



SECeDGE STUDIO™

GETTING STARTED GUIDE

May 7, 2024 | Version 1.2

THIS DOCUMENT IS PROVIDED BY SECeDGE™. THIS DOCUMENT, ITS CONTENTS, AND THE SECURITY SYSTEM DESCRIBED SHALL REMAIN THE EXCLUSIVE PROPERTY OF SECeDGE.

1. TABLE OF CONTENTS

- 1. TABLE OF CONTENTS..... 2**
- 2. SECEDGE STUDIO™ OVERVIEW..... 3**
 - 2.1. BENEFITS 3
 - 2.2. SECEDGE SERVICE PLATFORM..... 3
 - 2.3. SECEDGE STUDIO ARCHITECTURE..... 5
 - 2.4. PREREQUISITES TO USE SECEDGE STUDIO™ 5
- 3. SECEDGE STUDIO™ DEPLOYMENT TEST STEPS 6**
 - 3.1. START WITH SECEDGE STUDIO™ ON GOOGLE MARKETPLACE 6
 - 3.2. ACCEPT PRODUCT AGREEMENTS AND TERMS OF SERVICE 8
 - 3.3. DEPLOY THE SECEDGE STUDIO VMs 8
 - 3.4. MANAGE MICROEDGE AND CLOUDEDGE INSTANCES THROUGH SECEDGE STUDIO™ USER INTERFACE 11
 - 3.5. CUSTOMIZE AND TEST 13
- 4. SECEDGE STUDIO™ USER INTERFACE 13**
 - 4.1. MICROEDGE DEVICES 13
 - 4.1.1. MICROEDGE GROUPS 14
 - 4.1.2. MICROEDGE EDGES..... 14
 - 4.2. CLOUDEDGE DEVICES 15
 - 4.2.1. CLOUDEDGE GROUPS..... 15
 - 4.2.2. CLOUDEDGE DEVICES 15
- 5. CUSTOMIZE VM AND TEST TUNNEL 16**
 - 5.1. CREATE A VM INSTANCE TO HOST A WEB SERVER 17
 - 5.2. START THE WEB SERVER IN APP WEB SERVER VM..... 17
 - 5.3. CONNECT FROM MICROEDGE VM TO WEB SERVER VM 18
 - 5.3.1. ACCESS MICROEDGE VM..... 18
 - 5.3.2. CONNECT FROM THE MICROEDGE VM TO THE APP WEB SERVER VM..... 23
- 6. NEXT STEPS 24**
- 7. ACCESSING SERIAL TERMINAL TROUBLESHOOTING 24**

2. SECeDGE STUDIO™ OVERVIEW

This guide provides an overview of SecEdge Studio™ and the steps to set up and test security capabilities offered by MicroEdge™, CloudEdge™ and ControlEdge™. An example illustrates the SecEdge Studio end-to-end functionality. This guide also introduces the SecEdge Studio User Interface which enables the user to manage and configure MicroEdge and CloudEdge device groups, devices and their connectivity.

SecEdge Studio is a development and test environment for SecEdge's chip-to-cloud security solution, available on Google Cloud 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. IPsec Chip to Cloud Tunnels is automatically set up through SecEdge platform, enabling the configuration, policy, key management system and dashboard 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. Overall, security development and test time can be reduced from months to weeks.

After completing this guide, please see the SecEdge Studio Tutorial for instructions on how to configure and test one or multiple tunnel scenarios, and samples of how to rotate keys and certs. Please see the SecEdge Studio User Guide for information about capabilities, concepts and functionality. These resources are available on the SecEdge website.

2.1. BENEFITS

SecEdge Studio benefits include:

- + Decouple the cloud application team dependency from end device hardware availability.
- + Accelerates migration from sandbox environment to real edge device hardware.
- + Test end-to-end the solution with the security capabilities offered by MicroEdge, CloudEdge and ControlEdge.
- + Turnkey solution for secure connectivity enabling compliance with security industry standards and guidelines.

2.2. 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 on embedded devices. The solution can be deployed to a variety of devices. It is installed on devices equipped with Linux OS. It has been tested on diverse hardware including devices with Variscite SOM modules. Some examples of implementations are 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, depicted in Figure 1.

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.

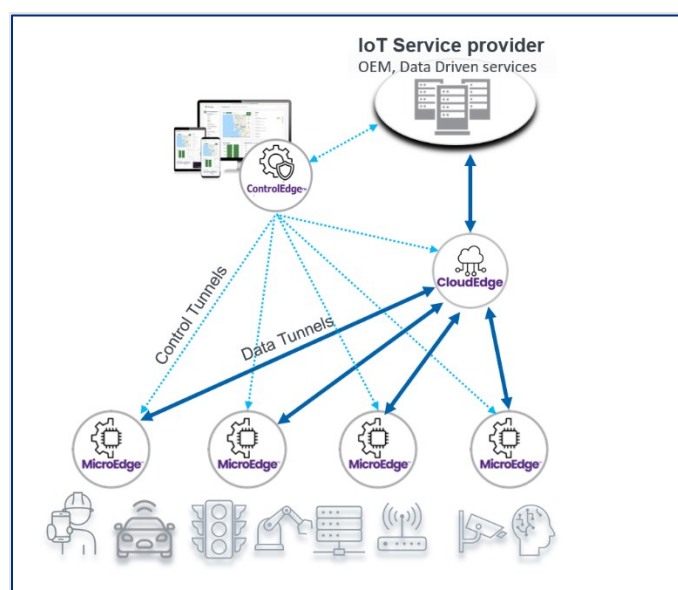


Figure 1 SecEdge Service Platform Architecture

2.3. SECeDGE STUDIO ARCHITECTURE

SecEdge Studio enables development and test end-to-end the SecEdge security solution in Google Cloud Platform (GCP) cloud environment without hardware. Shown in Figure 2, SecEdge Studio uses ControlEdge in GCP supported by SecEdge and deploys virtual machines (VMs) in the GCP customer's account.

ControlEdge in GCP

- + Orchestrates security services between MicroEdge (in VM1) and CloudEdge (in VM2).
- + User has full control to test end-to-end the various security features via SecEdge Studio dashboard.

VMs in Customer's GCP Account

- + VM1: Emulates edge device and its applications connectivity via an IPsec tunnel with MicroEdge.
- + One or more IPsec tunnel(s) can be implemented from the emulated device (in VM1) and tested easily (with one CloudEdge per tunnel).
- + VM2: CloudEdge receives encrypted data from the emulated device and delivers it to customer's backend application.

