

## Mediant Virtual Edition (VE) SBC

### Deployment on Google Cloud

Version 7.6



Google Cloud



---

## Table of Contents

---

<b>Notice .....</b>	<b>iii</b>
Security Vulnerabilities .....	iii
WEEE EU Directive .....	iii
Customer Support.....	iii
Stay in the Loop with AudioCodes.....	iii
Abbreviations and Terminology .....	iii
Document Revision Record .....	iii
Documentation Feedback.....	iv
<b>1 Introduction .....</b>	<b>1</b>
<b>2 Deployment Methods .....</b>	<b>2</b>
<b>3 Prerequisites .....</b>	<b>3</b>
3.1 AudioCodes Mediant VE Image .....	3
3.2 Network Architecture.....	4
3.2.1 Network Architecture for Standalone Deployment .....	4
3.2.2 Network Architecture for HA Deployment.....	5
3.2.3 Firewall Rules .....	6
3.3 Machine Types .....	7
<b>4 Deploying Mediant VE via Google Cloud Platform Console.....</b>	<b>8</b>
<b>5 Deploying Mediant VE via Stack Manager .....</b>	<b>10</b>
5.1 HA Deployment Topology .....	11
5.2 External IP Addresses .....	12
5.3 Internal IP Addresses.....	13
5.4 Management Traffic.....	13
<b>6 Changing Network Configuration after Deployment.....</b>	<b>14</b>
6.1 Adding a Network Interface .....	14
6.2 Deleting the Network Interface.....	17
<b>7 Licensing the Product .....</b>	<b>19</b>
7.1 Obtaining and Activating a Purchased License Key.....	19
7.2 Installing the License Key .....	20
7.3 Product Key .....	21

## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: April-10-2025

## Security Vulnerabilities

All security vulnerabilities should be reported to [vulnerability@audiocodes.com](mailto:vulnerability@audiocodes.com).

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

## Stay in the Loop with AudioCodes



## Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

## Document Revision Record

LTRT	Description
11027	Initial document release for Version 7.6.

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

# 1 Introduction

This document describes the deployment of AudioCodes' Mediant Virtual Edition (VE) Session Border Controller (SBC), hereafter referred to as *Mediant VE*, in a Google Cloud environment.



- For configuring the Mediant VE, refer to the *Mediant Software SBC User's Manual*.
- For instructions on how to install Mediant VE in other virtual environments such as VMware, refer to the *Mediant Virtual Edition SBC for VMware-KVM-HyperV Installation Manual*.

## 2 Deployment Methods

You can deploy Mediant VE as a virtual machine (VM) in the Google Cloud environment using one of the following methods:

- **Standalone SBC Deployments:** Use Google Cloud Platform Console to launch a new VM instance (see Section 4).
- **HA SBC Deployment (Two SBC Instances Operating in 1+1 Active/Standby Mode):** Use Stack Manager to create the deployment (see Section 5).



Mediant VE supports only IPv4 addresses (not IPv6) on Google Cloud.

## 3 Prerequisites

Prior to deploying Mediant VE SBC in the Google Cloud environment, make sure that you meet the following prerequisites:

- You have a Google Cloud account. If you don't have a Google Cloud account, you can sign up for one on Google's website at <https://cloud.google.com>.
- You have uploaded AudioCodes Mediant VE/CE Image to the image repository. For more information, see Section 3.1.
- You have created all Subnets needed for Mediant VE deployment and corresponding Firewall Rules for standalone deployment. For more information, see Section 3.2.

### 3.1 AudioCodes Mediant VE Image

To deploy Mediant VE on Google Cloud, you must use the *Mediant VE/CE Image for Google Cloud*. For more information, go to <https://www.audiocodes.com/library/firmware>.

**To upload Mediant VE image to Google Cloud image repository:**

1. Extract the .tar.gz file from the Mediant VE/CE Image for the Google Cloud .zip file.
2. In the Google Cloud Platform Console, go to the **Storage > Browser** page (<https://console.cloud.google.com/storage/browser>).
3. Choose an existing bucket or create a new one.
4. Choose an existing folder(s) inside the bucket or create a new one if needed.
5. Click **Upload files**, and then select the Mediant VE/CE image for the Google Cloud .tar.gz file.
6. When the upload completes, go to the **Compute Engine > Images** page (<https://console.cloud.google.com/compute/images>).
7. Click **Create Image**.
8. Enter a name for the image.
9. Specify the source as the Cloud Storage file, and then choose the .tar.gz file that you uploaded in the previous steps.
10. Specify the location where Mediant VE will be deployed.
11. Specify the additional properties for your image (e.g., family or description).
12. Click **Create** to create the image.

