

## Mediant Cloud Edition (CE)

Deployment in OpenStack | VMware | Private  
Cloud Environments

Version 7.6

---

## Table of Contents

---

<b>Notice</b> .....	<b>iv</b>
Security Vulnerabilities.....	iv
WEEE EU Directive.....	iv
Customer Support.....	iv
Stay in the Loop with AudioCodes.....	iv
Abbreviations and Terminology.....	iv
Document Revision Record.....	iv
Documentation Feedback.....	iv
<b>1 Introduction</b> .....	<b>1</b>
1.1 Architecture Overview.....	2
1.2 Deployment Topology.....	3
<b>2 Deployment in OpenStack</b> .....	<b>4</b>
2.1 Prerequisites.....	4
2.1.1 AudioCodes Mediant VE/CE Image.....	4
2.1.2 Network Prerequisites.....	4
2.1.3 Instance Flavors.....	5
2.2 Deployment via Stack Manager.....	5
<b>3 Deployment in Private Cloud Environments (e.g., VMware)</b> .....	<b>9</b>
3.1 Prerequisites.....	9
3.1.1 Network Prerequisites.....	9
3.1.2 Virtual Machine Types.....	10
3.2 Redundancy Deployment Options.....	11
3.2.1 Protection from Software Failure.....	11
3.2.2 Protection from Hardware Failure.....	11
3.2.3 Redundancy Deployments Summary.....	12
3.2.4 Protection from Hardware and Software Failure.....	12
3.3 Creating Virtual Machines.....	13
3.4 Deployment via Manual Installation and Configuration.....	14
<b>4 Managing Mediant CE</b> .....	<b>22</b>
<b>5 Default Security Rules</b> .....	<b>23</b>
<b>6 Upgrading the Software Version</b> .....	<b>24</b>
<b>7 Downgrading Software Version</b> .....	<b>25</b>

<b>8</b>	<b>Licensing Mediant CE.....</b>	<b>26</b>
8.1	Obtaining and Activating a Purchased License Key.....	26
8.2	Installing the License Key .....	27
8.3	Product Key .....	28

## 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-20-2025

## 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
11030	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

**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
- Private cloud environments (e.g., VMware)

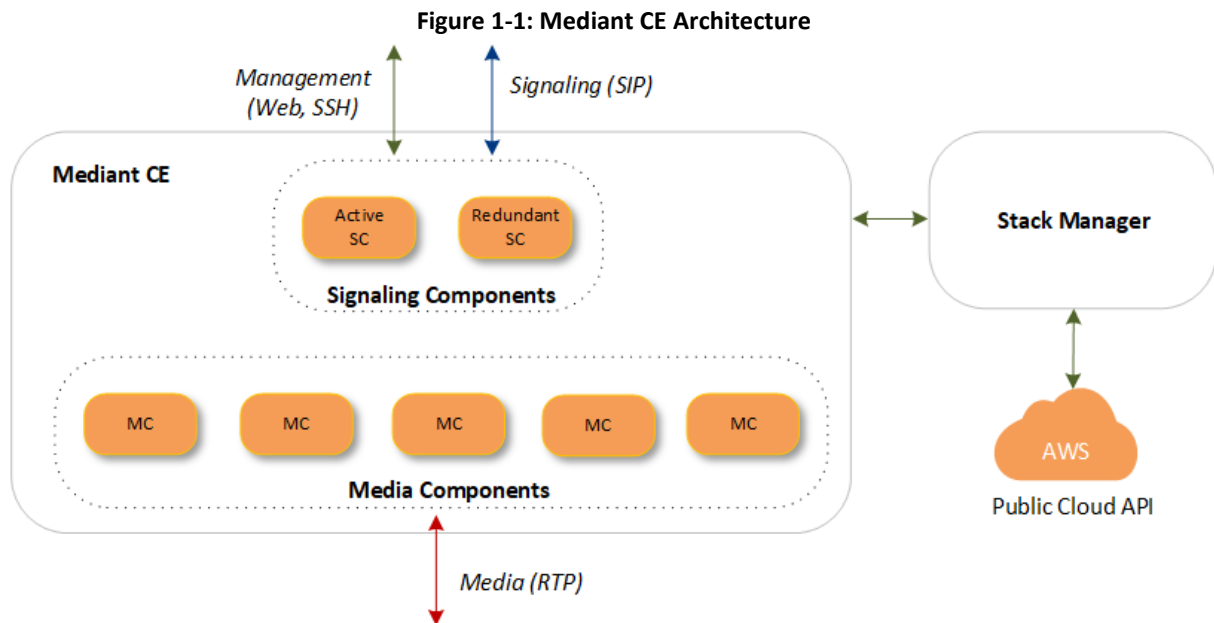
This document describes the deployment of Mediant CE in OpenStack and private cloud environments (e.g., VMware).

