Installation Manual

AudioCodes Mediant™ Family of Session Border Controllers (SBC)

Mediant Cloud Edition (CE)

Deployment in Google Cloud

Version 7.4

audiocodes

Table of Contents

List of Figures

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: May-16-2023

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.

Related Documentation

Manual Name
Release Notes
Stack Manager for Mediant VE-CE SBC User's Manual
Mediant Software SBC User's Manual

Document Revision Record

LTRT	Description
10865	Initial document release for Version 7.4
10869	Instance types updated; miscellaneous
10872	Creating private EC2 endpoint in Cluster subnet added; note added to software upgrade; downgrading software section added
10875	Note added regrading IP version support
10876	VM sizes (Standard_D8s_v3)
10879	Mediant CE notice in upgrade section
10891	NW prerequisites; internal/external IPs; machine types; management traffic
10892	Updates to redundancy deployment options
10897	Instance types m5.2xlarge, m5n.large, m5n.xlarge; Standard_D8ds_v4 for SC; Firewall Rules section updated
10913	Dedicated document for Mediant CE for Google Cloud

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

Mediant Cloud Edition (CE) Session Border Controller (SBC), hereafter referred to as *Mediant CE*, is a software-based product that can be deployed in one of the following operational environments:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- OpenStack
- Non-cloud virtual environments (e.g. VMware)

This document describes deployment of Mediant CE in a Google Cloud environment.

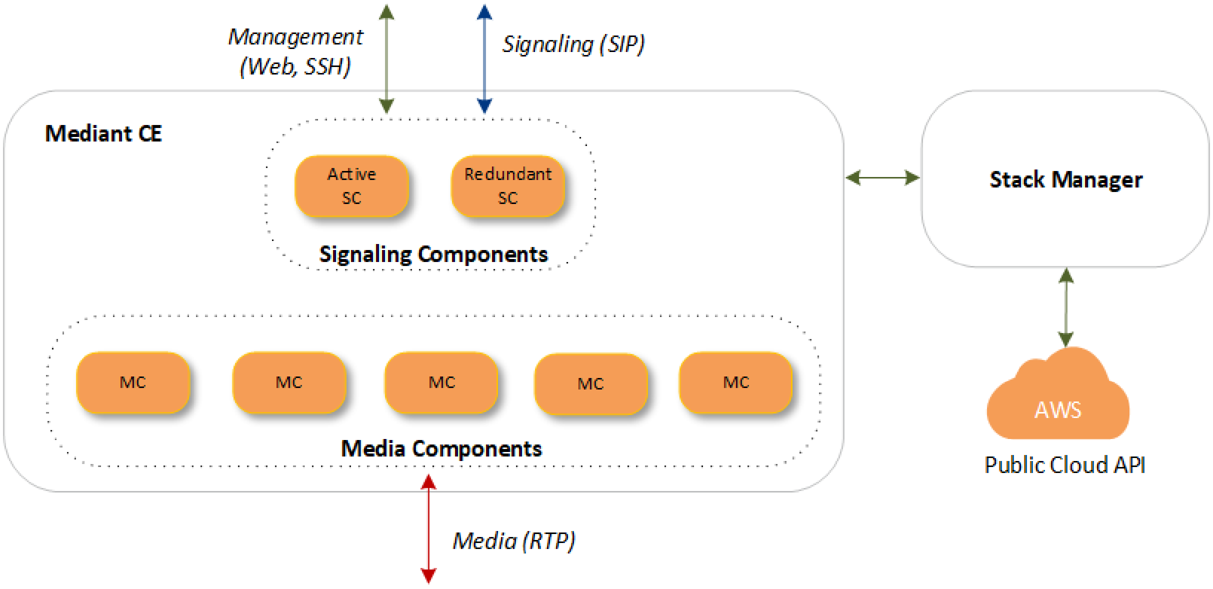
For detailed instructions on Mediant CE installation in other operational environments (for example, VMware), refer to the dedicated installation manual.

Note:

- The scope of this document does not fully cover security aspects for deploying the product in the Google Cloud. Security measures should be done in accordance with Google Cloud security policies and recommendations.
- For configuring Mediant CE SBC, refer to the *Mediant Software SBC User's Manual*.
- Mediant CE deployments support only IPv4 addresses (not IPv6).

1.1 Architecture Overview

Figure 1-1: Mediant CE Architecture



Mediant CE cluster is comprised of multiple components (virtual machines) that perform distinct functions:

- **Signaling Components:** Handle signaling (SIP) and management (Web, SSH, etc) traffic. It also determines which Media Component (see below) handles the specific media traffic, which is based on load balancing between the Media Components.

- **Media Components:** Handle media (RTP, RTCP) traffic, including transcoding functionality. Up to 21 Media Components can be used in the deployed Mediant CE.

Incoming calls are initially processed (at signaling level) by Signaling Components, that choose a Media Component based on the current cluster utilization and pass the media streams to it.

Signaling Components also serve as a “single point of contact” for all management tasks. They provide Web and CLI interfaces through which customers have complete control over all cluster components.

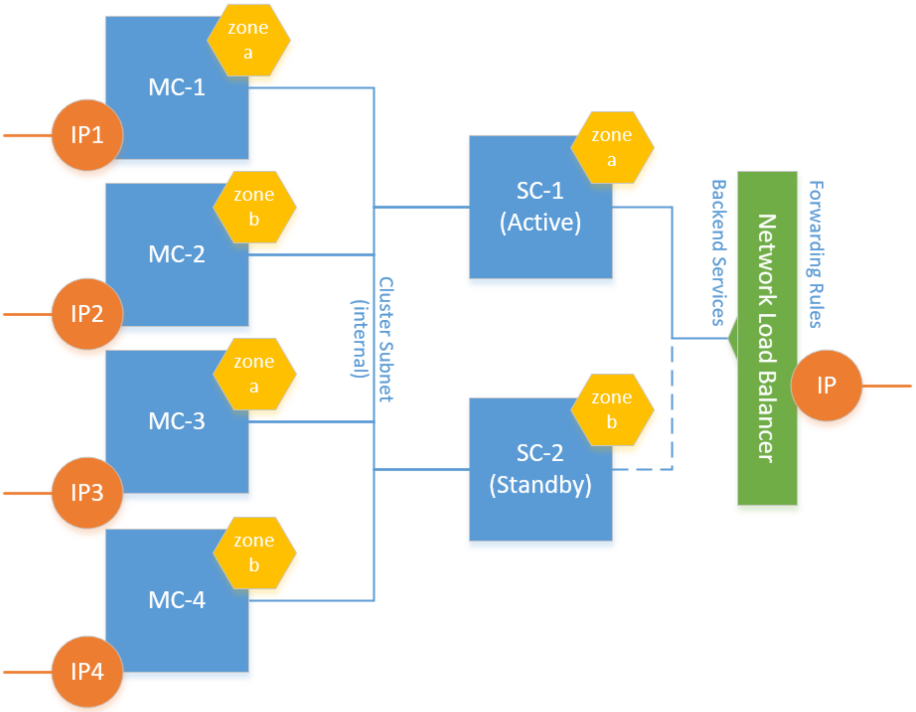
1.2 Deployment Topology

In a typical Mediant CE deployment, two Signaling Components are created and operate in 1+1 Active / Standby mode. They are placed behind Google Load Balancer to enable preservation of management and signaling IP addresses, as well as established calls, during a switchover.