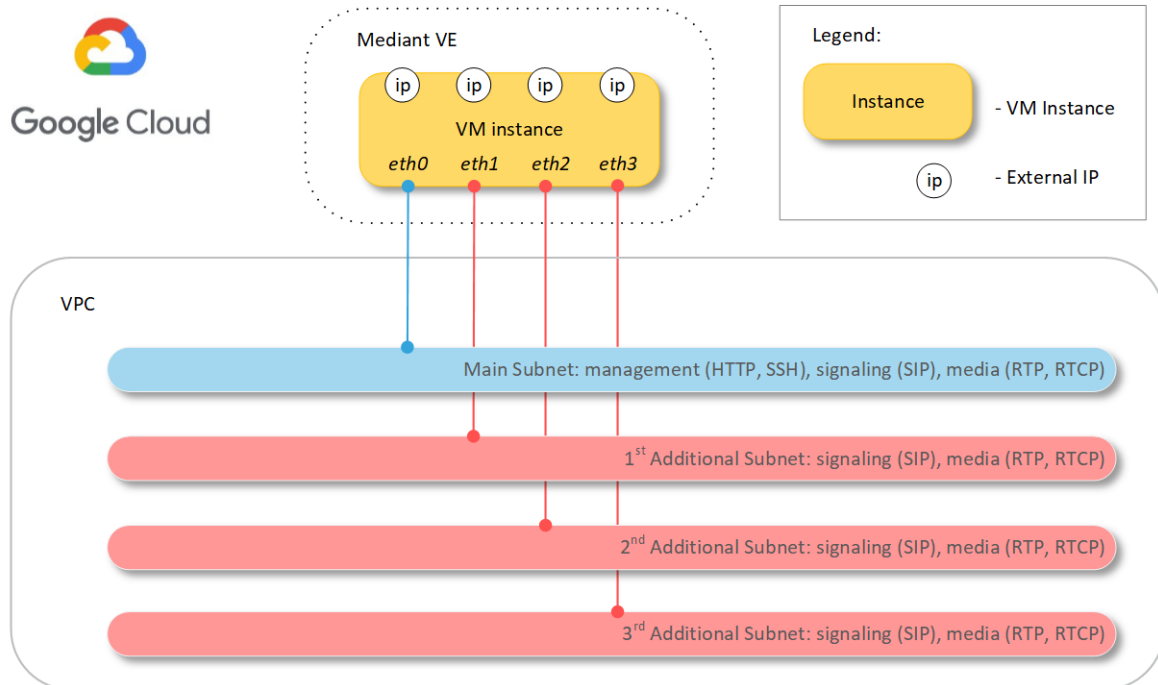
## 3.2 Network Architecture

This chapter describes the network architecture of Mediant VE on Google Cloud.

### 3.2.1 Network Architecture for Standalone Deployment

The network architecture for a standalone Mediant VE on Google Cloud is illustrated below.

**Figure 3-1: Network Architecture for Standalone Deployment**



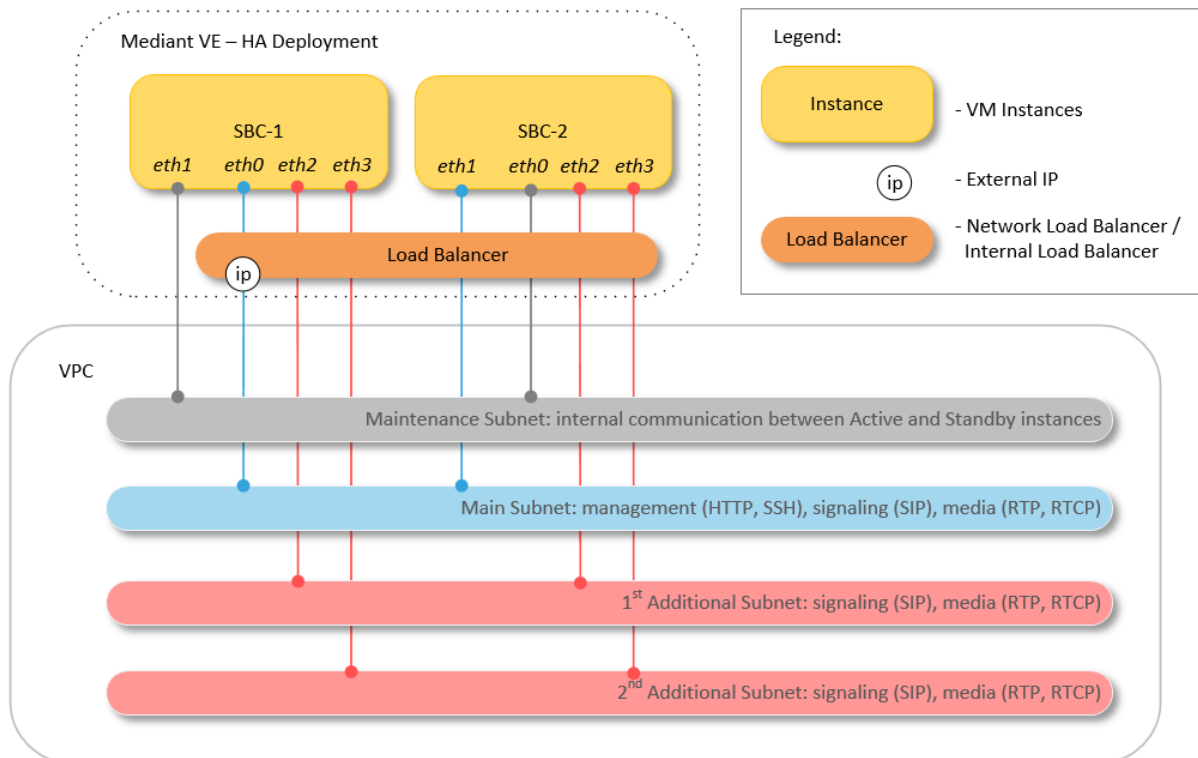
Up to three subnets may be used:

- **Main Subnet:** Carries management (e.g., HTTP and SSH), signaling (SIP) and media (RTP and RTCP) traffic. This is connected to the VM instance as the first network interface (eth0).
- **1<sup>st</sup>, 2<sup>nd</sup> and 3<sup>rd</sup> Additional Subnets:** Carry signaling (SIP) and media (RTP and RTCP) traffic. These are connected to the VM instance as additional network interfaces (eth1, eth2, and eth3). These subnets are optional, as the Main Subnet may carry all traffic types.

### 3.2.2 Network Architecture for HA Deployment

The network architecture for Mediant VE in High-Availability (HA) mode on Google Cloud is illustrated below.