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



- Mediant CE deployment in OpenStack and private cloud environments is currently available for **evaluation purposes only**.
- Deployments in VMware and private cloud environments are done manually, without the Stack Manager tool, and lack certain lifecycle management features (e.g., automatic scaling).
- For configuring Mediant CE SBC, refer to the *Mediant Software SBC User's Manual*.

## 1.1 Architecture Overview



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, which choose the Media Component based on current cluster utilization and pass the media streams to it.

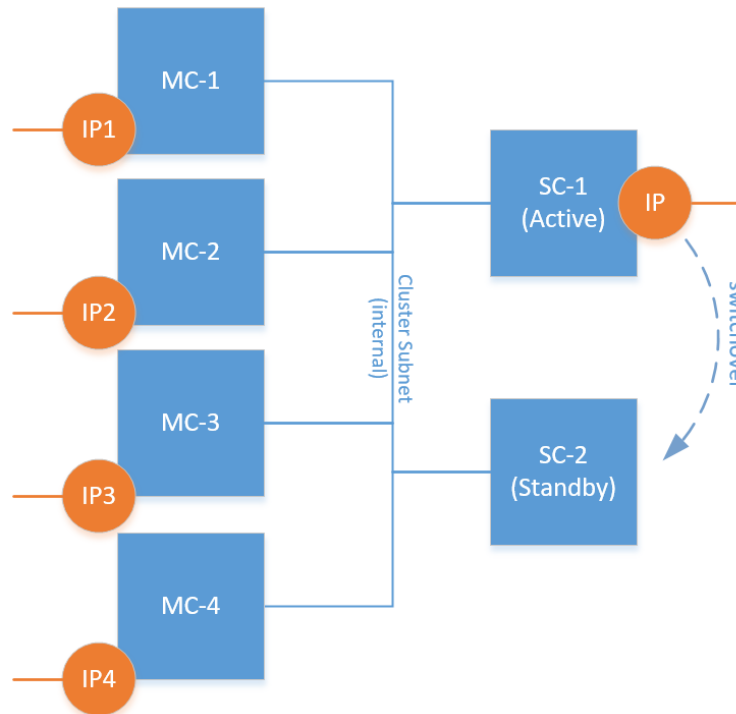
Signaling components also serve as a “single point of contact” for all management tasks. They provide Web and CLI interfaces through which customers have complete control over all cluster components.

## 1.2 Deployment Topology

In a typical Mediant CE deployment, two Signaling Components are created and operate in 1+1 Active / Standby mode. In case of a failure in the active signaling component, all IP addresses are seamlessly moved to the remaining (newly active) signaling component and all established calls are preserved.

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

**Figure 1-2: Signaling Components Switchover**



You can 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” operation.

You may also deploy Mediant CE in private cloud environments (e.g., VMware) via manual installation and configuration instructions, provided below. Such deployments don't support the Stack Manager component and certain cluster management features. For example, they don't support automatic scaling.



- Mediant VE and CE products share the same software image. Therefore, in some places in this document, the Mediant VE product name is referenced even though the document concerns Mediant CE.
- The scope of this document does not fully cover security aspects for deploying the product in the intended environment. Security measures should be done in accordance with specific security policies and recommendations of the intended environment.
- For configuring Mediant CE, refer to the *Mediant Software SBC User's Manual*.

## 2 Deployment in OpenStack

### 2.1 Prerequisites

Prior to deploying Mediant CE in the OpenStack environment, make sure that you meet the following prerequisites:

- You have uploaded the 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.