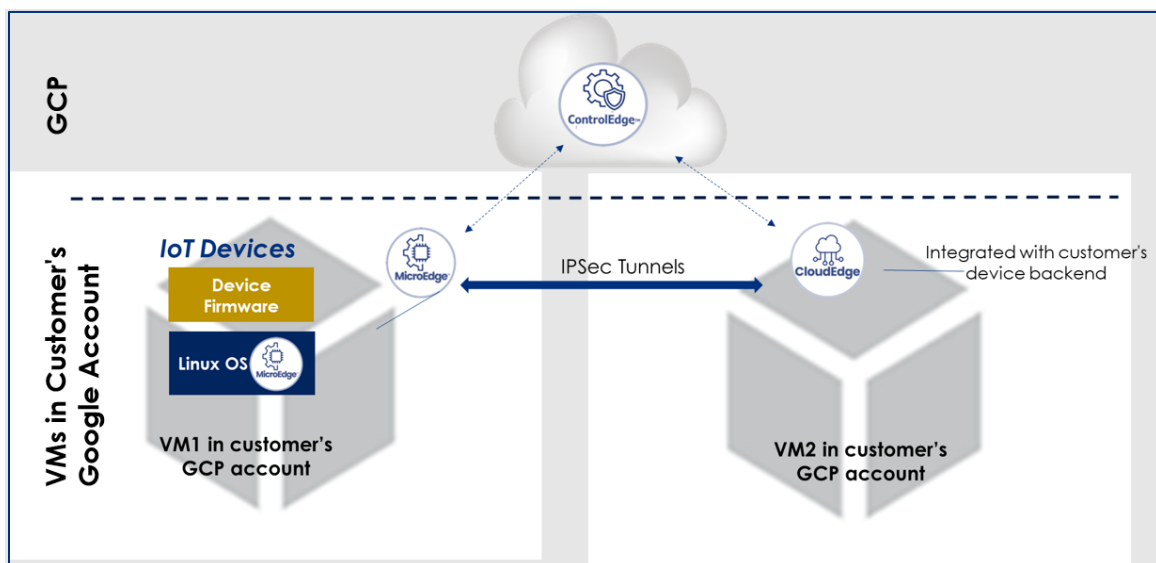


Figure 2 Architecture Overview

2.4. 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
 - o Commerce Producer Viewer
 - o Compute Instance Admin (v1)
 - o Consumer Procurement Entitlement Manager
 - o Deployment Manager Editor
 - o IAP-secured Tunnel User
 - o Service Account User
 - o Service Management Administrator
- + The following APIs enabled
 - o Compute Engine API
 - o Cloud Deployment Manager V2 API
 - o Cloud Runtime Configuration API
- + Familiarity with the following services in Google Cloud Console:
 - o Compute Engine
 - o VPC Network
 - o 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. This will be used for testing SecEdge Studio.
 - + Note: you can also 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 API,
<https://console.cloud.google.com/marketplace/product/google/compute.googleapis.com>
 - + Cloud Deployment Manager V2 API,
<https://console.cloud.google.com/marketplace/product/google/deploymentmanager.googleapis.com>
4. Go to Marketplace section and search for “SecEdge” product.
5. Select SecEdge Studio.
6. The SecEdge Studio **Product details** page shows overview, pricing and support information, Figure 3.

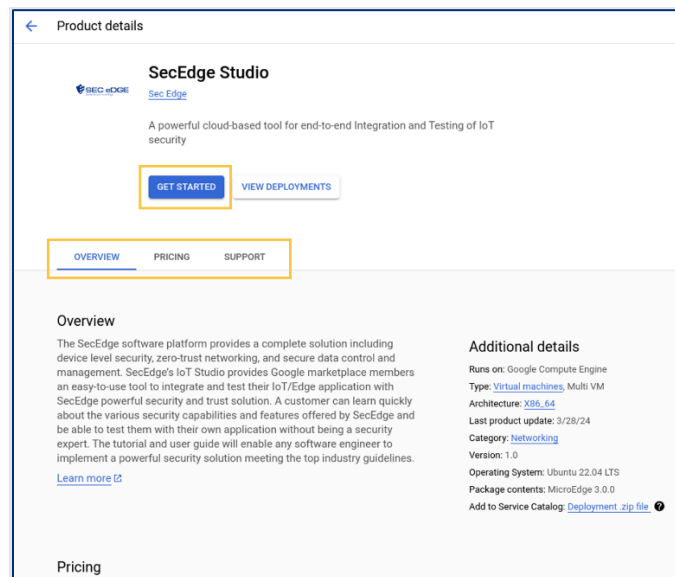


Figure 3 SecEdge Studio Product Details page

7. Click on **GET STARTED** to continue and access the **Agreements** page.

3.2. ACCEPT PRODUCT AGREEMENTS AND TERMS OF SERVICE

On the Google Cloud, **Agreements** page, Figure 4, you accept the agreements to start using the product.

1. On the **Agreements** page, accept the terms and agreements, by ticking on the checkbox and clicking on **AGREE**. The End User License Agreement (EULA) includes a Non-disclose agreement.

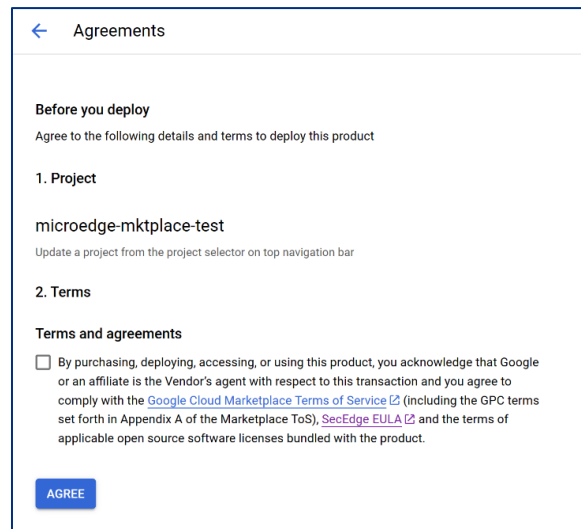


Figure 4 SecEdge Studio Terms and Agreements

2. After agreeing, you are ready to deploy your project. Click on **DEPLOY**, Figure 5

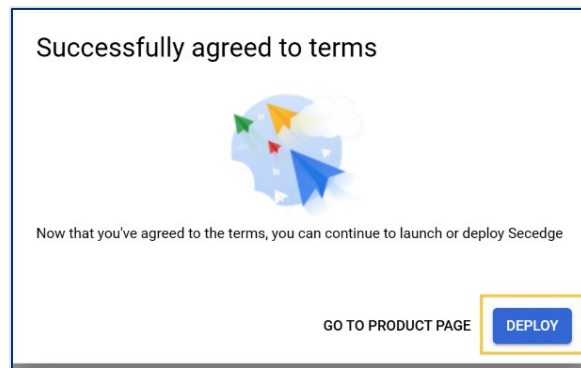


Figure 5 Deploy

3.3. DEPLOY THE SECEDGE STUDIO VMs

Clicking on **DEPLOY** launches a process to setup two VMs for your current project. One VM has MicroEdge and the other has CloudEdge installed. ControlEdge remains always available and configured to work with the VMs.