**Figure 3-2: Network Architecture for HA Deployment**



Up to four subnets may be used:

- **Main Subnet:** Carries management (e.g., HTTP and SSH), signaling (SIP) and media (RTP and RTCP) traffic. This is connected to the VM instances as the first network interface (eth0).
- **Maintenance Subnet:** For internal communication between Active and Standby Mediant VE instances. This is connected to the VM instances as the second network interface (eth1).
- **1<sup>st</sup> and 2<sup>nd</sup> Additional Subnets:** Carry media (RTP, RTCP) traffic and connected to VM instances as the third and fourth network interfaces (eth2 and eth3), respectively. These subnets are optional, as the Main Subnet may carry all types of traffic.



For deployments done via Stack Manager Version 3.3.9 and later, the maintenance subnet is optional. If it's not used, internal communication between active and standby Mediant VE instances is over the main subnet, and the 1<sup>st</sup> and 2<sup>nd</sup> additional subnets are connected as the second and third network interfaces (eth1 and eth2), respectively.

Each subnet must reside in a different Virtual Private Cloud (VPC) network due to a network design of Google Cloud (refer to <https://cloud.google.com/vpc/docs/create-use-multiple-interfaces>).

All needed VPC networks and subnets must be created prior to Mediant VE deployment.

During deployment, Stack Manager creates all relevant Mediant VE components, including VM instances, load balancer and external IP addresses.

Mediant VE on Google Cloud uses the following native Google Cloud load balancers in front of two VM instances to achieve 1+1 active/standby HA operation mode:

- Network Load Balancer (<https://cloud.google.com/load-balancing/docs/network/>) for external (public) IPs.
- Internal Load Balancer (<https://cloud.google.com/load-balancing/docs/internal>) for internal (private) IPs.

Since Network Load Balancer supports only the primary VM's network interface, external IP addresses may be assigned *only* to the primary network interface (eth0) connected to the Main Subnet. It's possible to assign multiple external IP addresses to the primary network interface (eth0) if needed (see Section 5.2). It's possible to assign both external and internal IP addresses to the primary network interface (eth0) if needed (see Section 5.3) and use the internal IP address for management (see Section 5.4). It's also possible to move management traffic to the secondary network interfaces, connected to the 1<sup>st</sup> and 2<sup>nd</sup> Additional Subnets, respectively (see Section 5.4).

### 3.2.3 Firewall Rules



This section applies only to standalone (i.e., non-HA) deployments performed via the Google Cloud console. For deployments performed via Stack Manager Version 2.8.1 or later, firewall rules are automatically created during stack deployment.

On Google Cloud, firewall rules are configured at network level rather than at the instance / network interface level. Therefore, you must manually configure them prior to the first Mediant VE deployment, as described below.

It's recommended to create firewall rules for the "sbc" target tag and assign the latter to VM instances during creation. For deployment via Stack Manager, assigned tags may be customized by changing the **tags** parameter in the stack configuration file (default value is "sbc,ve").

The following firewall rules must be created for successful Mediant VE deployment:

Network	Name	Source IP Ranges	Target Tags	Protocols and Ports	Description
<b>Main</b>	main-ssh	0.0.0.0/0	ve	tcp: 22	SSH traffic
	main-http	0.0.0.0/0	ve	tcp: 80	Web traffic
	main-https	0.0.0.0/0	ve	tcp: 443	Secure Web traffic
	main-sip	0.0.0.0/0	ve	tcp: 5060-5090 udp: 5060-5090	SIP signaling traffic
	main-media	0.0.0.0/0	ve	udp: 6000-65535	RTP media traffic
<b>Additional 1 and 2</b>	additional-sip	0.0.0.0/0	ve	tcp: 5060-5090 udp: 5060-5090	SIP signaling traffic
	additional-media	0.0.0.0/0	ve	udp: 6000-65535	RTP media traffic

**To create Firewall Rules:**

1. In the Google Cloud Platform Console, go to the **VPC Network > Firewall rules** page (<https://console.cloud.google.com/networking/firewalls>).
2. Click **Create Firewall Rule**.
3. Create firewall rules according to the table above:
  - Network: <network>
  - Direction of traffic: "Ingress"
  - Action on match: "Allow"
  - Targets: "Specified target tags"
  - Target tags: <tags>
  - Source filter: "IPv4 ranges"
  - Source IPv4 ranges: <ranges>
  - Protocols and ports: "Specified protocols and ports"
    - ◆ <protocol>: <ports>

### 3.3 Machine Types

It is recommended to use the following machine types for Mediant VE instances:

- **Deployments without transcoding:** n2-standard-2 (for two network interfaces) or n2-standard-4 (for three or four network interfaces)
- **Deployments with transcoding:** n2-standard-8

## 4 Deploying Mediant VE via Google Cloud Platform Console

This section describes the deployment of a standalone Mediant VE via Google Cloud Platform Console.



This method is applicable only to standalone (i.e., non-HA) deployments.

### To deploy a standalone Mediant VE via Google Cloud Platform Console:

1. In the Google Cloud Platform Console, go to the **Compute Engine > VM Instances** page (<https://console.cloud.google.com/compute/instances>).
2. Click **Create Instance**.
3. Enter a name for the VM.
4. Choose a region and zone where the deployment will be performed.
5. Choose the machine type, as described in Section 3.3.
6. Change Boot disk to use custom image, and then select *Mediant VE/CE Image for Google Cloud* that you created in Section 3.1.
7. Expand the 'Management, security, disks, networking, sole tenancy' section.
8. Under the **Networking** tab, configure Network tags as "sbc".
9. For the primary network interface, configure the network, subnet, and external IP address.
10. Add additional network interfaces if needed and configure them accordingly.
11. Click **Create**.
12. Wait until the new instance is created. Wait an additional 5 minutes for the SBC software to fully start.
13. Determine the internal and external IP addresses assigned to the created instance.
14. Connect to the instance through one of the following:
  - Web browser
  - SSH client
  - Serial console (Google Cloud Platform Console > **Instance details** > **Connect to serial console**)

Default login credentials are:

- Username: **Admin**
- Password: **Admin**



You will be unable to connect to the instance using Google Cloud Platform Console's built-in SSH client. Instead, use an external client such as PuTTY.