#### 2.1.1 AudioCodes Mediant VE/CE Image

To deploy Mediant CE on OpenStack, you must use the *Mediant VE/CE QCOW2 Image for KVM/OpenStack*. For more information, go to <https://www.audiocodes.com/library/firmware>.

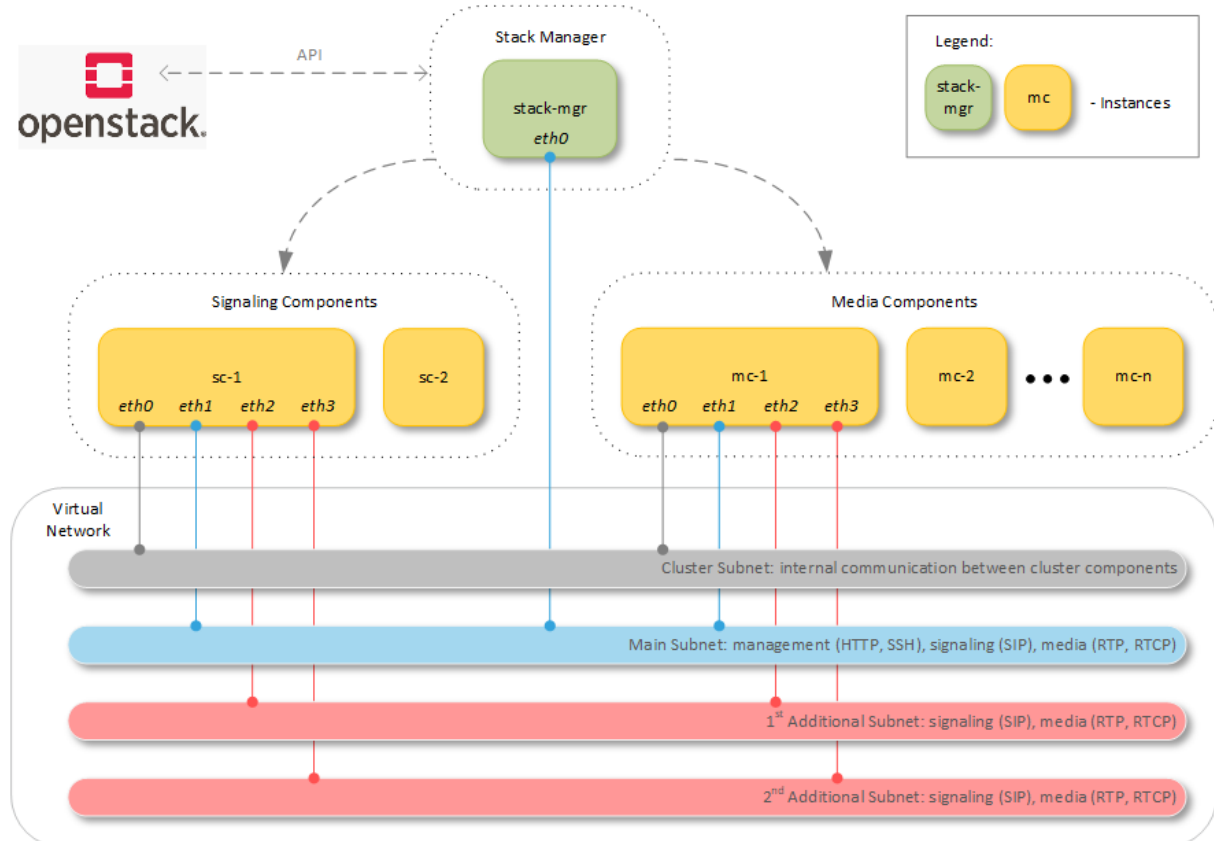
Upload the image to the OpenStack image repository, using the following command:

```
# openstack image create --disk-format qcow2 \
  --container-format bare --public \
  --file ./sbc-F7.20A.202.204.qcow2 sbc-F7.20A.202.204
```

#### 2.1.2 Network Prerequisites

Mediant CE on OpenStack uses the following network architecture:

Figure 2-1: Mediant CE Network Architecture – OpenStack





Up to four subnets may be used:

- **Cluster Subnet:** For internal communication between Mediant CE components. It's connected to both Signaling Component and Media Component instances as the first network interface (eth0).
- **Main Subnet:** Carries management (HTTP, SSH, etc.), signaling (SIP) and media (RTP, RTCP) traffic. It's connected to both Signaling Component and Media Component instances as the second network interface (eth1) and to the Stack Manager instance.
- **1<sup>st</sup> and 2<sup>nd</sup> Additional Subnets:** Carry signaling (SIP) and media (RTP, RTCP) traffic. They are connected to Media Component 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.