On the **New SecEdge Studio deployment** page, configure the **MicroEdge** VM and **CloudEdge** VM, Figure 6.

New SecEdge Studio deployment

! Prices don't include private offer discounts

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

Deployment name *
secedge-studio-draft-1

Zone
us-east-1-b

Enter your email *
This mail should be used for signup with secedge

MicroEdge
Instance Count: 1

Machine type


General purpose Compute optimized Memory optimized

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

Additional information

SecEdge Studio overview
Product provided by Sec Edge

License for Cloud Marketplace virtual machine image solution with billing service secedge-vspace.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 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)

CloudEdge

Instance Count: 1

Machine type


General purpose Compute optimized Memory optimized

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(1an interface)

Network interfaces
default default (10.142.0.0/20)

ADD A NETWORK INTERFACE

DEPLOY

Figure 6 New SecEdge Studio Deployment

Click on **DEPLOY**. SecEdge Studio activates the CloudEdge and MicroEdge VMs and adds them to a default group. During activation the following credentials are used:

- + 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.

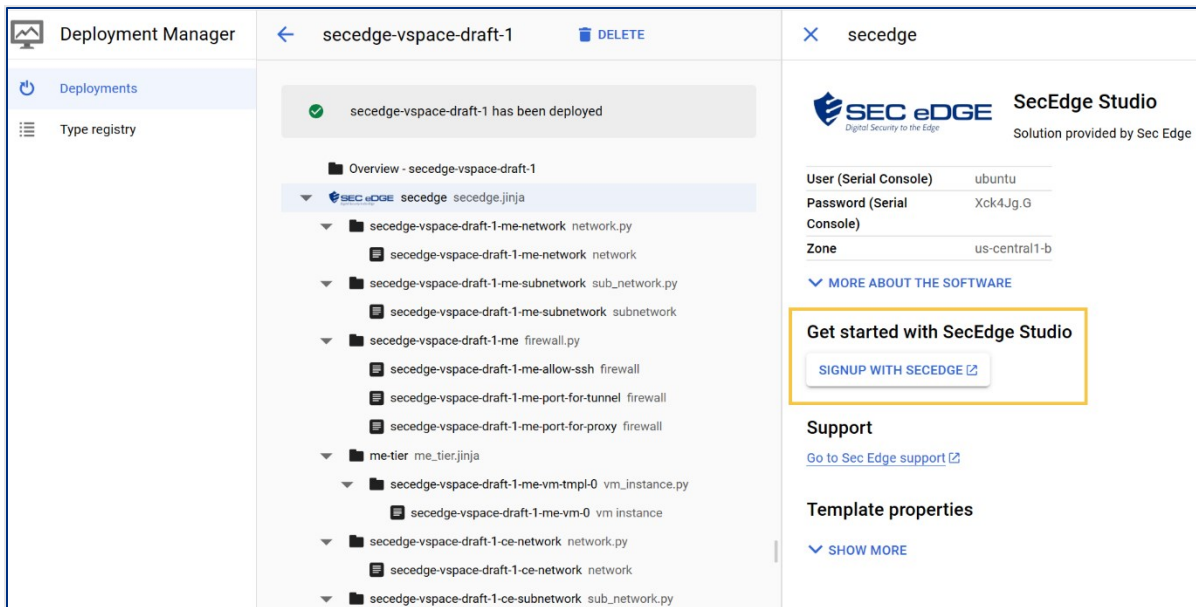


Figure 7 Deployment Manager Page

The Google Cloud, Compute Engine, **VM instances** page shows the two deployed VMs, Figure 8:

- + CloudEdge VM, **SecEdge-vspace-draft-1-ce-vm-0**, which has two network interfaces one LAN and one WAN.
- + MicroEdge VM, **SecEdge-vspace-draft-1-me-vm-0**, which has one WAN network interface.

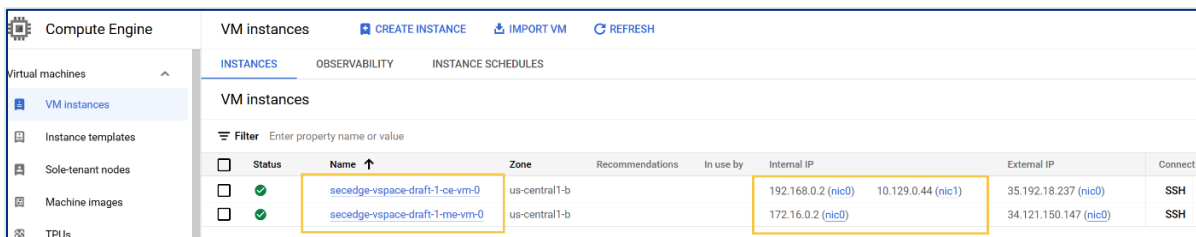


Figure 8 VM Instances page after deploying SecEdge Studio VMs

3.4. 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.
 - + Sign up on the **Welcome to SecEdge** page of the user interface.

Figure 9 SecEdge Studio Sign up

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

+ To access directly after you have signed up:

<https://console.me.secedge.com>

3.5. CUSTOMIZE AND TEST

Later in this document, there are instructions to customize your work environment in the VMs and test the tunnel by running an example that exercises end-to-end the security capabilities offered by MicroEdge, CloudEdge and ControlEdge. There is also an introduction to configure multiple tunnel scenarios.

4. SECeEDGE STUDIO™ USER INTERFACE

The dashboard, Figure 10, 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.