**Figure 4-1: Creating New Instance via Google Cloud Platform Console**

Google Cloud Platform AudioCodes Prod

← Create an instance

To create a VM instance, select one of the options:

- New VM instance**  
Create a single VM instance from scratch
- New VM instance from template**  
Create a single VM instance from an existing template
- New VM instance from machine image**  
Create a single VM instance from an existing machine image
- Marketplace**  
Deploy a ready-to-go solution onto a VM instance

**Name** ⓘ  
Name is permanent  
sb-1

**Labels** ⓘ (Optional)  
+ Add label

**Region** ⓘ  
us-central1 (Iowa)

**Zone** ⓘ  
Zone is permanent  
us-central1-a

**Machine configuration**

**Machine family**  
General-purpose | Memory-optimized | Compute-optimized  
Machine types for common workloads, optimized for cost and flexibility

**Series**  
N1  
Powered by Intel Skylake CPU platform or one of its predecessors

**Machine type**  
n1-standard-2 (2 vCPU, 7.5 GB memory)

**CPU platform and GPU**

**Container** ⓘ  
☐ Deploy a container image to this VM instance. [Learn more](#)

**Boot disk** ⓘ  
New 10 GB standard persistent disk  
Image  
sb-7-2-256-511 [Change](#)

**Identity and API access** ⓘ

**Service account** ⓘ  
Compute Engine default service account

**Access scopes** ⓘ  
☒ Allow default access  
☐ Allow full access to all Cloud APIs  
☐ Set access for each API

**Firewall** ⓘ  
Add tags and firewall rules to allow specific network traffic from the Internet  
☐ Allow HTTP traffic  
☐ Allow HTTPS traffic

**Management** Security Disks **Networking** Sole Tenancy

**Network tags** ⓘ (Optional)  
sb-1

**Hostname** ⓘ  
Set a custom hostname for this instance or leave it default. Choice is permanent  
sb-1.c.audiocodes-prod.internal

**Network interfaces** ⓘ  
Network interface is permanent

**Network interface**

**Network** ⓘ  
oam

**Subnetwork** ⓘ  
oam (10.0.2.0/24)

**Primary internal IP** ⓘ  
Ephemeral (Automatic)

**External IP** ⓘ  
Ephemeral

**Network Service Tier** ⓘ  
☒ Premium (Current project-level tier, [change](#)) ⓘ  
☐ Standard (us-central1) ⓘ

**IP forwarding** ⓘ  
Off

**Public DNS PTR Record** ⓘ  
☐ Enable  
PTR domain name

[Done](#) [Cancel](#)

[+ Add network interface](#)

[Less](#)

You will be billed for this instance. [Compute Engine pricing](#) ⓘ

[Create](#) [Cancel](#)

**\$48.95 monthly estimate**  
That's about \$0.067 hourly  
Pay for what you use. No upfront costs and per second billing  
[Details](#)

## 5 Deploying Mediant VE via Stack Manager

This section describes the deployment of Mediant VE via Stack Manager.



This method is applicable to standalone and HA deployments.

### To deploy Mediant VE via Stack Manager:

1. Install the Stack Manager tool, as described in the *Stack Manager User's Manual*, which you can download from AudioCodes website at <https://www.audiocodes.com/library/technical-documents>.
2. Create a new Mediant VE stack via Stack Manager's **create** command, as described in the *Stack Manager User's Manual*.

**Figure 5-1: Creating New Instance via Stack Manager**

Create new stack

Name

stack-1

Stack type

Mediant VE

Environment

Google

Region

us-central1

Image

sbc-7-2-256-511

Compute

HA Mode

enable

VM Type

n1-standard-2

Networking

HA Subnet

cluster

Main Subnet

oam

1st Additional Subnet

-- none --

2nd Additional

-- none --

Admin User

Username

sbcadmin

Password

.....

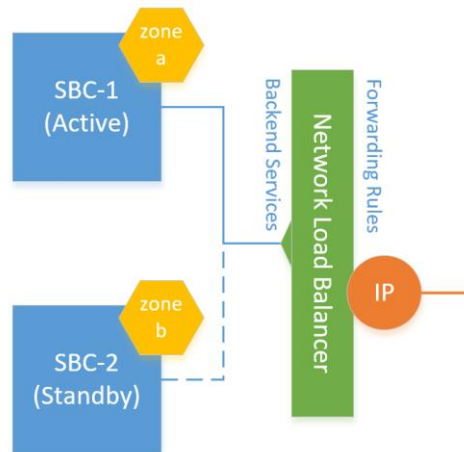
Create

Cancel

## 5.1 HA Deployment Topology

HA deployment of Mediant VE consists of two VM instances deployed across two availability zones of the Google Cloud region.

**Figure 5-2: HA Deployment Topology**



Communication is done through the IP addresses attached to Google Load Balancer that steers inbound (signaling and management) traffic towards the active SBC instance. The following load balancer types are used:

- Network Load Balancer for external IP addresses
- Internal Load Balancer for internal IP addresses

Google Load Balancers don't perform NAT translation and forward traffic without modifying the IP packet's destination address. Therefore, IP addresses (external and internal) attached to the Load Balancer are configured as secondary IP addresses in both SBC instances and should be used for all applications instead of primary IP addresses.



Primary IP addresses, for example "eth0", are still present in SBC instance's Interface Table. However, they *should not* be used. Instead, all applications, for example SIP Interfaces, should be connected to secondary IP addresses, for example, "eth0:1".