Mediant CE cluster may contain up to 21 Media Components that operate in N+1 Load Sharing mode. In case of specific Media Component failure, calls handled by it are re-distributed across remaining Media Components, with no visible effect on established calls.

Mediant CE components are deployed across two availability zones of the Google Cloud region.

Figure 1-2: Mediant CE Deployment Topology (Google)



It is possible to adjust cluster size by scaling Media Components “in” or “out” based on cluster utilization and/or explicit customer request. ”Scaled down” Media Components are kept in “stopped” state, which ensures that they can be quickly started during “scale out” operations.

1.3 Google Load Balancer

Communication with Signaling Components is performed via the IP addresses attached to Google Load Balancer that steers inbound (signaling and management) traffic towards the active Signaling Component. The following load balancer types are used:

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

Google Load Balancer doesn't perform NAT translation and forwards 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 Signaling Components and should be used for all applications instead of primary IP addresses.

Note: Primary IP addresses, for example "eth0", are still present in the Signaling Component's IP Interfaces 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".

Since Network Load Balancer supports only the primary virtual machine's network interface, external IP addresses may be assigned *only* to the "eth0" network interface of Signaling Components connected to the Main subnet. Multiple external IP addresses are supported.

Internal IP addresses may be used to communicate with Signaling Components via Internal Load Balancer that may be connected to all available subnets (Main, Additional 1, and Additional 2).

Communication with Media Components is performed via internal and external IP addresses directly attached to them and doesn't require any Load Balancer configuration.

1.4 Stack Manager

The Stack Manager tool is provided as part of the solution. It is used for initial Mediant CE cluster deployment and complete lifecycle management; for example update of network topology, rebuild of cluster components in case of underlying cloud resources corruption or accidental removal etc.

Stack Manager also supports automatic scaling of Media Components based on cluster utilization, thus significantly reducing associated infrastructure costs.

2 Installation Prerequisites

Prior to installing Mediant CE in the Google Cloud, 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 AudioCodes Mediant VE/CE Image.
- You have created all subnets needed for Mediant CE deployment. For more information, see Section Network Prerequisites.

2.1 AudioCodes Mediant VE/CE Image

> **Note:** Mediant VE and CE products share the same software image published by AudioCodes.

To deploy Mediant CE 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.

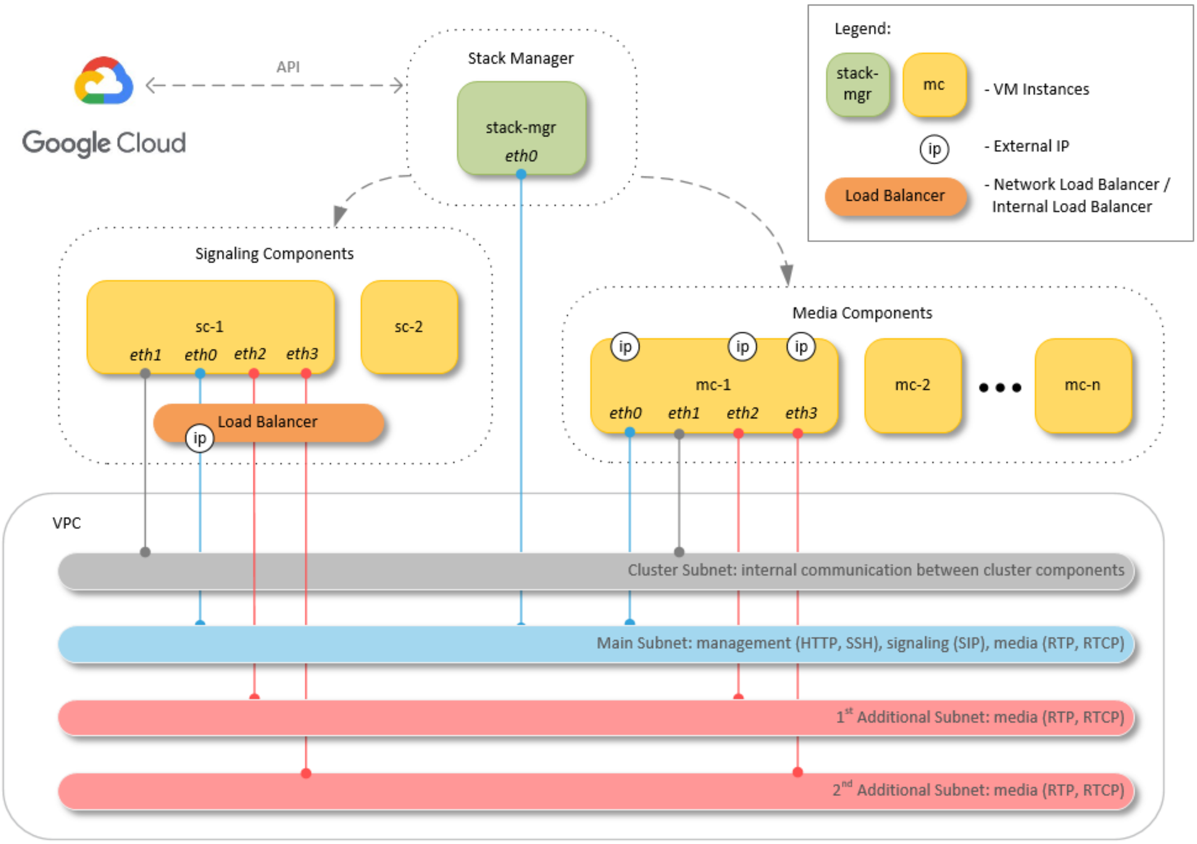
➢ To upload Mediant VE/CE image to Google Cloud image repository:

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. Wait until the upload completes.
7. Go to the Compute Engine > Images page https://console.cloud.google.com/compute/images.
8. Click **Create Image**.
9. Enter an image name.
10. Specify the source as the Cloud Storage file, and then choose the .tar.gz file that you uploaded in previous steps.
11. Specify the location where Mediant CE will be deployed.
12. Specify the additional properties for your image (e.g. family or description).
13. Click **Create** to create the image.

2.2 Network Prerequisites

Mediant CE on Google Cloud uses the following network architecture:

Figure 2-1: Mediant CE Network Architecture – Google Cloud


Google Cloud
API
Stack Manager
stack-mgr
eth0
Legend:
stack-mgr
mc
- VM Instances
ip
- External IP
Load Balancer
- Network Load Balancer / Internal Load Balancer
Signaling Components
sc-1
eth1
eth0
eth2
eth3
sc-2
Load Balancer
ip
Media Components
ip
ip
ip
mc-1
eth0
eth1
eth2
eth3
mc-2
mc-n
VPC
Cluster Subnet: internal communication between cluster components
Main Subnet: management (HTTP, SSH), signaling (SIP), media (RTP, RTCP)
1st Additional Subnet: media (RTP, RTCP)
2nd Additional Subnet: media (RTP, RTCP)

Up to four subnet may be used:

- **Cluster Subnet:** Carries internal communication between Mediant CE components; connected to both signaling and Media Components as the second network interface (eth1).
- **Main Subnet:** Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic; connected to both Signaling Components and Media Components as the first network interface (eth0). It is also recommended to connect Stack Manager to the Main subnet to simplify communication with deployed Mediant CE stack.
- **1st and 2nd Additional Subnets:** Carries media (RTP, RTCP) traffic; connected to Media Components only as the third and fourth network interfaces (eth2 and eth3) correspondingly. These subnets are optional, as the Main Subnet may carry all types of traffic.