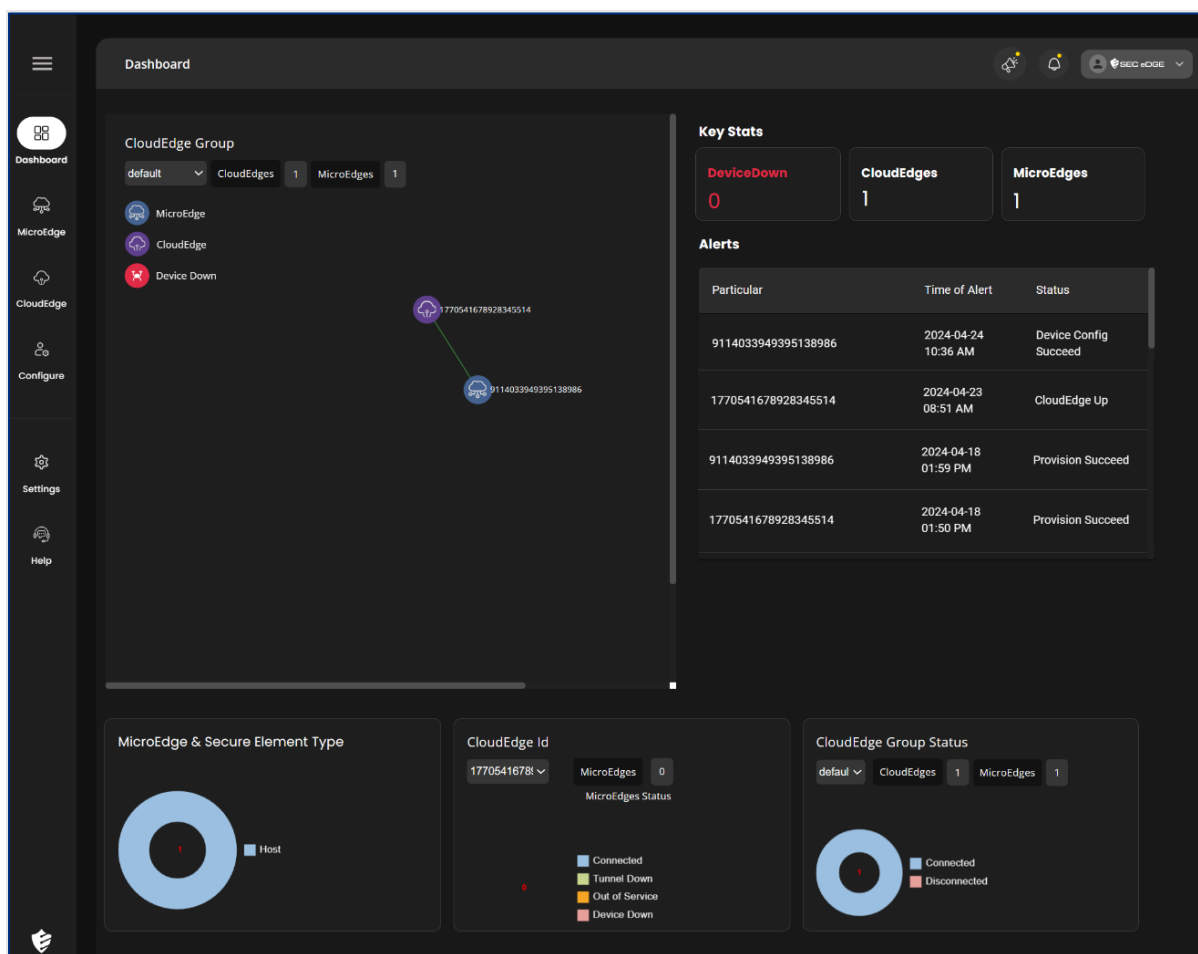


Figure 10 SecEdge Studio Dashboard

4.1. MICROEDGE DEVICES

The system permits management of Groups and Edges devices.

4.1.1. MICROEDGE GROUPS

Selecting **MicroEdge** and then **Groups** shows the group to which the MicroEdge device was added during deployment. Its configuration can be changed and additional groups can be added, as shown in Figure 11.

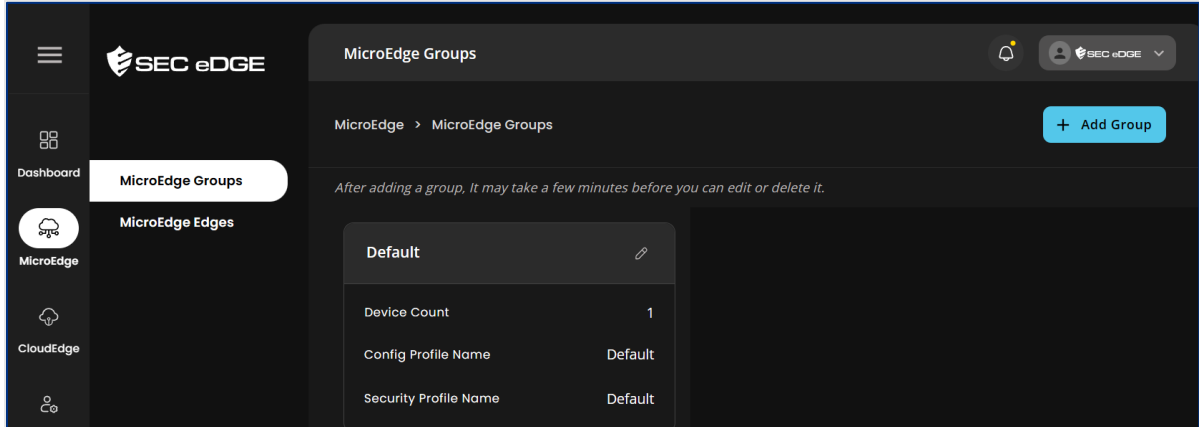


Figure 11 MicroEdge Groups

4.1.2. MICROEDGE EDGES

The **Edges** option lists the deployed device, its connectivity status, and facilitates managing and adding devices. Note that the deployed device status is **ACTIVE** as shown in Figure 12.

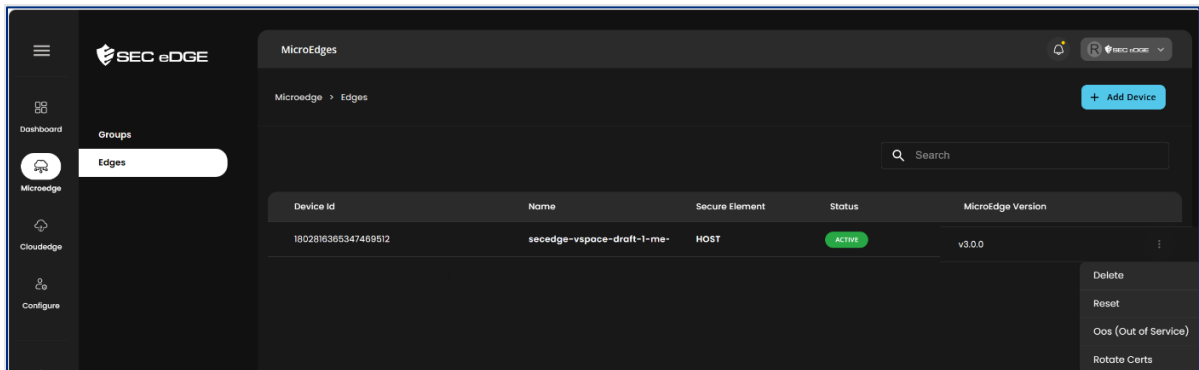


Figure 12 MicroEdge Edge List

Per device, additional information is available, shown in Figure 13:

- + Characteristics
- + List of tunnels
- + List of networks

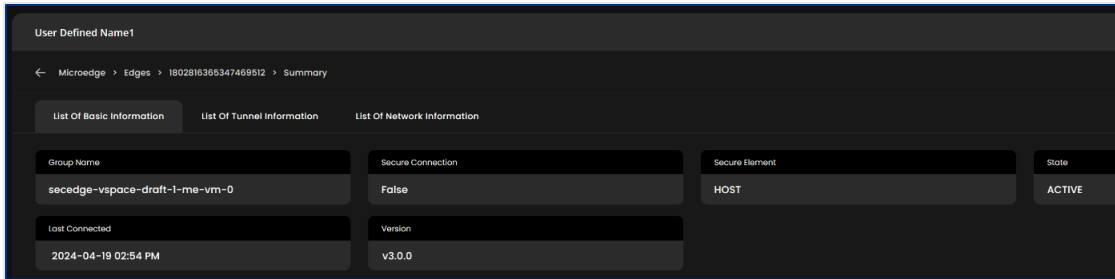


Figure 13 MicroEdge Edge Detail

4.2. CLOUDEDGE DEVICES

The CloudEdge Edge Option shows Groups information, Edges and connectivity State.

4.2.1. CLOUDEDGE GROUPS

Selecting **CloudEdge** and then **Groups** shows the group to which the CloudEdge device was added during deployment. Its configuration can be changed. Additional groups can be added, Figure 14.

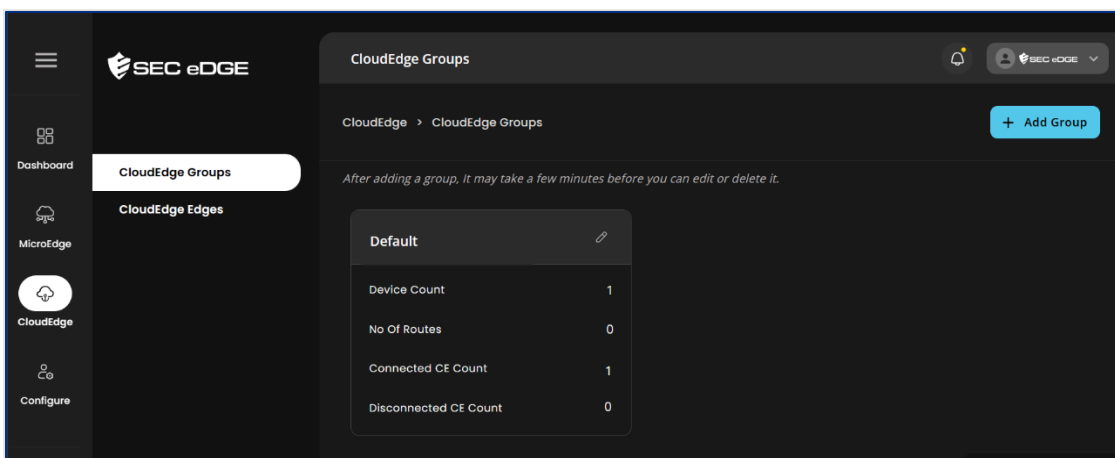


Figure 14 CloudEdge Groups

4.2.2. CLOUDEDGE DEVICES

The **Edges** option lists the deployed device. Note that its state is **ACTIVE**. Additional CloudEdge devices can be added, Figure 15.

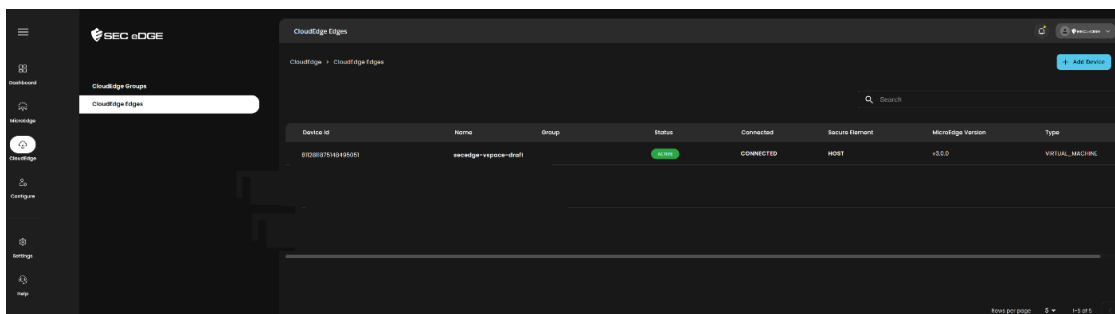


Figure 15 CloudEdge Devices

5. CUSTOMIZE VM AND TEST TUNNEL

With the secure tunnel established between MicroEdge and CloudEdge, the setup can be further customized. You can perform complete end-to-end testing.

To illustrate the SecEdge Studio capabilities, this section guides you through an example that uses the VMs deployed in your project and a sample [app-web-server](#) VM:

- + App Web Server VM that you create to run a web server and is connected to the CloudEdge VM through a test network to the LAN interface, [app-web-server](#).
- + CloudEdge VM, the LAN interface is the same as the network App Web Server.
- + MicroEdge VM is on a different network than the App Web Server and runs an IoT app that intends to connect to the App Web Server.

The example exercises the end-to-end solution and security capabilities offered by MicroEdge, CloudEdge and ControlEdge. When the IPsec Tunnel is active between the MicroEdge and CloudEdge VMs, the MicroEdge VM can access the web server. When the IPsec Tunnel is not active, access from the MicroEdge VM to the App Web Server fails. The three VMs are depicted in Figure 16.