Communication via external IP addresses is through the Network Load Balancer. Since the Network Load Balancer supports only the primary VM's network interface, external IP addresses may be assigned *only* to the primary network interface (eth0) connected to the Main Subnet. Multiple external IP addresses on the primary network interface (eth0) are supported.

Communication via internal IP addresses is through the Internal Load Balancer. It may be connected to all network interfaces, connected to available subnets (Main, Additional 1, and Additional 2). Multiple internal IP addresses on the same network interface are supported.

## 5.2 External IP Addresses

During Mediant VE stack creation, Stack Manager lets you specify which subnets (and corresponding network interfaces) are assigned with public (external) IP addresses, using the **Public IPs** parameter in the **Networking** section.

If you choose to assign External IP addresses to some subnets, the following occurs:

### ■ HA Deployment:

Due to Google's Network Load Balancer limitations, external IP addresses may be assigned only to the Main subnet (connected via the primary VM network interface "eth0"). If you choose to assign external IP address to Main subnet, the following entities are created:

- External IP address.
- Two Regional Back-End Services for TCP and UDP traffic, respectively.
- Two Forwarding Rules (with `loadBalancingScheme == EXTERNAL`) that implement forwarding of incoming TCP and UDP traffic.
- Secondary IP address entries in the network Interfaces SBC configuration table of both SBC instances. Applications (e.g., SIP Interfaces) should be connected to these secondary IP addresses and not to primary IP addresses.

### ■ Standalone Deployment:

External IP addresses are assigned directly to the primary address of the corresponding network interface. It is possible to assign external IPs to any network interface.

For HA deployments, it is also possible to assign multiple external IP addresses to the Main subnet, by using the **public\_ips** advanced configuration parameter (in **Advanced Config** section). The example below assigns two external IP addresses to the Main subnet:

```
public_ips = main:2
```



When the **public\_ips** advanced configuration parameter is specified (in **Advanced Config** section), it overrides any value configured through **Public IPs** parameter in the **Networking** section.

It is not possible to assign multiple external IP addresses to the same subnet for standalone deployments, due to the limitations of Google Cloud.

## 5.3 Internal IP Addresses

If you choose not to assign the External IP Address to some subnets, the following entities are created for each corresponding subnet:

### ■ HA Deployment:

For each subnet that is configured not to use an External IP address, the following entities are created:

- Internal IP address.
- Two Regional Back-End Services for TCP and UDP traffic respectively.
- Two Forwarding Rules (with `loadBalancingScheme == INTERNAL`) that implement forwarding of incoming TCP and UDP traffic.
- Secondary IP address entries in the network Interfaces SBC configuration table of both SBC instances. Applications (e.g., SIP Interfaces) should be connected to these secondary IP addresses and not to primary IP addresses.

### ■ Standalone Deployment:

Regular internal IP addresses of the VM are used.

It's also possible to use both internal and external IP addresses on the same network interface (connected to a specific subnet) and/or use multiple internal IP addresses on the same network interface. This may be done by configuring the **additional\_ips** advanced configuration parameter (in **Advanced Config** section). For example, the following configuration for HA deployment:

```
Public IPs: "Main subnet"
Advanced Config:
    additional_ips = main
```

creates “eth0:1” external IP address, placed behind the Network Load Balancer, and “eth0:2” internal IP address, placed behind the Internal TCP/UDP Load Balancer.

## 5.4 Management Traffic

For HA deployment, if an external IP address is assigned to the Main subnet, by default it's also used for management traffic (Web, SSH, and SNMP). However, this may be changed by using the **oam\_ip** advanced configuration parameter:

- You may attach both external and internal IP addresses to the Main subnet and use the latter for management traffic by specifying:

```
Public IPs: "Main subnet"
Advanced Config:
    additional_ips = main
    oam_ip = internal
```

- You may move management traffic to Additional 1 or Additional 2 subnets by specifying their name as the **oam\_ip** parameter value, for example:

```
Public IPs: "Main subnet"
Advanced Config:
    oam_ip = additional1
```

## 6 Changing Network Configuration after Deployment

During initial deployment, Mediant VE automatically discovers all network interfaces and external IP addresses attached to it and populates corresponding network configuration tables accordingly.

If network configuration is changed after deployment (during normal Mediant VE operation), corresponding Mediant VE network configuration tables must be manually updated to match the updated Google Cloud configuration.

The following sections describe the most common network configuration changes to the deployed standalone Mediant VE instance and provide detailed instructions on how to perform them.

Change of networking configuration for Mediant VE HA deployment should be done through Stack Manager. Refer to the *Stack Manager User Manual* for details.

### 6.1 Adding a Network Interface



This section is applicable only to a standalone Mediant VE deployment performed via Google Cloud console. Change of networking configuration for Mediant VE deployments performed via Stack Manager should be done through the Stack Manager. Refer to Stack Manager User Manual for details.