Each subnet must reside in a different virtual network.

All needed subnets must be created prior to Mediant CE deployment.

During deployment, Stack Manager creates all relevant Mediant CE components, including Signaling Component and Media Component instances, load balancer and external IP addresses.

2.3 Firewall Rules

Stack Manager versions earlier than 2.8.1 required manual creation of firewall rules prior to Mediant CE deployment. For Stack Manager versions 2.8.1 and later, this is no longer needed because firewall rules are automatically created during stack deployment.

2.4 Machine Types

The following machine types are used by default Mediant CE deployment:

- **Signaling Component instances:** n2-standard-8
- **Forwarding Media Component instances:** n2-standard-2 (for two network interfaces) or n2-standard-4 (for three or four network interfaces)
- **Transcoding Media Component instances:** n2-standard-8

You may customize machine types during stack creation.

Refer to the SBC Series Release Notes for a complete list of machine types supported by Mediant CE, their capacities and capabilities.

This page is intentionally left blank.

3 Deploying Mediant CE

Deployment of Mediant CE on Google Cloud is performed via the Stack Manager.

Stack Manager is a management tool developed by AudioCodes that enables simple and intuitive deployment and complete lifecycle management of Mediant VE and Mediant CE products on public clouds. The tool provides the following features for Mediant CE:

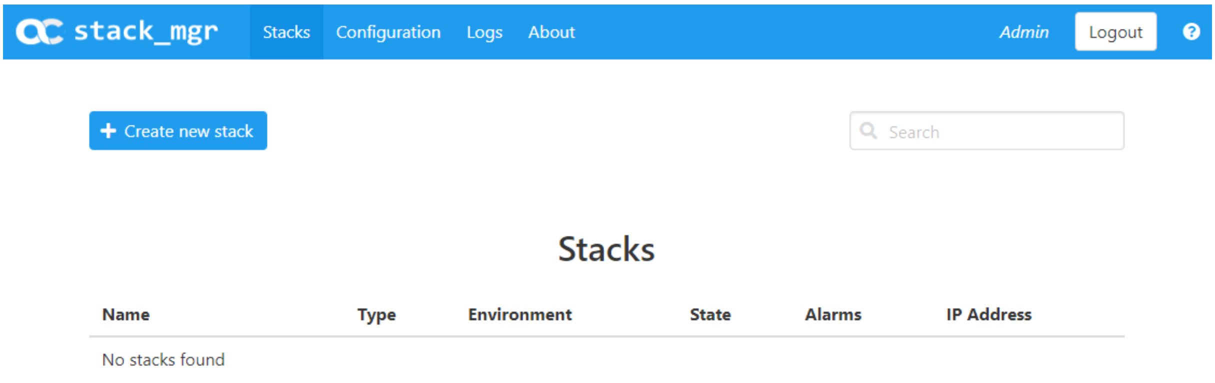
- Initial product deployment.
- Update of deployed stack’s network topology
- Automatic and on-demand scaling of Media Components, to adjust stack footprint and minimize infrastructure costs.
- Monitoring of deployed Azure resources and recovery in case of their corruption / accidental removal
- Upgrade of software on all Mediant CE components
- Removal of all deployed resources in case of stack deletion

Stack Manager uses dynamically generated Deployment Manager templates for stack deployments on Google Cloud and is not involved in call processing or any other services provided by Mediant CE.

➢ **To deploy Mediant CE:**

1. Install the Stack Manager tool, as described in the Stack Manager User's Manual.
2. Log into the Stack Manager tool after the deployment; the following screen appears:

Figure 3-1: Stack Manager Main Screen

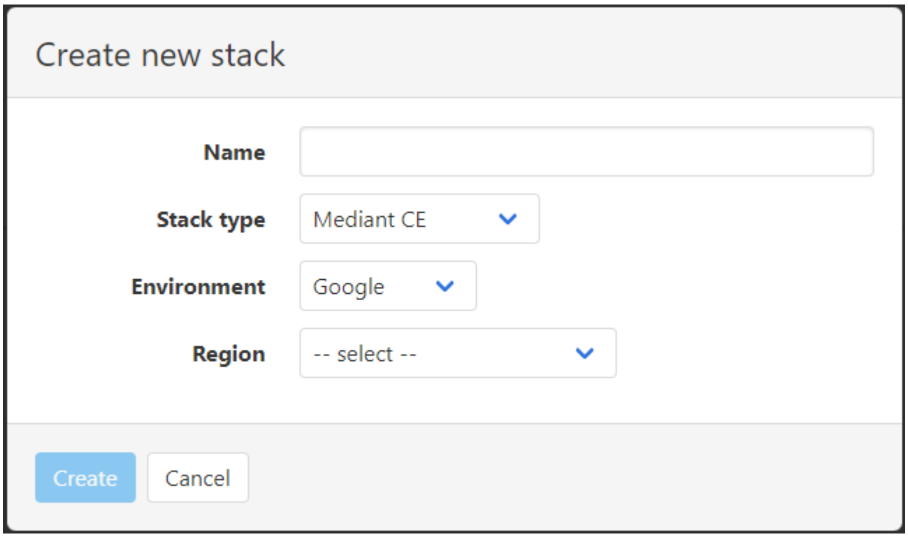


Stacks

Name	Type	Environment	State	Alarms	IP Address
No stacks found					

3. Click **Create** to create a new stack; the following dialog box appears:

Figure 3-2: Create Stack Dialog – Step 1



Create new stack

Name:

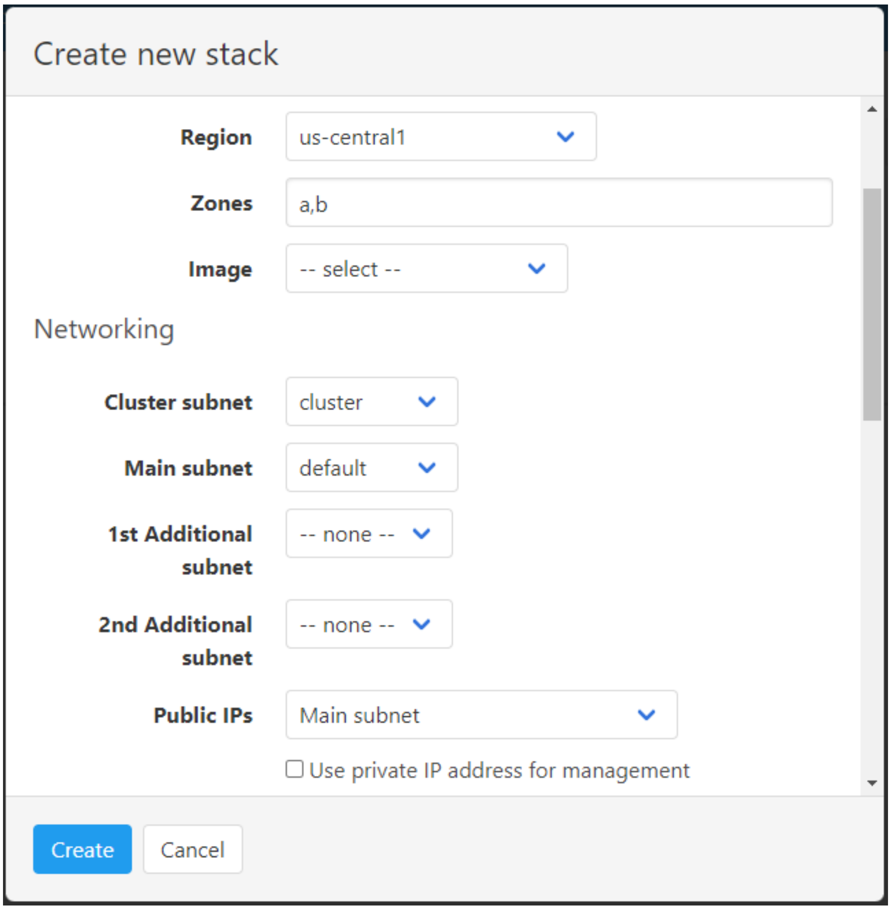
Stack type: Mediant CE

Environment: Google

Region: -- select --

4. In the 'Name' field, enter the name of the stack (e.g., “mediant-ce”).
5. From the 'Stack type' drop-down list, select Mediant CE.
6. From the 'Region' drop-down list, select a region where the stack will be deployed; additional fields appear:

Figure 3-3: Create Stack Dialog – Step 2



Create new stack

Region: us-central1

Zones: a,b

Image: -- select --

Networking

Cluster subnet: cluster

Main subnet: default

1st Additional subnet: -- none --

2nd Additional subnet: -- none --

Public IPs: Main subnet

□ Use private IP address for management

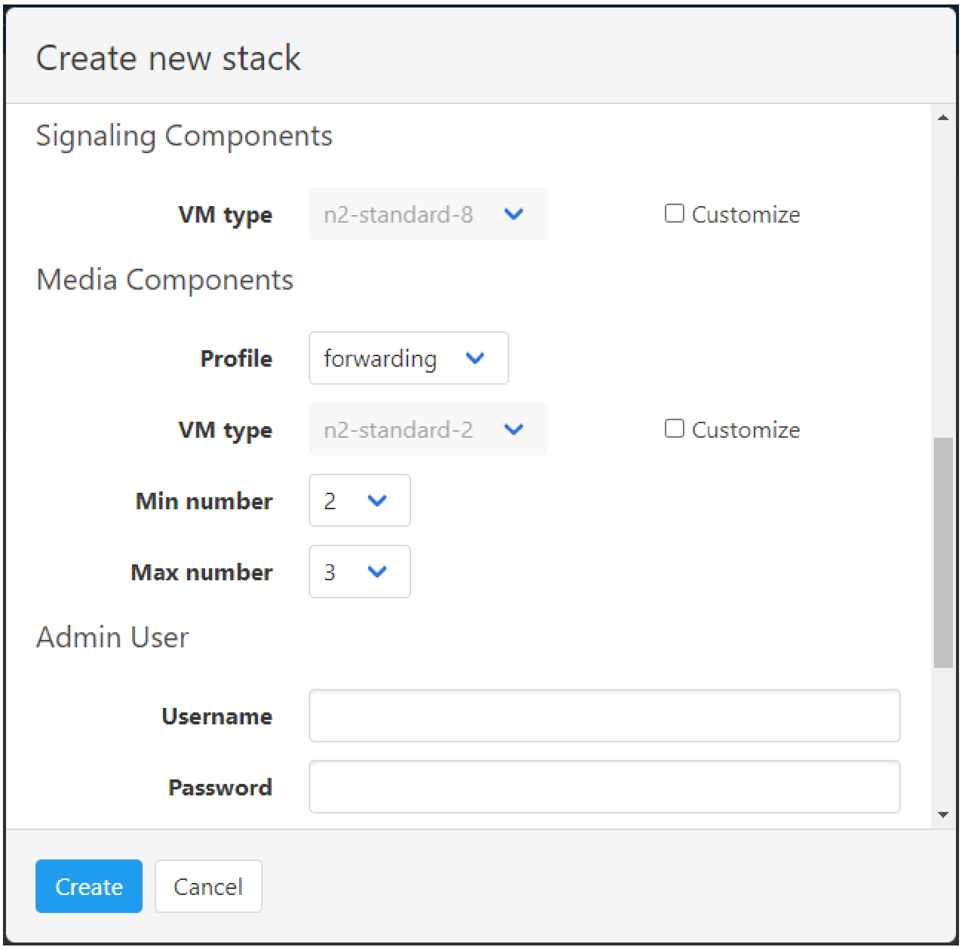
7. In the 'Zones' field, enter the zones where Mediant CE will be deployed. The value is a comma-separated list of two zone names (e.g., “a,b”).
8. From the 'Image' drop-down list, select the Mediant VE/CE image that you uploaded to your account, as described in Section AudioCodes Mediant VE/CE Image.

9. Select the subnets that Mediant CE will be connected to.

10. From the 'Public IPs' drop-down list, select which subnets need to communicate with external equipment via public IP addresses. Based on the selected value, Stack Manager places corresponding Signaling Component's network interfaces behind Public or Internal Load Balancer and assigns public IP addresses to the Media Components.

11. If you assign Public IP address to the Main subnet, Stack Manager by default configures the corresponding Network Load Balancer's frontend IP address as Mediant CE's management IP address and uses it for communicating with the deployed stack. You may override this behaviour, by selecting the 'Use private IP address for management' checkbox. In this case, Stack Manager creates an additional (secondary) IP address on the Signaling Component's first network interface (eth0), attached to the Main subnet, places it behind the Internal Load Balancer, configures this Internal Load Balancer's frontend IP address as Mediant CE's management IP address, and uses it to communicate with the deployed stack.

Figure 3-4: Create Stack Dialog – Step 4



Create new stack

Signaling Components

VM type: n2-standard-8 ☐ Customize

Media Components

Profile: forwarding

VM type: n2-standard-2 ☐ Customize

Min number: 2

Max number: 3

Admin User

Username:

Password:

12. The VM type for both Signaling Components and Media Components is pre-selected and automatically updated based on other parameters that you define in the Create Stack dialog box. If you want to modify it, select the 'Customize' checkbox next to it and select a value from the 'VM type' drop-down list.

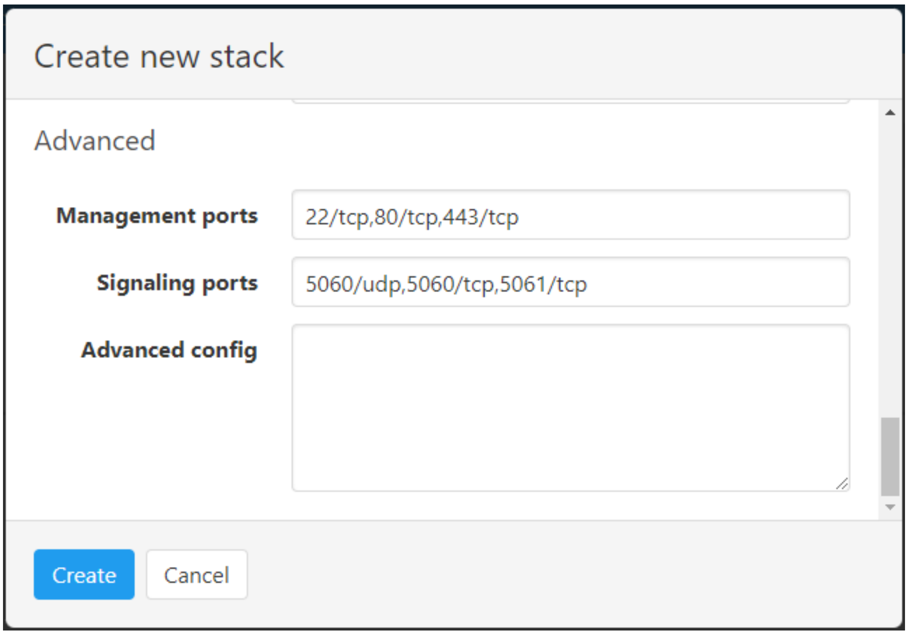
13. From the 'Profile' drop-down list, select whether you need Media Components to perform simple media stream **forwarding** (includes RTP-to-SRTP translation and vice versa) or need **transcoding** capabilities (for coder conversion or DTMF detection).