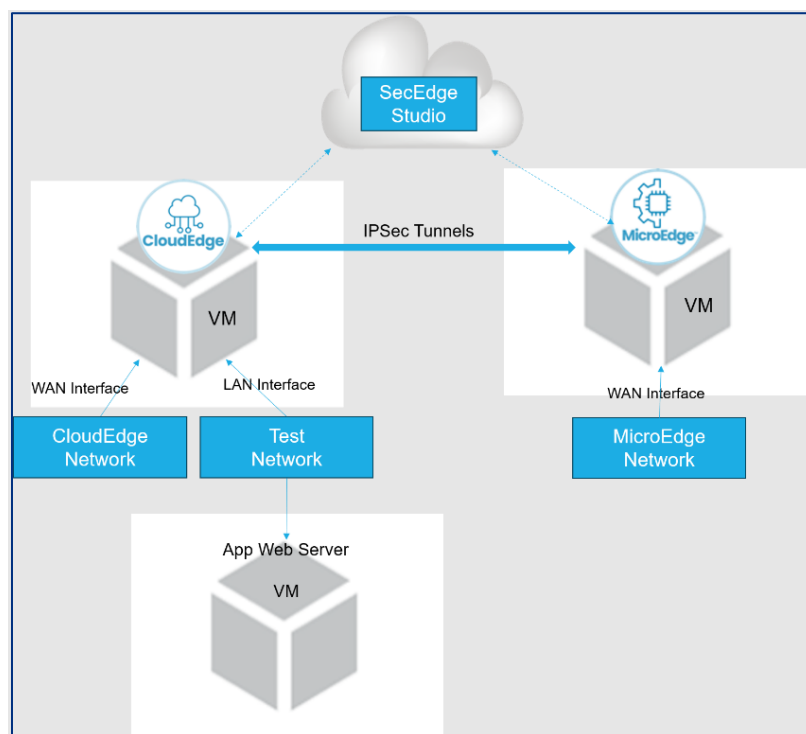


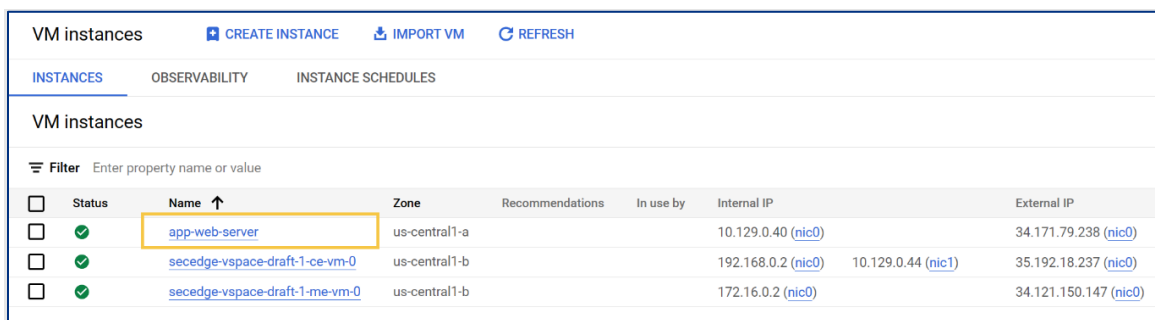
Figure 16 Connectivity Example

5.1. CREATE A VM INSTANCE TO HOST A WEB SERVER

On the Google Cloud **VM instances** page use the **CREATE INSTANCE** option to deploy a VM where the web server is hosted. This guide refers to that VM as “**app-web-server**”.

- + Keep the same **Region** as the MicroEdge and CloudEdge VMs previously created in your deployment. The **Zone** can be different.
- + The App Web Server VM, **app-web-server**, should be connected to the CloudEdge VM through a test network to the LAN interface.
- + The CloudEdge VM LAN interface should be the same as the **app-web-server** network.

Figure 17 shows sample VMs and IP addresses on the Google Cloud **VM instances** page.



Status	Name	Zone	Recommendations	In use by	Internal IP	External IP
✓	app-web-server	us-central1-a			10.129.0.40 (nic0)	34.171.79.238 (nic0)
✓	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)
✓	secedge-vspace-draft-1-me-vm-0	us-central1-b			172.16.0.2 (nic0)	34.121.150.147 (nic0)

Figure 17 Connectivity Example VM Instances

5.2. START THE WEB SERVER IN APP WEB SERVER VM

3. Connect to the **app-web-server** VM.

- + On the Google Cloud VM instances page, use the SSH options to connect to the server, for example:

```
compute ssh app-web-server
```

- + Notice the internal IP of the web server VM. Figure 18 shows sample output.

```
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 mq state UP group default qlen 1000
    link/ether 42:01:0a:81:00:28 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 10.129.0.40/32 metric 100 scope global dynamic ens4
        valid_lft 2268sec preferred_lft 2268sec
    inet6 fe80::4001:aff:fe81:28/64 scope link
        valid_lft forever preferred_lft forever
```

Figure 18 Terminal Window app-web-server VM

- Start the webserver. Figure 19 shows command execution.

```
sudo su

python3 -m http.server 8080
```

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

Figure 19 app-web-server VM running http.server

5.3. CONNECT FROM MICROEDGE VM TO WEB SERVER VM

5.3.1. ACCESS MICROEDGE VM

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:

- Click on the **CONNECT TO SERIAL CONSOLE** drop down menu, Figure 20.

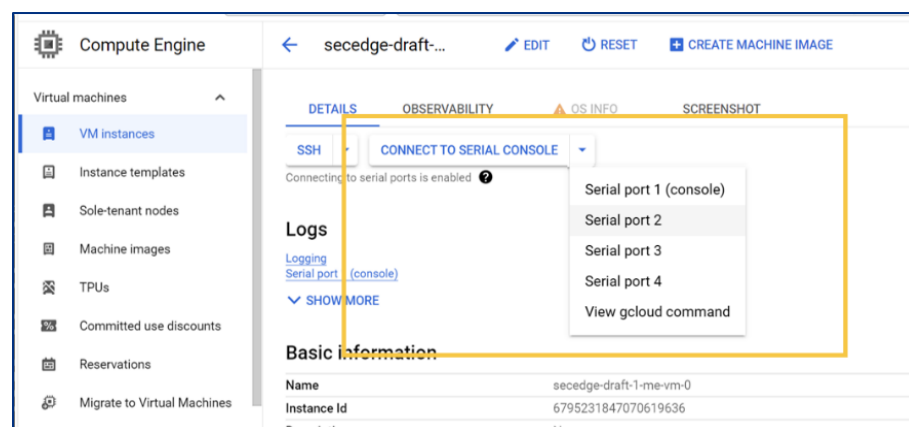


Figure 20 Google Cloud, VM Instances, CONNECT TO SERIAL CONSOLE Options

- 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 21.

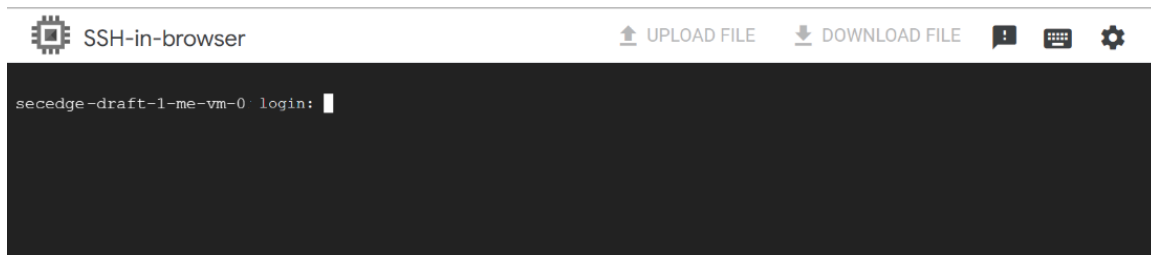


Figure 21 MicroEdge Serial Console Login

- 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, as show in Figure 22.