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

### 2.1.3 Instance Flavors

It's recommended to use the following instance flavors for Mediant CE components:

- Signaling Component instances: 4 vCPU (hyperthreading enabled), 16GB RAM
- Forwarding Media Component instances: 2 vCPU (Hyper-threading enabled), 4GB RAM
- Transcoding Media Component instances: 8 vCPU (Hyper-threading enabled), 8GB RAM

## 2.2 Deployment via Stack Manager

The recommended method for deploying Mediant CE in an OpenStack environment is via the Stack Manager tool. Alternatively, you may perform manual installation and configuration as described in Section Deployment via Manual Installation and Configuration.

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

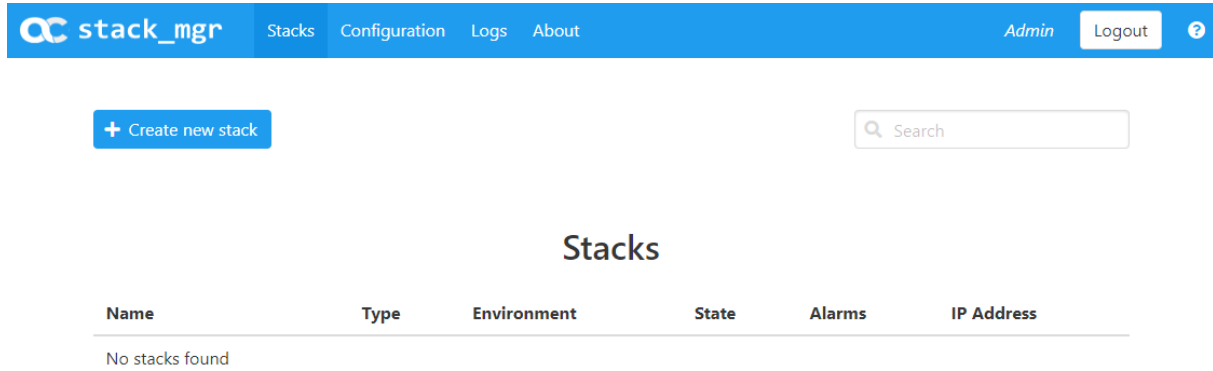
- Initial product deployment.
- Update of deployed stack's network topology
- Automatic and on-demand scaling of media components, to adjust stack footprint and minimize infrastructure costs.
- Monitoring of deployed OpenStack resources and recovery in case of their corruption / accidental removal
-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

Stack Manager uses dynamically generated Heat templates for stack deployment on the OpenStack platform 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 deployment; the following screen appears:

Figure 2-2: Stack Manager Main Screen



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

Figure 2-3: Create Stack Dialog – Step 1

4. In the 'Name' field, enter a name for the stack (e.g., "mediant-ce").
5. From the 'Stack type' drop-down list, select **Mediant CE**.

- From the 'Image' drop-down list, select the AudioCodes Mediant VE/CE image, prepared as described in Section AudioCodes Mediant VE/CE Image.
- From the 'Key pair' drop-down list, select the key pair that you will use to access the deployed stack's CLI interface (via SSH protocol). Alternatively, you may use username / password (defined in the same dialog box later) to access both Web and CLI interfaces.
- Select the subnets that Mediant CE will be connected to.