14. In the 'Min number' and 'Max number' drop-down lists, select the minimum and maximum number of Media Components in the stack. Stack Manager creates the configured maximum number of Media Components, but initially starts only with the

minimum number of them. You may later adjust the number of running Media Components via **scale out** and **scale in** actions.

15. In the 'Username' and 'Password' fields, enter the admin user credentials that will be configured on the deployed stack. You use these credentials when connecting to the stack via Web or CLI management interfaces. Note that Stack Manager uses different credentials to communicate with the stack – **StackMgr** user and randomly generated password. Therefore, even if you later change admin user credentials (e.g., via Mediant CE's Web or CLI interface) communication between Stack Manager and the deployed Mediant CE stack is not affected.

Figure 3-5: Create Stack Dialog – Step 5



Create new stack

Advanced

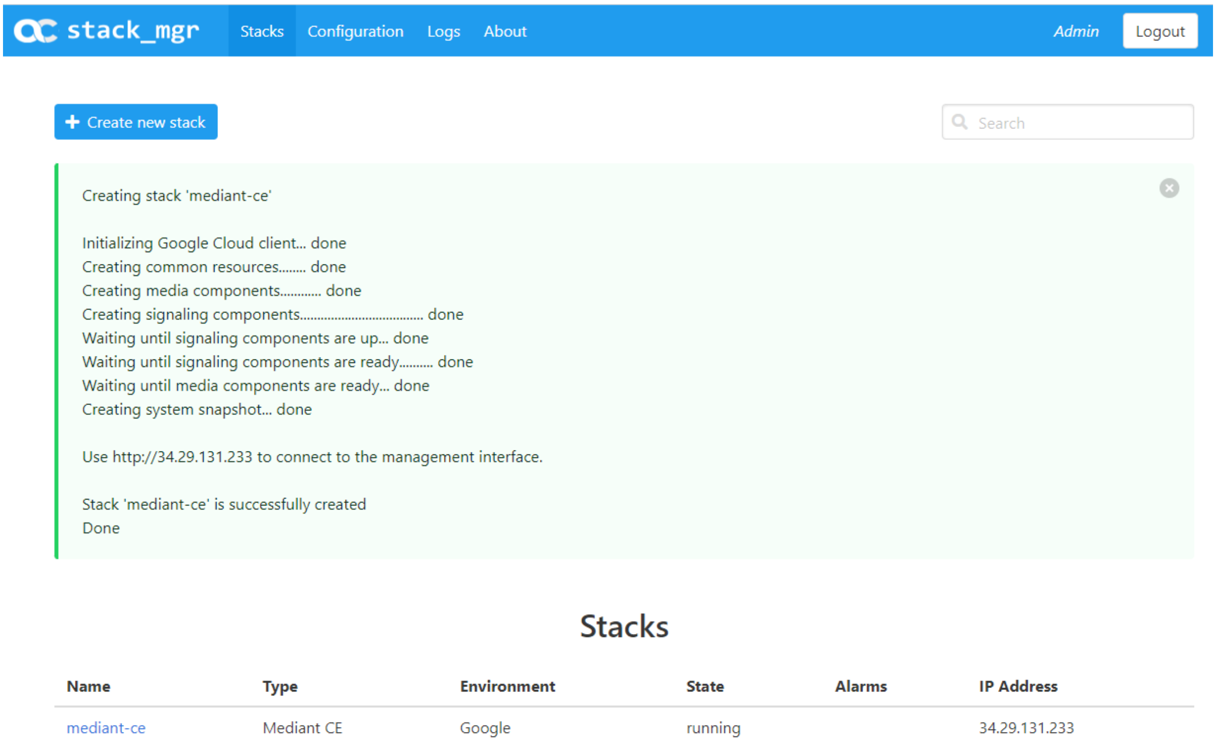
Management ports: 22/tcp,80/tcp,443/tcp

Signaling ports: 5060/udp,5060/tcp,5061/tcp

Advanced config:

16. In the 'Management ports' and 'Signaling ports' fields, enter a list of management and signaling ports respectively that should be open on Mediant CE. Firewall rules are then configured for specified ports, and corresponding rules are created in Google Load Balancer. The value is a comma-separated list of the following elements:
    - <port>/udp: Opens a specific UDP port for all sources (e.g., 161/udp)
    - <port>/udp/<cidr>: Opens a specific UDP port for traffic originating from a specific CIDR (e.g., 161/udp/172.16.0.0/16 opens UDP port 161 for traffic from 172.16.0.0/16 subnet)
    - <port>/tcp: Opens a specific TCP port (e.g., 22/tcp)
    - <port>/tcp/<cidr>: Opens a specific TCP port for traffic originating from a specific CIDR (e.g., 22/tcp/172.16.1.0/24)
17. In the 'Advanced config' text box, enter advanced configuration parameters, if needed. See the next sections for a partial list of supported advanced configuration parameters. Refer to *Stack Manager User's Manual* for a complete list.
18. Click **Create** to start stack creation.
19. Wait until stack is created.

Figure 3-6: Successful Stack Creation



```
Creating stack 'mediant-ce'

Initializing Google Cloud client... done
Creating common resources........ done
Creating media components........... done
Creating signaling components.................................. done
Waiting until signaling components are up... done
Waiting until signaling components are ready......... done
Waiting until media components are ready... done
Creating system snapshot... done

Use http://34.29.131.233 to connect to the management interface.

Stack 'mediant-ce' is successfully created
Done
```

Stacks

Name	Type	Environment	State	Alarms	IP Address
mediant-ce	Mediant CE	Google	running		34.29.131.233

3.1 External IP Addresses

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

Stack Manager by default applies the same configuration for both Signaling Components and Media Components. For each subnet that is configured to use a Public IP address, the following is created:

Note:

- Due to Google Network Load Balancer limitations, external IP addresses may be assigned only to the Signaling Component's Main subnet, connected to the primary network interface "eth0".
- Due to Google Cloud limitations, it is impossible to assign more than one external IP address to the Media Component's network interface.

- **For Signaling Components**:
  - 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 IP Interfaces configuration table of both Signaling Components. Applications (e.g., SIP Interfaces) should be connected to these secondary IP addresses and not to primary IP addresses.

- **For Media Components**:

  External IP addresses are assigned directly to the primary address of the corresponding network interface. it's possible to assign external IPs to any network interface, except for the one connected to the Cluster Subnet.

You can specify different configuration for Signaling Components and Media Components. It is also possible to assign multiple external IP addresses to the Main subnet for Signaling Components, by using the **sc_public_ips** and **mc_public_ips** advanced configuration parameter in **Advanced Config** section.