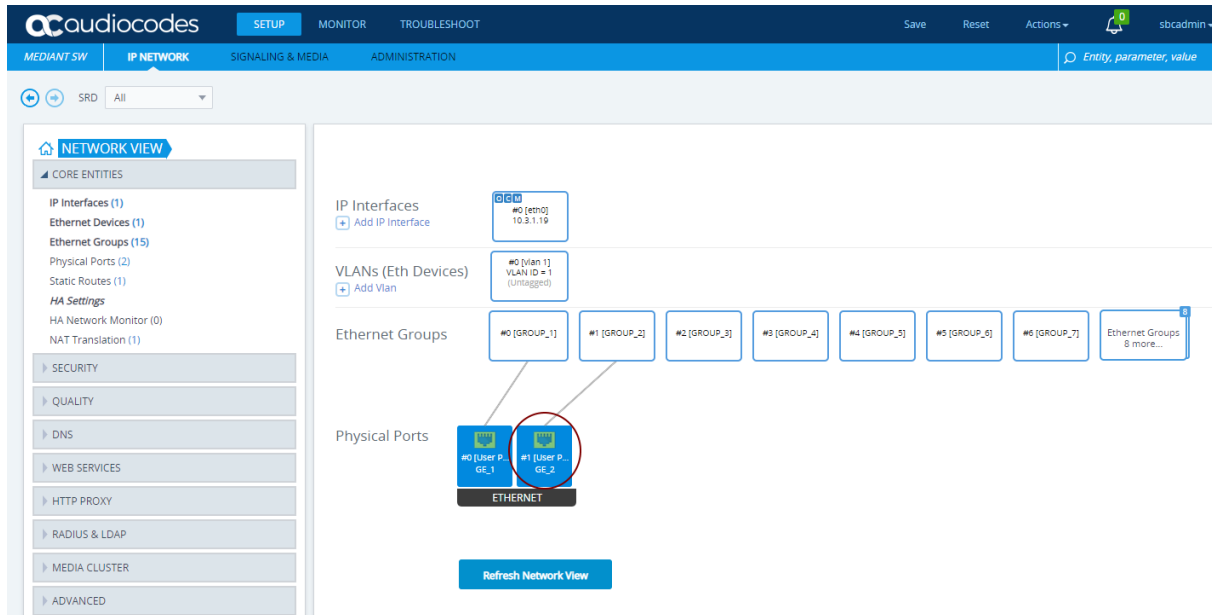
#### To add a network interface to deployed Mediant VE:

1. In the Google Cloud Platform Console, go to the **Compute Engine > VM Instances** page (<https://console.cloud.google.com/compute/instances>).
2. Stop the VM instance.
3. Click the VM instance, and then on the VM Instance Details page, click **EDIT**.
4. Add a new network interface and configure its properties.
5. Start the VM instance.
6. Determine the IP address of the created network interface.
7. Connect to the Mediant VE management interface through its Web interface.
8. Open the Network View page (**SETUP > IP NETWORK > NETWORK VIEW**).



Mediant VE detected a new network interface and created corresponding Physical Ports configuration object. The object is already attached to the corresponding Ethernet Group. However, Ethernet Device (VLAN) and IP Interface configuration is missing and must be manually created.

Figure 6-1: New Physical Ports Configuration Object



9. Click **Add Vlan** to create a new Ethernet Device (VLAN) configuration object, as follows:
  - Configure 'VLAN ID' as the next unused VLAN number.
  - Configure 'Tagging' as **Untagged**.
  - Configure 'Name' with a unique value (e.g., **vlan <VLAN ID>**).
  - Configure 'Underlying Interface' to reference the Ethernet Group associated with the new physical port.

Figure 6-2: New Ethernet Device (VLAN) Configuration

The screenshot shows the 'Ethernet Devices' configuration window with the 'GENERAL' tab selected. The fields are as follows:

GENERAL	
Index	1
Name	vlan 2
VLAN ID	2
Underlying Interface	#1 [GROUP_2] <a href="#">View</a>
Tagging	Untagged
MTU	1500

At the bottom of the window are two buttons: 'Cancel' and 'APPLY'.

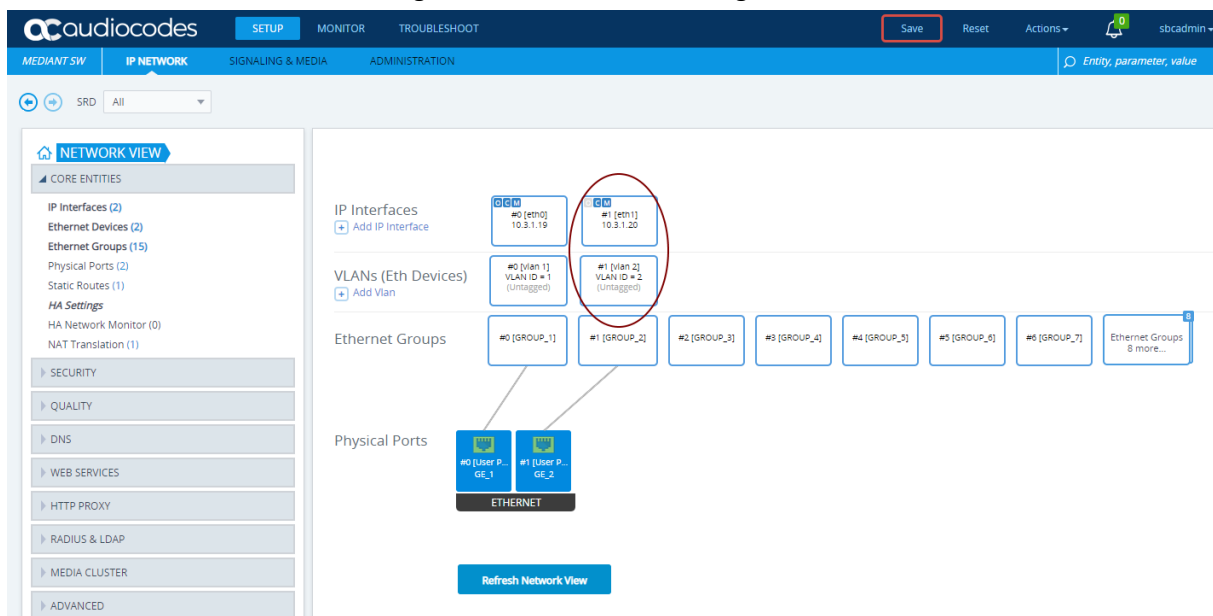
10. Click **Apply**; you are returned to the Network View page.