Figure 2-4: Create Stack Dialog – Step 2

Create new stack

Signaling Components

VM type -- select --  Customize

Media Components

Profile forwarding

VM type -- select --  Customize

Min number 2

Max number 3

Admin User

Username

Password

Advanced

Advanced config

Create Cancel

- From the 'VM type' drop-down list, select the type of virtual machine for the signaling and media components.
- 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).
- In the 'Min number' and 'Max number' fields, select the minimum and maximum number of media components in the stack. Stack Manager creates the selected maximum number of media components, but initially starts only creating the selected minimum number of them. You may later adjust the number of running media components via **scale out** and **scale in** actions.

12. 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 deployed Mediant CE stack is not affected.
13. 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.
14. Click **Create** to start stack creation.
15. Wait until the stack is created.

## 3 Deployment in Private Cloud Environments (e.g., VMware)

### 3.1 Prerequisites

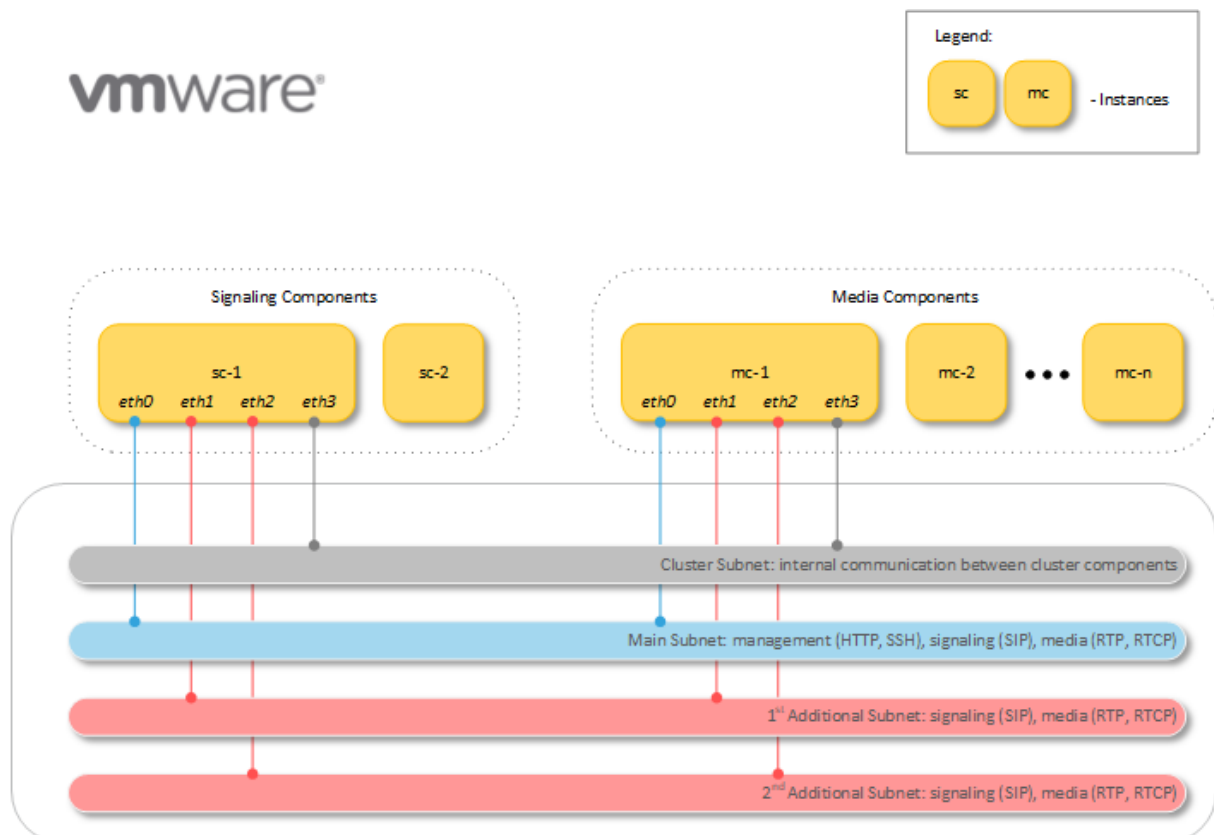
Prior to deploying Mediant CE in a private cloud environment (e.g., VMware), make sure that you meet the following prerequisites:

- You have AudioCodes Mediant VE/CE image for your environment (e.g., OVF image for VMware). Images can be downloaded from AudioCodes website at <https://www.audiocodes.com/library/firmware>.
- All subnets needed for Mediant CE deployment are available, including the Cluster subnet. For more information, see the following section.