> **Note:** When the **sc_public_ips** or **mc_public_ips** advanced configuration parameter is specified in the **Advanced Config** section, it overrides any value configured via the **Public IPs** parameter in the **Networking** section for the corresponding components (Signaling Component or Media Component).

- **sc_public_ips**

  Contains a comma-separated list of subnet names (only “main” is valid for Google Cloud), which are assigned with public IP addresses and optionally, with the number of public IP addresses on the corresponding network interface.

  For example, below configuration attaches two external IP addresses to the network interface connected to the Main subnet (eth0):

  ```
  sc_public_ips = main:2
  ```

- **mc_public_ips**

  Same as above, but for Media Component network interfaces.

  For example:

  ```
  mc_public_ips = main,additional1:2
  ```

3.2 Internal IP Addresses

For each subnet that is configured **not** to use a Public IP address, the following is created:

- **For Signaling Components**:
  - 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 IP Interfaces configuration table of both Signaling Components. Applications (e.g., SIP Interfaces) should be connected to these secondary IP addresses and not to primary IP addresses.
- **For Media Components:**
  - Regular internal IP addresses of the virtual machine 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 **sc_additional_ips** or **mc_additional_ips** advanced configuration parameters in the **Advanced Config** section.

For example, the below configuration creates on Signaling Components the "eth0:1" external IP address, placed behind the Network Load Balancer, and "eth0:2" internal IP address, placed behind the Internal Load Balancer:

```
sc_public_ips = main
sc_additional_ips = main
```

3.3 Management Traffic

By default, the primary IP address of the "eth0" network interface, connected to the Main subnet, is used for management traffic (Web, SSH, and SNMP).

If the Main subnet is configured to use the Public IP address, this IP address is placed behind the Network Load Balancer. Mediant CE management should be performed via the corresponding Load Balancer's external IP address.

If the Main subnet is configured **not** to use a Public IP address, this IP address is placed behind the Internal Load Balancer. Mediant CE management should be performed via the corresponding Load Balancer's internal IP address.

You may use the 'Use private IP address for management' parameter during Mediant CE creation to create both private and public IP addresses on the Main subnet (placed behind the Internal and Network Load Balancers, respectively) and use a private IP address for management. The same may be achieved by configuring the **oam_ip** advanced configuration parameter after stack creation:

```
oam_ip = internal
```

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

```
sc_public_ips = main
oam_ip = additional1
```

3.4 Firewall Rules

Stack Manager creates firewall rules during Mediant CE deployment that enable only relevant traffic for each component and subnet. These firewall rules are assigned to unique tags created for both Signaling Components and Media Components during deployment.

The following table lists the default firewall rules. You may change signaling and media rules by updating the 'Signaling ports' and 'Media ports' parameters, as described previously.

Table 3-7: Inbound Rules for Default Security Groups

Component	Traffic	Subnet	Protocol	Port
Signaling Component	SSH	Main	TCP	22
	HTTP	Main	TCP	80
	HTTPS	Main	TCP	443
	SIP over UDP	▪ Main ▪ Additional1 ▪ Additional2	UDP	5060
	SIP over TCP/TLS	▪ Main ▪ Additional1 ▪ Additional2	TCP	5060, 5061
	Keep-alives from Azure Load Balancer	▪ Main ▪ Additional1 ▪ Additional2	TCP	315
Media Component	RTP, RTCP	▪ Main ▪ Additional1 ▪ Additional2	UDP	6000-65535
All	Internal	Cluster	UDP	669, 680, 925, 3900
		Cluster	TCP	80, 2442, 224

Inbound security rules in the Main and Additional subnets are configured by default to accept all traffic, including management traffic, from all sources, which constitutes a significant security risk. It's highly recommended to modify them after Mediant CE creation to allow inbound traffic only from specific IP addresses / subnets, especially for management traffic.

Inbound security rules in the Cluster subnet are configured by default to accept traffic from Mediant CE instances. Therefore, there is no need to further adjust them.

3.5 Deployment Troubleshooting

Stack Manager uses dynamically generated Deployment Manager templates to perform deployment on Google Cloud.

If Mediant CE deployment fails and the error description provided by Stack Manager is not detailed enough, refer to the Deployment Manager logs for additional information.

4 Upgrading Software Version

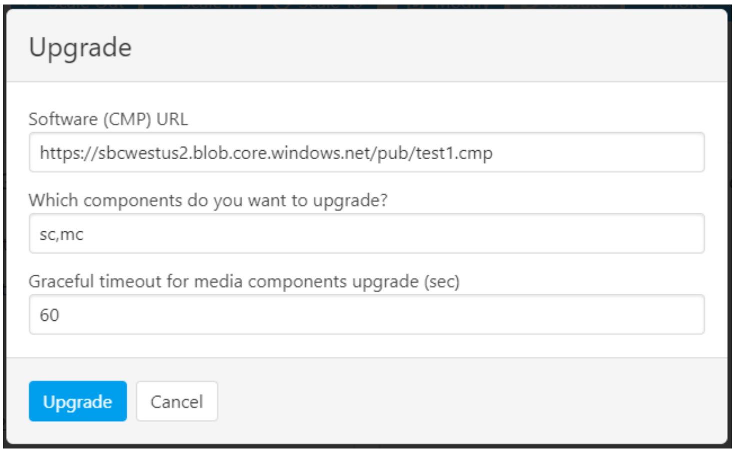
IMPORTANT NOTICE

For upgrading Mediant CE SBC to a version using a digitally signed .cmp file, you **must** follow the upgrade prerequisites and instructions in the document Mediant SW-90xx SBC Signed-CMP Upgrade Procedure Configuration Note.

You may upgrade the software version of the deployed Mediant CE using the Software Version file (.cmp) through one of the following means:

- Using Mediant CE Web interface:
  - Upgrade Signaling Components using the Software Upgrade Wizard (**Action > Software Upgrade**).
  - Upgrade "active" (currently running) Media Components using the Cluster Management page (**SETUP > IP NETWORK > MEDIA CLUSTER > Cluster Management**).
  - Upgrade "idle" (currently stopped) Media Components using Stack Manager (**Update Idle MCs**).
- Using Stack Manager's Web interface:
  - Upgrade all components at once using the **Upgrade** operation

Figure 4-1: Upgrading Mediant CE via Stack Manager



Upgrade

Software (CMP) URL: https://sbcwestus2.blob.core.windows.net/pub/test1.cmp

Which components do you want to upgrade?: sc,mc

Graceful timeout for media components upgrade (sec): 60

Note: Make sure that the Signaling Components have the same or later version than the Media Components.

Upgrade using the Software Version file (.cmp) may be performed only within the same OS version stream.

The following streams are available:

- 7.20A stream – based on OS Version 6
- 7.20CO stream – based on OS Version 8
- 7.40A stream – based on OS Version 8

For example, if your Mediant CE is currently running software version 7.20A.256.396 (i.e., 7.20A stream, based on OS Version 6), you may use 7.20A.258.010 .cmp file to upgrade it to a newer version (also based on OS Version 6). However, you may not use 7.40A.005.509 .cmp file to perform a similar upgrade to a version from the 7.40A stream (based on OS Version 8).

If you want to upgrade Mediant CE deployed with a version from 7.20A stream (based on OS Version 6) to a version from 7.20CO or 7.40A streams (based on OS Version 8), use one of the following methods:

- **Method 1:** Deploy a new Mediant CE instance using OS Version 8 software image, configure it, and then switch live traffic to the new instance. See Section 4.1 for detailed instructions.
- **Method 2:** Rebuild the existing Mediant CE instance from the new OS Version 8 image. See Section 4.2 for detailed instructions.