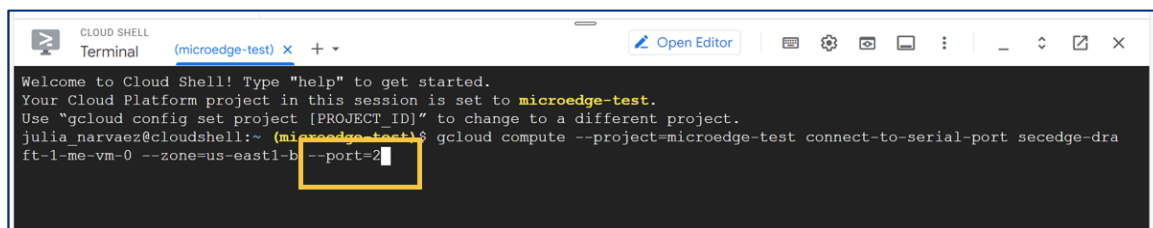


Figure 22 Cloud Shell Terminal Connect To Serial Port Command

- + Press [Enter](#) when the new side bar opens and authorize Cloud Shell to use your credentials for the Gcloud CLI command, Figure 23.

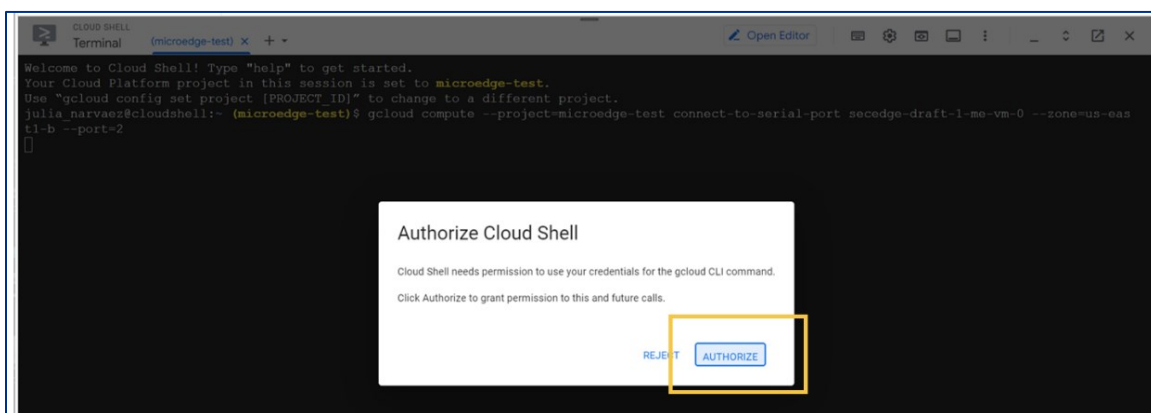


Figure 23 Cloud Shell Authorization

- + When the command succeeds, the login information is requested, Figure 24.

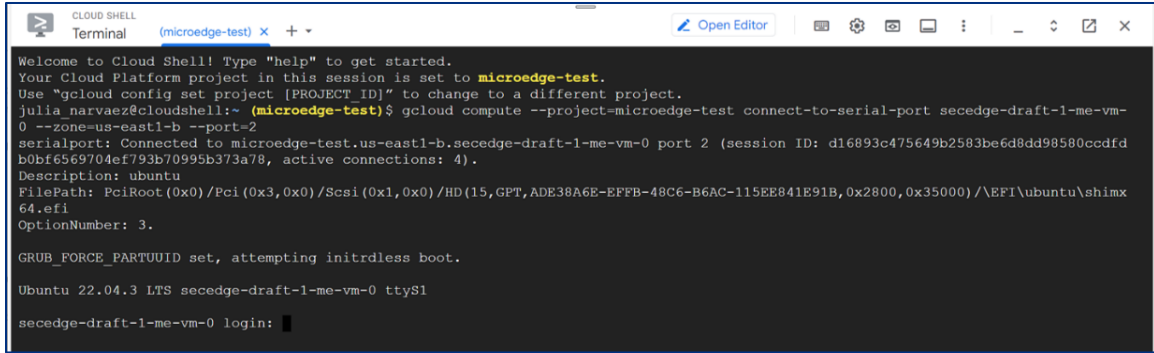


Figure 24 Cloud Shell Success and Login Prompt

If you encounter errors because your Gcloud user account, please see 7 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.

4. Identify the serial console password on one of the two following locations.
 - o From the **Deployment Manager** section, Figure 25, click on the deployment name to which the MicroEdge VM belongs.

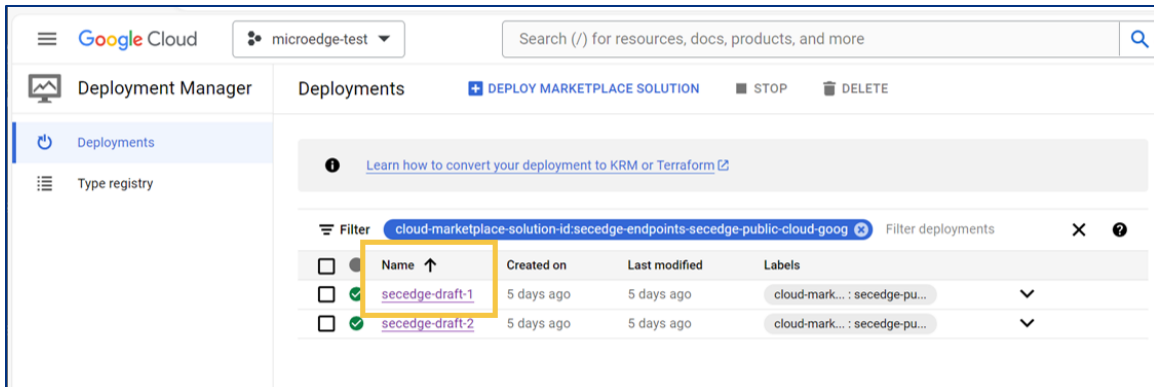


Figure 25 Google Cloud, Deployment Manager, Deployments page

Note that the user is **ubuntu**. Take note of the password, shown in Figure 26.