#### 3.1.1 Network Prerequisites

Mediant CE in private cloud environments (e.g., VMware) uses the following network architecture:

**Figure 3-1: Mediant CE Network Architecture – Private Cloud Environments (e.g., VMware)**



Up to four subnets may be used:

- **Cluster Subnet:** For internal communication between Mediant CE components.
- **Main Subnet:** Carries management (HTTP, SSH, etc.), signaling (SIP), and media (RTP, RTCP) traffic.

- **1<sup>st</sup> and 2<sup>nd</sup> Additional Subnets:** Carries signaling (SIP) and media (RTP, RTCP) traffic. These subnets are optional because the Main Subnet may carry all types of traffic. The 1<sup>st</sup> network interface (eth0) is typically connected to the Main subnet. The last network interface is typically connected to the Cluster subnet.

### 3.1.2 Virtual Machine Types

The recommended virtual machine types for Mediant CE components depend on the host's CPU type:

- **Prior to Intel® Xeon® Scalable Processors:**
  - Signaling Component instances:
    - ◆ 4 vCPU (non-hyperthreaded, 4 physical cores)
    - ◆ 16GB RAM, 50GB Storage
  - Forwarding-only Media Component instances:
    - ◆ 1 vCPU (non-hyperthreaded, 1 physical core)
    - ◆ 4GB RAM, 10GB Storage
  - Transcoding Media Component instances:
    - ◆ 8 vCPU (non-hyperthreaded, 8 physical cores)
    - ◆ 8GB RAM, 10GB Storage
- **Intel® Xeon® Scalable Processors or later:** it's recommended to utilize Hyper-Threading capability, which provides improved performance while using lower CPU resources.
  - Signaling Component instances:
    - ◆ 4 vCPU (hyperthreaded, 2 physical cores)
    - ◆ 16GB RAM, 50GB Storage
  - Forwarding-only Media Component instances:
    - ◆ 2 vCPU (hyperthreaded, 1 physical core)
    - ◆ 4GB RAM, 10GB Storage
  - Transcoding Media Component instances:
    - ◆ 8 vCPU (hyperthreaded, 4 physical cores)
    - ◆ 8GB RAM, 10GB Storage

## 3.2 Redundancy Deployment Options

### 3.2.1 Protection from Software Failure

Software protection of the Signaling Component is achieved using 1+1 instances of Signaling Component's (1+1 VM's).

Software Protection of the Media Components is achieved using N+1 instances of Media Component's (N+1 VM's).

### 3.2.2 Protection from Hardware Failure

Hardware failure is more restrictive than software failure because a failure of a single server may pose simultaneous failures of multiple virtual machines (either Signaling Component or Media Component) residing on that server.

When protection from a hardware failure is required on the Signaling Component, two host servers should be deployed and occupy a single Signaling Component on each. These servers can deploy Media Component virtual machines as well.

When protection from a hardware failure is required for the Media Components, calculation of the minimum number of servers required for allocation of Media Components should take into account the following factors:

- Maximum active media sessions allowed on a single server. For figures, refer to the *Release Notes* (Section 'Mediant CE SBC for VMware'), which is currently 4,000 sessions.
- Transcoding capacity required and transcoding capacity per Media Component (refer to the *Release Notes* for the specific transcoding type/s required).
- Session capacity required, and session capacity per Media Component (refer to the *Release Notes*).

It's recommended to consult with AudioCodes to reach the minimum number of servers.

### 3.2.3 Redundancy Deployments Summary

The following table describes redundancy options for deployment:

Component Module (VM Type)	Redundancy Protection		Number of Components (VMs) Required	Servers (Hosts) Deployment
	Software Failure Only	Software and Server (Host) Failures		
Signaling Components	-	-	1	Single Signaling Component on a single server
	+	-	1+1	Both Signaling Components can reside on the same server, or different servers
	+	+	1+1	Each Signaling Component on a different server
Media Components	-	-	$N^1$	Each server can occupy as many Media Components as possible
	+	-	At least $N+1$	Each server can occupy as many Media Components as possible
	+	+	At least $\frac{N*S}{S-1}$	Each server should occupy at least $\frac{N}{S-1}$ Media Components

### 3.2.4 Protection from Hardware and Software Failure

When protection from both hardware and software failure is required on the Signaling Component, two host servers should occupy a single Signaling Component on each.

