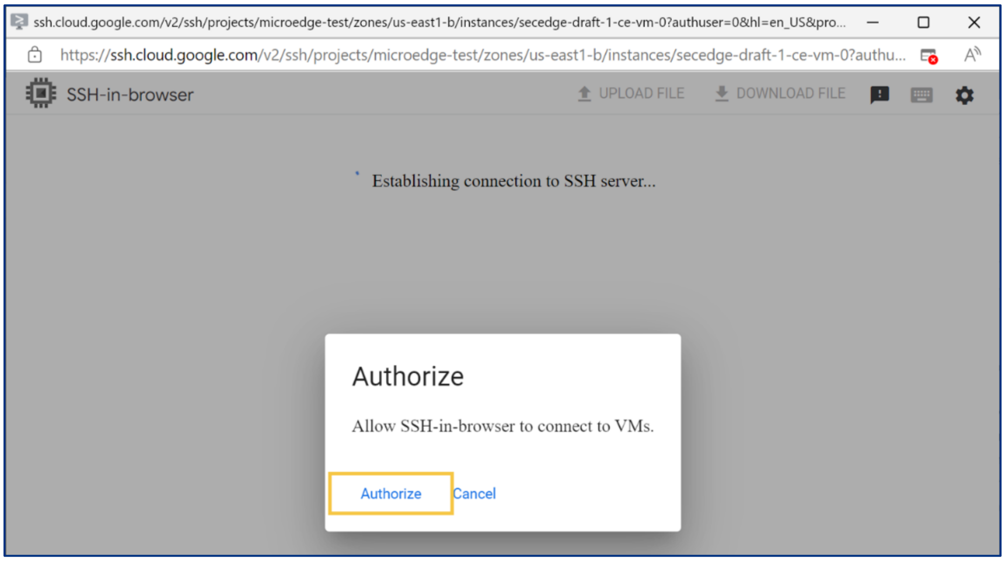
https://console.cloud.google.com/compute/instances?cloudshell=false&project=microedge-test

VM instances

	Status	Name	Zone	Recommendations	In use by	Internal IP		External IP	Connect
□	✓	secedge-draft-1-ce-vm-0	us-east1-b			192.168.0.3 (nic0)	10.142.0.16 (nic1)	35.196.98.132 (nic0)	SSH
□	✓	secedge-draft-1-ce-vm-1	us-east1-b			192.168.0.2 (nic0)			
□	✓	secedge-draft-1-me-vm-0	us-east1-b			172.16.0.2 (nic0)			
□	✓	secedge-draft-2-ce-vm-0	us-east1-b			192.168.0.2 (nic0)			
□	✓	secedge-draft-2-me-vm-	us-east1-			172.16.0.2 (nic0)		35.196.246.222 (nic0)	SSH

Figure 66 Google Cloud VM Instances SSH Options

- Authorize SSH-in-browser to connect to the VM, Figure 67.



ssh.cloud.google.com/v2/ssh/projects/microedge-test/zones/us-east1-b/instances/secedge-draft-1-ce-vm-0?authuser=0&hl=en_US&pro...

https://ssh.cloud.google.com/v2/ssh/projects/microedge-test/zones/us-east1-b/instances/secedge-draft-1-ce-vm-0?authu...

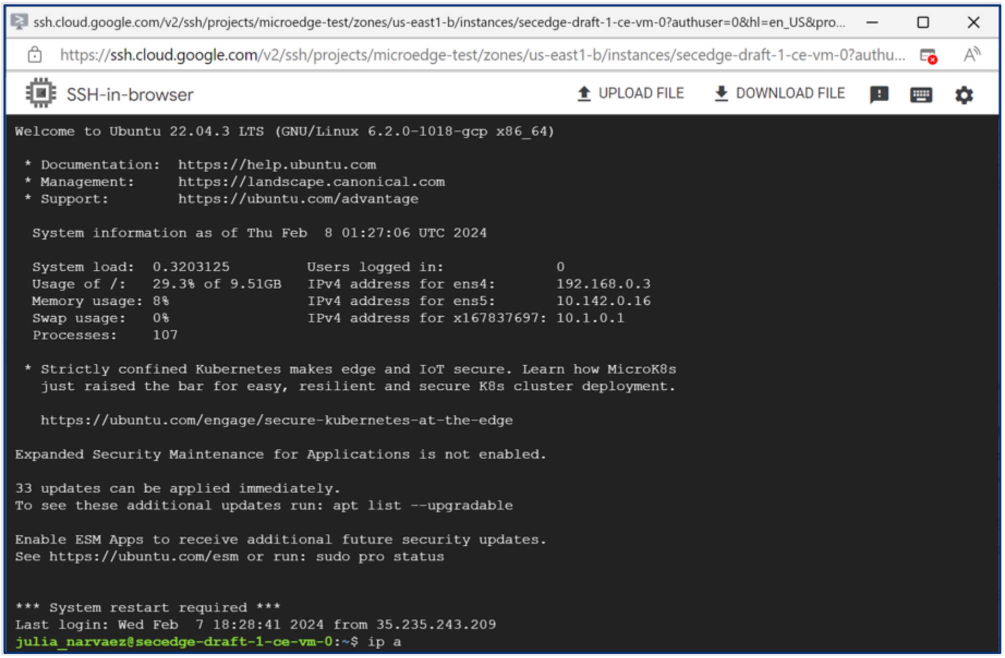
Establishing connection to SSH server...