Advantages and disadvantages of each method are listed in the table below:

Method	Advantages	Disadvantages
Method 1	▪ In case of any problems with the new software version (based on OS Version 8), live traffic may be switched back to the old instance, running the old software version. ▪ Traffic may be gradually moved to a new instance (assuming VoIP equipment that sent traffic towards the Mediant CE supports such functionality), thereby providing better control over the upgrade process and minimizing service downtime.	▪ Requires the use of additional resources for the duration of the upgrade. ▪ Implies a change of IP addresses (both public and private) and therefore, requires re-configuration of VoIP equipment that communicates with the Mediant CE. ▪ Requires a new License Key for the new Mediant CE instance.
Method 2	▪ Doesn't require additional resources. ▪ Preserves public and private IP addresses of the deployed CE instance.	▪ Requires a new License Key after the upgrade (because Signaling Component's serial number changes). ▪ Service is unavailable while instances are rebuilt (typically for 10-15 minutes).

4.1 Method 1 – Side-By-Side Deployment of New Version

This section describes the upgrade of the Mediant CE instance running software version from the 7.20A stream (based on OS Version 6) to a version from the 7.20CO or 7.40A streams (based on OS Version 8) via side-by-side installation of a new Mediant CE instance and gradual migration of live traffic from the old to the new instance.

➢ **To perform upgrade via "side-by-side deployment" method:**

1. Deploy a new Mediant CE instance using Stack Manager, as described in Section 3.1. Choose **OS Version = 8** during the deployment. Connect the new Mediant CE instance to the same Virtual Network and Subnets as the existing Mediant CE instance.
1. Download the configuration (INI) file from the existing Mediant CE instance: **Actions > Configuration File > Save INI File**.
2. Remove all networking configuration from the downloaded file, by doing one of the following:
   - Using the ini_cleanup.py script from the *Mediant VE Installation Kit* available on www.audiocodes.com portal:

     ```
     # python ini_cleanup.py old.ini new.ini
     ```

   - Manually: Open the file in a text editor (e.g. Notepad++), and then delete the following elements:
     - Configuration tables: PhysicalPortsTable, EtherGroupTable, DeviceTable, InterfaceTable, MtcEntities
     - Configuration parameters: HARemoteAddress, HAUnitIdName, HARemoteUnitIdName, HAPriority, HARemotePriority, HALocalMAC, HARemoteMAC
3. Load the "cleaned up" configuration file to the new Mediant CE instance as an incremental INI file: **SETUP > ADMINISTRATION > MAINTENANCE > Auxiliary Files > INI file (incremental)**.
4. Obtain, activate and apply the license to the new Mediant CE instance, as described in Section 5.
5. Switch live traffic from the old Mediant CE instance to the new one. This typically requires a change in the SBC IP address in the VoIP equipment that communicates with the Mediant CE. Consider performing gradual traffic migration if your VoIP equipment supports it. For example, first switch 10% of your live traffic to the new Mediant CE instance, verify that it's processed as expected, and only after that switch the rest of the traffic.
6. After all live traffic is switched to the new Mediant CE instance and service operates normally, delete the old Mediant CE instance.

4.2 Method 2 – Rebuild Existing Mediant CE Instance from New Image

This section describes the upgrade procedure of Mediant CE instance running software version from the 7.20A stream (based on OS Version 6) to a version from the 7.20CO or 7.40A streams (based on OS Version 8) via a rebuild of existing Mediant CE instance from a new image.

The described procedure preserves all IP addresses (private and public) assigned to the Mediant CE instance, as well as most of the SBC configuration. However, the following configuration elements will be lost and must be manually restored after the procedure:

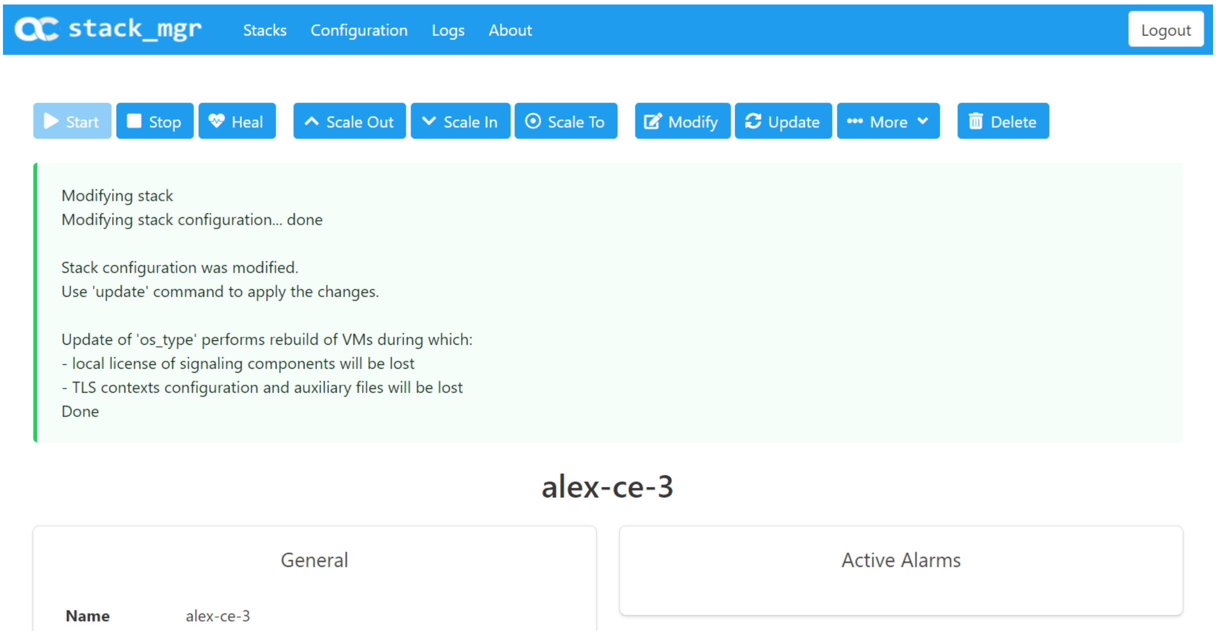
- TLS Contexts configuration (certificates and private keys)
- Auxiliary files (e.g., Pre-recorded Tone files)
- License keys (as the serial number of rebuilt instances changes)

➢ To perform upgrade via "rebuild from a new image" method:

1. Connect to the Stack Manager Web interface.
2. Click the corresponding stack name.
3. Click **Modify,** and then change the **OS Version** to **8**.
4. Click **Update** to rebuild the stack.
5. Wait for the **Update** operation to complete. The operation typically takes 10-15 minutes, during which all VM instances are rebuilt and service is unavailable. Mediant CE configuration, including private and public IP addresses is preserved.
6. Restore parts of the SBC configuration that have been lost during the rebuild (i.e., TLS certificates, private keys and auxiliary files).
7. Obtain, activate and apply the license to the Signaling Components, as described in Section 5.

Your Mediant CE is now running the new software version based on OS Version 8 and is fully operational.