When protection from both hardware and software failure is required on the Media Component, the minimum number of servers required for allocation of Media Components can be calculated as follows:

$$S \geq \frac{N + Ns}{Ns}$$

Where:

- $S$  is the number of servers required (minimum 2).
- $N$  is the number of Media Components required to reach the required media capacity (forwarding and transcoding).
- $Ns$  is the maximum number of Media Components that can be installed on a single server.

<sup>1</sup>  $N$  is the number of MCs required to achieve the required media capacity (forwarding and transcoding) without redundancy.  $S$  is the number of servers in the deployment.



## 3.3 Creating Virtual Machines

Create virtual machines for signaling and media components as follows:

1. For each server (host) in the deployment, configure BIOS settings according to Section 3.1 "Configuring the Server's BIOS" in the *Mediant Virtual Edition SBC Installation Manual*.
2. Create a virtual machine for the first signaling component, according to Section 3 in the *Mediant Virtual Edition SBC Installation Manual*. For example, for VMware vSphere ESXi, follow detailed instructions in:
  - Section 3.2 "Installing Mediant VE SBC on VMware vSphere ESXi"
  - Section 3.7 "Configuring Console Access Method".
  - Section 3.8 "Reconfiguring Default IP Address to Match Network Settings"



Section 3.9 "Adding Transcoding Capabilities" is not applicable to Mediant CE.

3. Repeat Step 2 to create a virtual machine for the second signaling component. This signaling component should reside on the same server (host) or on a different server according to Section Redundancy Deployment Options.
4. Configure two signaling components as a high-availability (HA) pair, as described in Section 3.13 in the *Mediant Virtual Edition SBC Installation Manual*.
5. Repeat Step 2 to create virtual machines for media components. The number of media components is determined according to Section Redundancy Deployment Options.
6. Follow the instructions in Section Deployment via Manual Installation and Configuration.

### 3.4 Deployment via Manual Installation and Configuration

This deployment method enables Mediant CE deployment in private cloud environments (e.g., VMware). All needed resources (e.g., subnets and virtual machines) must be manually created and properly configured by the operator, as described below.

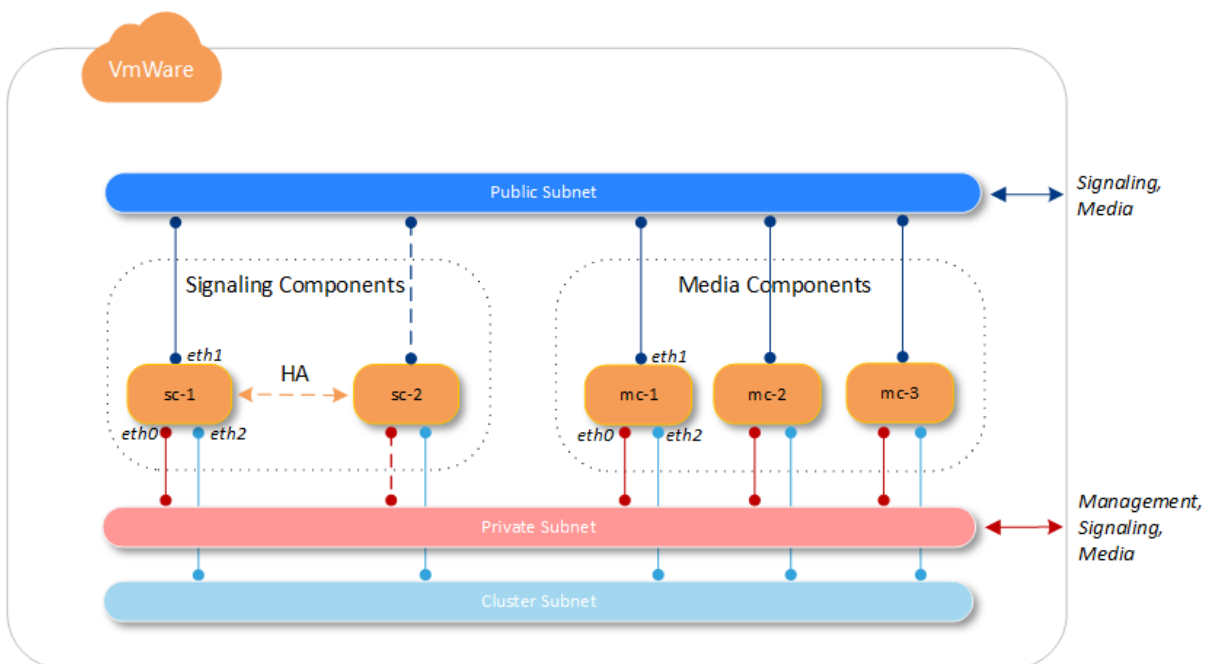
As this deployment method doesn't include a "management component", automatic scaling is not supported. Manual scaling may be done by creating and configuring additional resources, but it's considerably more complicated than when using Stack Manager.