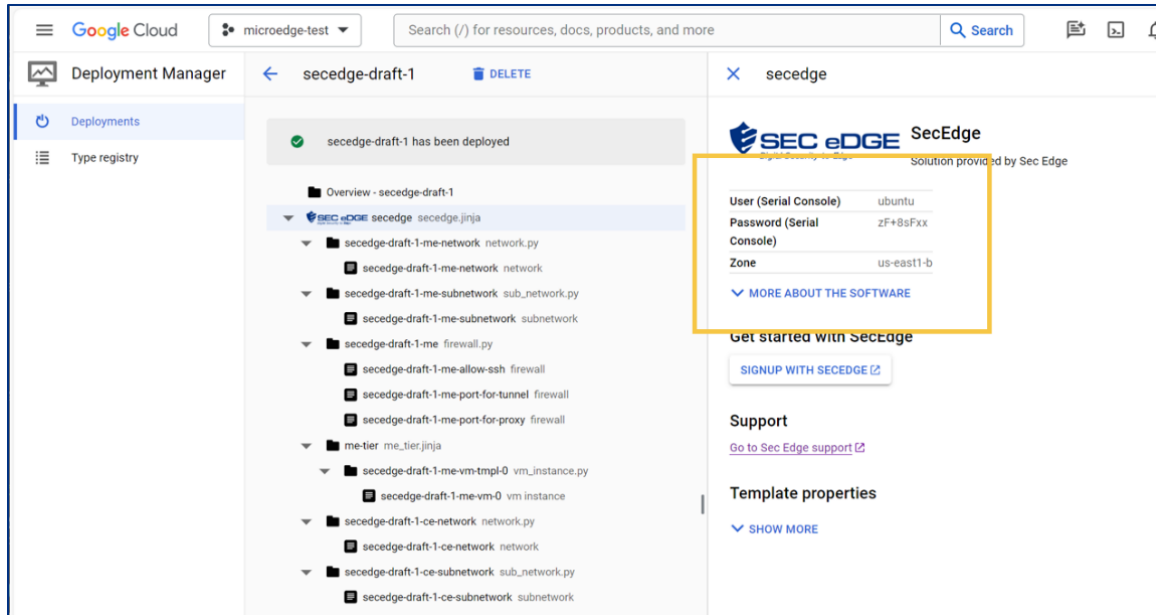


Figure 26 Google Cloud, Deployments Manager, Selected Deployment page

- o 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 27

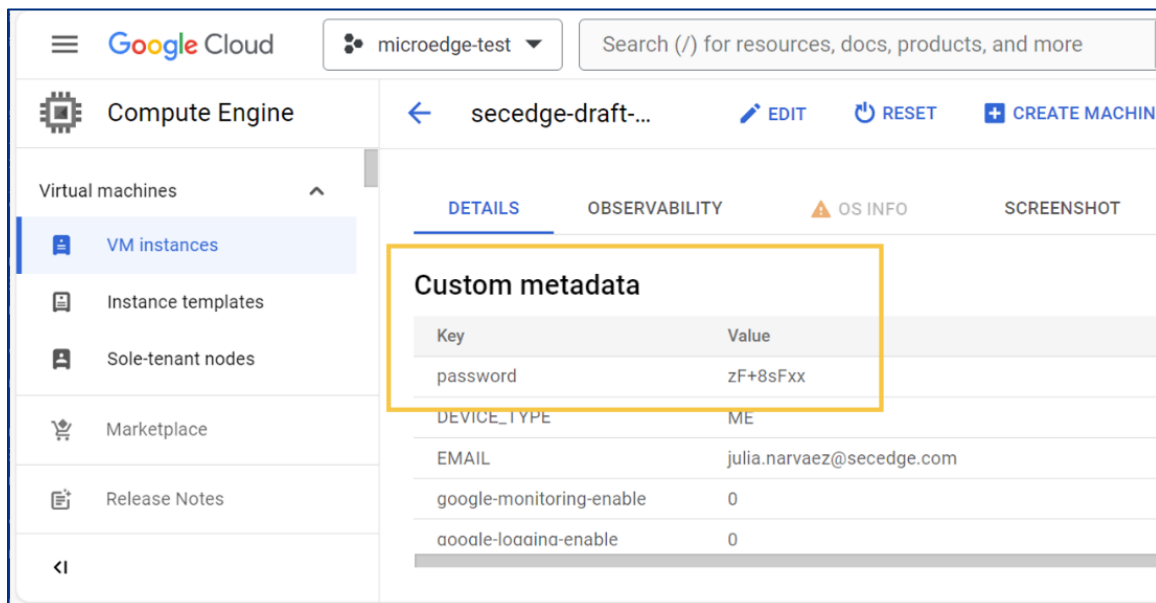


Figure 27 Google Cloud, VM instances, Details, Custom metadata

5. Enter the login and password when prompted, Figure 28.

```

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 28 Ubuntu Login

6. Execute `ip a` and notice the `xfrm` interface created by MicroEdge, Figure 29.

```

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 29 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 your 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 30.

```
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 30 Accessing Serial Console from gcloud cli shell

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

5.3.2. CONNECT FROM THE MICROEDGE VM TO THE APP WEB SERVER VM

- + Execute the following command to connect to the App Web Server using the VM internal IP address.

```
curl 10.129.0.40:8080
```

- + The MicroEdge VM connects, Figure 31.

```
root@secedge-vspace-draft-1-me-vm-0:/home/julia_narvaez# curl 10.129.0.40:8080
curl: (7) Failed to connect to 10.129.0.40 port 8080 after 5 ms: Connection refused
root@secedge-vspace-draft-1-me-vm-0:/home/julia_narvaez# curl 10.129.0.40:8080
<!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_history">.bash_history</a></li>
<li><a href=".bash_logout">.bash_logout</a></li>
<li><a href=".bashrc">.bashrc</a></li>
<li><a href=".cache/">.cache</a></li>
<li><a href=".profile">.profile</a></li>
<li><a href=".ssh/">.ssh</a></li>
</ul>
<hr>
</body>
</html>
```

Figure 31 MicroEdge Request to app-web-server

The App Web Server also shows the received request, Figure 32.

```
root@app-web-server:/home/julia_narvaez# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.129.0.44 - - [05/Dec/2023 01:29:07] "GET / HTTP/1.1" 200 -
```

Figure 32 app-web-server Received Request from MicroEdge

The fact that the MicroEdge VM can access the web server demonstrates that the IPsec tunnel is active between the MicroEdge and CloudEdge VMs.

6. NEXT STEPS

Now that you have completed the example and tested the IPsec Tunnel between the MicroEdge and CloudEdge VMs, continue with the following steps:

- + Learn about SecEdge Studio capabilities, concepts and functionality explained in the SecEdge Studio User Guide, information about capabilities, concepts and functionality.
- + Configure and test multiple tunnels scenarios, guided step-by-step in the SecEdge Studio Tutorial.

Important note:

After the development and test of the SecEdge security solution are completed, the solution must be ported onto the actual device hardware. SecEdge Studio solution offers methods to (re)test the security parts with actual devices.

Additional documentation to test with actual device hardware is supplied upon request.

7. ACCESSING SERIAL TERMINAL TROUBLESHOOTING

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

This example 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-terminal 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-draft-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-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: c4b1e06e74a807c1146246da860256c10b6387ceff9ea201a69cb0d5e4b378a2, active connections: 2).
```