Figure 4-2: Upgrading Mediant CE to New Image Based on OS Version 8



```
Modifying stack
Modifying stack configuration... done

Stack configuration was modified.
Use 'update' command to apply the changes.

Update of 'os_type' performs rebuild of VMs during which:
- local license of signaling components will be lost
- TLS contexts configuration and auxiliary files will be lost
Done
```

alex-ce-3

General

Name alex-ce-3

Active Alarms

5 Downgrading Software Version

The procedure for downgrading Mediant CE software version is similar to the upgrading procedure, as described in the previous section, but in the reverse order:

- You first need to downgrade the Media Components.
- Afterwards, you need to downgrade the Signaling Components

This sequence ensures that the Signaling Components always have the same or later version than the Media Components.

When downgrading from version 7.40A.100.* or later to version 7.40A.005.*, the following additional configuration steps must be performed prior to the downgrade:

1. Connect to the Mediant CE's CLI interface (provided by Signaling Components) through an SSH client or a serial console.
2. Log in as an administrative user.
3. Run the following commands:

```
enable
    <password> (e.g. "Admin")
configure system
    voice-config
    TpncpEncryptionEnable = 0
    exit
exit
```

4. Reboot the Signaling Components using the `reload now` CLI command or the Web interface's **Reset** button.
5. Wait until the Media Components are connected. Verify that their displayed status is "Connected" and not "Connected (TLS)".

Note: The above procedure is required because the communication protocol between the Signaling Components and Media Components was changed in version 7.40A.100.*. Failure to perform this procedure will prevent the Media Components from connecting to the Signaling Components after the latter are downgraded to the 7.40A.005.* version.

This page is intentionally left blank.

6 Licensing Mediant CE

Once you have successfully installed Mediant CE, you need to obtain, activate and then install the License Key.

Note: Licensing is applicable only to Signaling Components; Media Components do not require licensing.

6.1 Obtaining and Activating a Purchased License Key

For Mediant CE to provide you with all the required capacity and features, you need to obtain and activate a License Key which enables these capabilities.

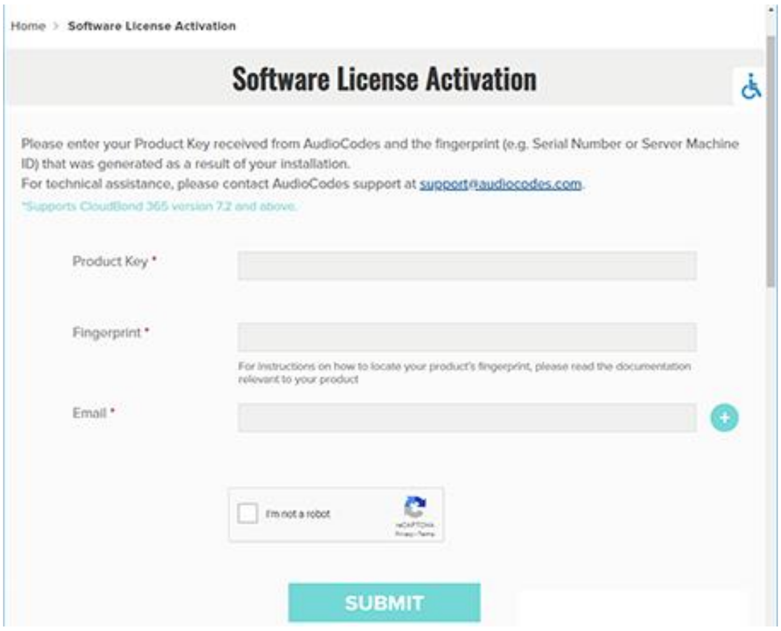
Note:

- 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 Mediant CE with two Signaling Component instances, each Signaling Component instance has its own Serial Number, Product Key and License Key. Therefore, the instructions in this section must be done per Signaling Component instance.

➢ **To obtain and activate the License Key:**

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

Figure 6-1: Software License Activation Tool



Software License Activation

Please enter your Product Key received from AudioCodes and the fingerprint (e.g. Serial Number or Server Machine ID) that was generated as a result of your installation.
For technical assistance, please contact AudioCodes support at support@audiocodes.com.
*Supports CloudBond 365 version 7.2 and above.

Product Key *

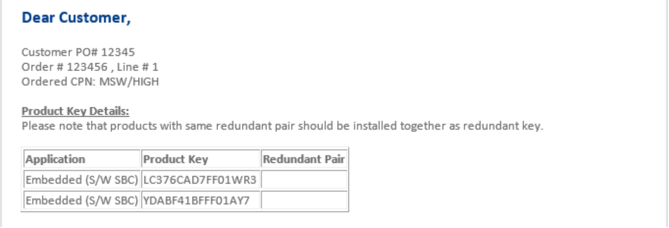
Fingerprint *

For instructions on how to locate your product's fingerprint, please read the documentation relevant to your product

Email *

2. Enter the following information:
    - **Product Key:** The Product Key identifies your specific Mediant CE 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 6-2: Product Key in Order Confirmation E-mail



Dear Customer,

Customer PO# 12345
Order # 123456 , Line # 1
Ordered CPN: MSW/HIGH

Product Key Details:
Please note that products with same redundant pair should be installed together as redundant key.

Application	Product Key	Redundant Pair
Embedded (S/W SBC)	LC376CAD7FF01WR3	
Embedded (S/W SBC)	YDABF41BFFF01AY7	

> **Note:** For Mediant CE orders with two Signaling Component instances, you are provided with two Product Keys, one for each Signaling Component instance. In such cases, you need to perform license activation twice to obtain License Keys for both Signaling Component instances.

- **Fingerprint:** The fingerprint is the Mediant CE'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.

3. Click **Submit** to send your license activation request.
4. 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 Signaling Component instance.

> **Warning:** Do not modify the contents of the License Key file.

6.2 Installing the License Key

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

> **Note:** The License Key file for Mediant CE with two Signaling Component instances must contain two License Keys - one for the active Signaling Component instance and one for the redundant Signaling Component instance. Each License Key has a different serial number ("S/N"), which reflects the serial number of each Signaling Component instance.

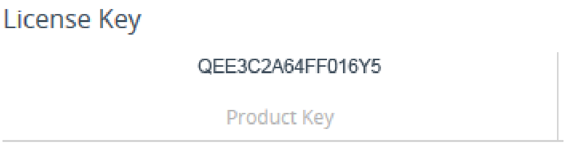
6.3 Product Key

The Product Key identifies a specific purchase of your Mediant CE deployment for the purpose of subsequent communication with AudioCodes (e.g., for 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 > **Maintenance** folder > **License Key**). The Product Key is displayed in the read-only 'Product Key' field, as shown in the example below:

Figure 6-3: Viewing Product Key



License Key

QEE3C2A64FF016Y5

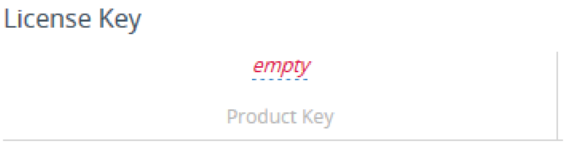
Product Key

- Device Information page.

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 6-4: Empty Product Key Field



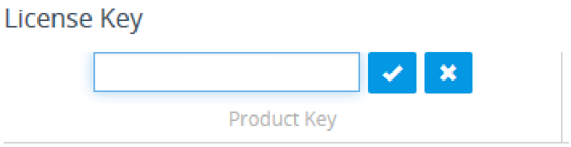
License Key

empty

Product Key

3. Click "empty"; the following appears:

Figure 6-5: Entering Product Key



License Key

✓ ✖

Product Key

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

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, 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

Document #: LTRT-10913