11. Click **Add IP Interface** to create a new IP Interface configuration object, as follows:
  - Configure 'IP Address' with the IP address of the created network interface (as determined in Step 6).
  - Configure 'Prefix Length' with the prefix length of the corresponding subnet.
  - Configure 'Default Gateway' with the corresponding default gateway.
  - Configure 'Name' with a unique value (e.g., **eth<id>**).
  - Configure 'Application Type' as **Media + Control**.
  - Configure 'Ethernet Device' to reference the Ethernet Device (VLAN) created in the previous step.

Figure 6-3: New IP Interface Configuration

12. Click **Apply**; you are returned to the Network View page.
13. Review the updated network configuration.

Figure 6-4: New Network Configuration



14. Click the **Save** button located on the toolbar to save the updated configuration.

## 6.2 Deleting the Network Interface

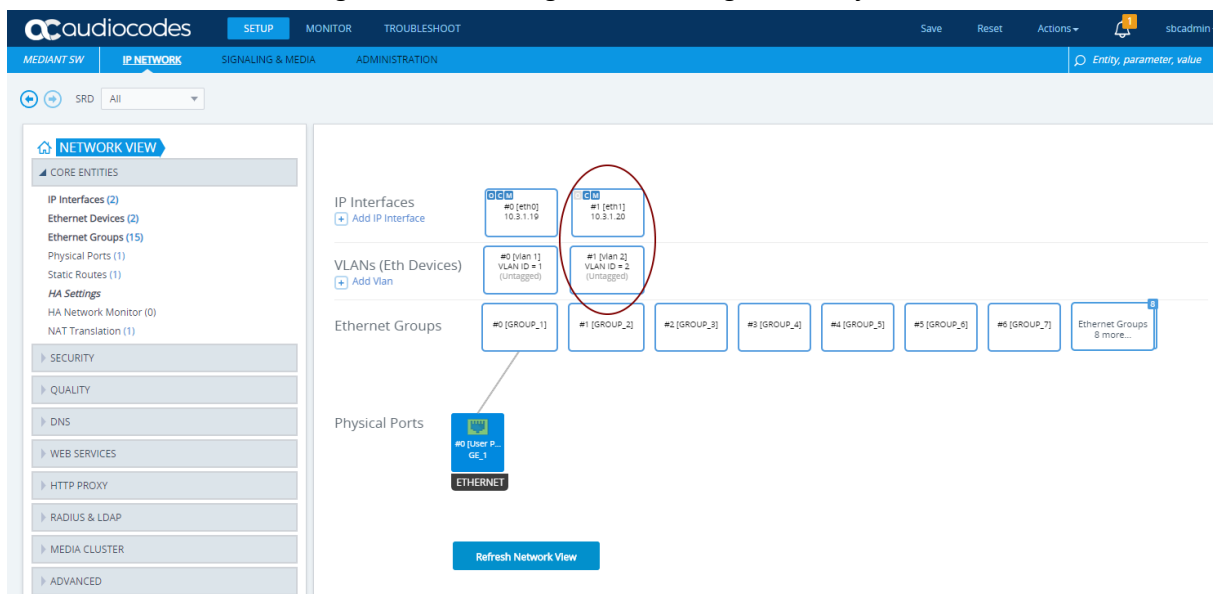


This section is applicable only to a standalone Mediant VE deployment performed via Google Cloud console. Change of networking configuration for Mediant VE deployments performed via Stack Manager should be done through the Stack Manager. Refer to Stack Manager User Manual for details.

### To delete network interface from deployed Mediant VE:

1. In the Google Cloud Platform Console, go to the **Compute Engine > VM Instances** page (<https://console.cloud.google.com/compute/instances>).
2. Stop the VM instance.
3. Click the VM instance, and then in the VM Instance Details screen, click **EDIT**.
4. Delete the new network interface.
5. Start the VM instance.
6. Connect to the Mediant VE management interface through its Web interface.
7. Open the Network View page (**SETUP > IP NETWORK > NETWORK VIEW**).
8. Locate the remaining network configuration objects that correspond to the deleted network interface.

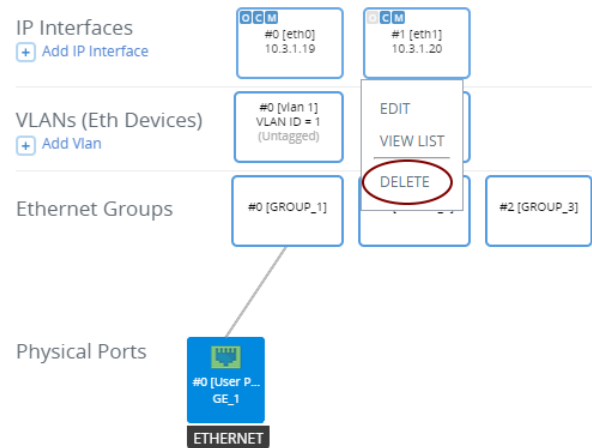
Figure 6-5: Remaining Network Configuration Objects



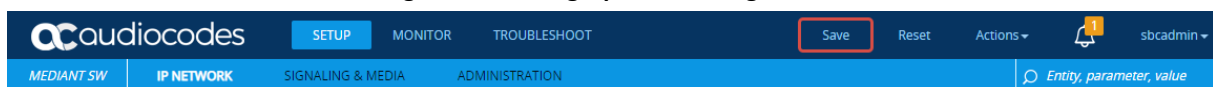
In the above example, the remaining network configuration objects include:

- IP Interface #1 [eth1]
- VLAN #1 [vlan 2]

9. Delete the remaining configuration objects—first the IP Interface and then the VLAN—by clicking them, and then from the shortcut menu, choosing **Delete**.