Authorize

Allow SSH-in-browser to connect to VMs.

Figure 67 Authorize SSH-in-browser

- Access the CloudEdge VM, Figure 68



ssh.cloud.google.com/v2/ssh/projects/microedge-test/zones/us-east1-b/instances/secedge-draft-1-ce-vm-0?authuser=0&hl=en_US&pro...
https://ssh.cloud.google.com/v2/ssh/projects/microedge-test/zones/us-east1-b/instances/secedge-draft-1-ce-vm-0?authu...
SSH-in-browser
UPLOAD FILE
DOWNLOAD FILE

```
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1018-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Feb  8 01:27:06 UTC 2024

  System load:  0.3203125         Users logged in:            0
  Usage of /:   29.3% of 9.51GB   IPv4 address for ens4:      192.168.0.3
  Memory usage: 8%                IPv4 address for ens5:      10.142.0.16
  Swap usage:   0%                IPv4 address for x167837697: 10.1.0.1
  Processes:    107

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

33 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***
Last login: Wed Feb  7 18:28:41 2024 from 35.235.243.209
julia_narvaez@secedge-draft-1-ce-vm-0:~$ ip a
```

Figure 68 CloudEdge VM SSH Terminal

14. ACCESSING SERIAL TERMINAL TROUBLESHOOTING

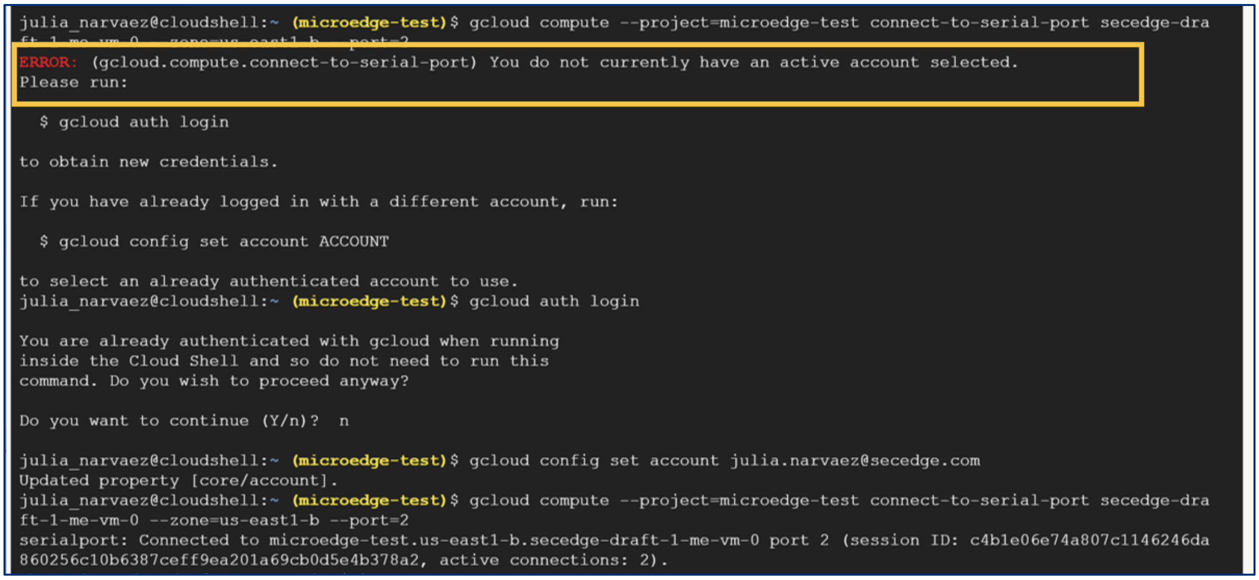
If you encounter errors because of your account authorization, please follow the instructions on the terminal.

For example, xx shows an error because the user does not have an active account selected. In this case, two options are suggested:

```
gcloud auth login

gcloud config set account ACCOUNT
```

Follow the instructions and try the command again:

```
gcloud compute --project=microedge-test connect-to-serial-port secedge-draft-1-me-vm-0 --zone=us-east1-b --port=2
```



```
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud compute --project=microedge-test connect-to-serial-port secedge-dra
ft-1-me-vm-0 --zone=us-east1-b --port=2
ERROR: (gcloud.compute.connect-to-serial-port) You do not currently have an active account selected.
Please run:

  $ gcloud auth login

to obtain new credentials.

If you have already logged in with a different account, run:

  $ gcloud config set account ACCOUNT

to select an already authenticated account to use.
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud auth login

You are already authenticated with gcloud when running
inside the Cloud Shell and so do not need to run this
command. Do you wish to proceed anyway?

Do you want to continue (Y/n)?  n

julia_narvaez@cloudshell:~ (microedge-test)$ gcloud config set account julia.narvaez@secedge.com
Updated property [core/account].
julia_narvaez@cloudshell:~ (microedge-test)$ gcloud compute --project=microedge-test connect-to-serial-port secedge-dra
ft-1-me-vm-0 --zone=us-east1-b --port=2
serialport: Connected to microedge-test.us-east1-b.secedge-draft-1-me-vm-0 port 2 (session ID: c4b1e06e74a807c1146246da
860256c10b6387ceff9ea201a69cb0d5e4b378a2, active connections: 2).
```

Figure 69 Troubleshooting