**Figure 6-6: Deleing Remaining IP Interface**

10. Click the **Save** button located on the toolbar to save the updated configuration.

**Figure 6-7: Saving Updated Configuration**

## 7 Licensing the Product

Once you have successfully completed Mediant VE deployment, you need to obtain, activate and then install your purchased SBC license.



By default, the product software installation provides a free license for up to three concurrent sessions (signaling and media) and three user registrations (far-end users). This allows you to evaluate the product prior to purchasing it with your required capacity and features. To allow call transcoding with this free license, you need to configure the 'SBC Performance Profile' parameter to **Optimize for Transcoding** (for more information, refer to the *User's Manual*).

### 7.1 Obtaining and Activating a Purchased License Key

For the product to provide you with all your capacity and feature requirements, you need to purchase a new License Key that allows these capabilities. The following procedure describes how to obtain and activate your purchased License Key.



- License activation is intended **only** for first-time software activation upon product purchase (or if your License Key is "lost", due to whatever reason). For subsequent software feature upgrades, the License Key file is e-mailed to you after your Purchase Order has been processed.
- For HA, each unit has its own Serial Number, Product Key and License Key. Therefore, the instructions in this section must be done for each unit.

To obtain and activate the License Key:

1. Open AudioCodes Web-based Software License Activation tool at <http://www.audiocodes.com/swactivation>:

Figure 7-1: Software License Activation Tool

The screenshot shows a web form titled "License Activation". It contains the following fields and elements:

- Product Key\***: A text input field.
- Fingerprint\***: A text input field.
- Email\***: A text input field with a "+" icon to its right.
- Validation**: A section containing a CAPTCHA image showing the characters "3ECF8". Below the image is a text input field for the user to enter the characters.
- Send**: A blue button at the bottom of the form.

Instructions on the page: "Please enter your Product Key received from AudioCodes and the fingerprint (e.g. Serial Number or Server Signature) that was generated as a result of your installation. For technical assistance, please contact AudioCodes support at support@audiocodes.com."

1. Enter the following information:

- **Product Key:** The Product Key identifies your specific Mediant VE SBC purchase for the purpose of subsequent communication with AudioCodes (for example, for support and software upgrades). The Product Key is provided in the Order Confirmation e-mail sent to you by AudioCodes upon your purchase, as shown in the example below:

**Figure 7-2: Product Key in Order Confirmation E-mail**



- **Fingerprint:** The fingerprint is the Mediant VE SBC's Serial Number. The Serial Number uniquely identifies the software installation. The Serial Number is displayed in the 'Serial Number' field on the Device Information page (**Monitor** menu > **Monitor** menu > **Summary** tab > **Device Information**).
  - **Email:** Provide one or more e-mail addresses to where you want the License Key to be sent.
2. Click **Send** to submit your license activation request.
3. Once AudioCodes processes and completes your license activation, you will receive an e-mail notification with the License Key file attached. Open the file with any text-based program (such as Notepad) and make sure that the serial number ("**S/N**") in the License Key is correct and reflects the Serial Number of your Mediant VE SBC.



Do not modify the contents of the License Key file.

## 7.2 Installing the License Key

For installing the License Key on Mediant VE, refer to the *Mediant Software SBC User's Manual*.



- The License Key installation process includes a device reset and is therefore traffic-affecting. To minimize disruption of current calls, it is recommended to perform this procedure during periods of low traffic.
- The License Key file for Mediant VE HA contains two License Keys - one for the Active device and one for the Redundant device. Each License Key has a different serial number ("S/N"), which reflects the serial number of each device in the HA system.

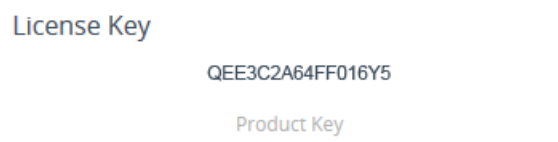
## 7.3 Product Key

The Product Key identifies a specific purchase of your device installation for the purpose of subsequent communication with AudioCodes (e.g., support and software upgrades). The Product Key is provided in the order-confirmation email sent to you upon your product purchase and is used for activating your license through AudioCodes Software License Activation tool.

The Product Key is included in the License Key. Once the License Key is installed, you can view the Product Key in the following Web pages:

- License Key page (**Setup** menu > **Administration** tab > **License** folder > **License Key**). The Product Key is displayed in the read-only 'Product Key' field, as shown in the example below:

**Figure 7-3: Viewing Product Key**

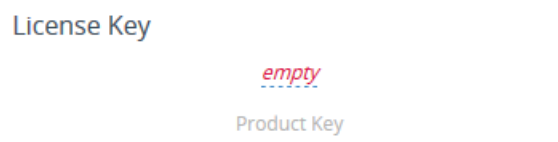


- Device Information page (**Monitor** menu > **Monitor** tab > **Summary** folder > **Device Information**).

If your License Key was purchased in an earlier version (for example, 7.0), the 'Product Key' field may appear empty. In such a scenario, request the Product Key from your AudioCodes sales representative. Once received, do the following:

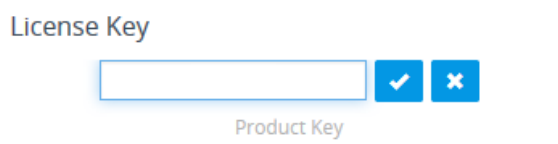
1. Open the License Key page.
2. Locate the Product Key group:



**Figure 7-4: Empty Product Key Field**



3. Click "empty"; the following appears:

**Figure 6-7-5: Entering Product Key**



4. In the field, enter the Product Key, and then click **Submit**  (or **Cancel**  to discard your entry).

**International Headquarters**

Naimi Park  
6 Ofra Haza Street  
Or Yehuda, 6032303, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

80 Kingsbridge Rd  
Piscataway, NJ 08854, USA  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com>

©2025 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-11027