For cloud environments, you should deploy Mediant CE using the Stack Manager tool, as described previously.

The following instructions describe the following Mediant CE deployment example:

**Figure 3-2: Sample Mediant CE Deployment In VMware**



The deployment consists of:

- Two signaling components: sc-1 and sc-2
- Three media components: mc-1, mc-2, and mc-3
- Private subnet, which is used for management (e.g., SSH and HTTP), signaling (SIP), and media (RTP) traffic
- Public subnet, which is used for signaling (SIP) and media (RTP) traffic
- Cluster subnet, which is used for internal communication between Mediant CE components

**To deploy Mediant CE:**

1. Create virtual machines for all Mediant CE components.
2. Connect all virtual machines to the subnets:
  - eth0 (1<sup>st</sup> network port) – private subnet
  - eth1 (2<sup>nd</sup> network port) – public subnet
  - eth2 (3<sup>rd</sup> network port) – cluster subnet
3. Configure IP addresses on the 1<sup>st</sup> Signaling Component (sc-1):
  - eth0 – Application Type is **O+C+M**
  - eth1 – Application Type is **C+M**
  - eth2 – Application Type is **Maintenance (HA)**
4. Configure IP addresses on the 2<sup>nd</sup> Signaling Component (sc-2):
  - eth0 – Application Type is **O+C+M**
  - eth2 – Application Type is **Maintenance (HA)**
5. Configure IP addresses on the Media Component (mc-1, mc-2, and mc-3):
  - eth0 – Application Type is **O+C+M**
  - eth1 – Application Type is **C+M**
  - eth2 – Application Type is **Cluster**
6. Configure HA connection between Signaling Components:
  - a. On the 1<sup>st</sup> Signaling Component (sc-1):
    - ◆ Open the HA Settings page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **HA Settings**).
    - ◆ Configure the 'HA Remote Address' parameter to the Maintenance IP address (eth2) of the 2<sup>nd</sup> Signaling Component (sc-2).
    - ◆ Save configuration.
  - b. On the 2<sup>nd</sup> Signaling Component (sc-2):
    - ◆ Open HA Settings page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **HA Settings**).
    - ◆ Configure the 'HA Remote Address' parameter to the Maintenance IP address (eth2) of the 1<sup>st</sup> Signaling Component (sc-1).
    - ◆ Save configuration.
  - c. Restart the 1<sup>st</sup> Signaling Component and wait until it boots up.
  - d. Restart the 2<sup>nd</sup> Signaling Component. When the restart completes, the 2<sup>nd</sup> Signaling Component establishes HA connection with the 1<sup>st</sup> Signaling Component and loses all its networking configuration, except for the Maintenance IP address. Therefore, you are unable to access its Web interface. Instead, you should check its status on the **Monitor** page on the Web interface of the 1<sup>st</sup> Signaling Component.

- e. Wait until the HA connection between Signaling Components is fully established and the **Monitor** page displays the 'HA Status' as "Operational" and both Active and Redundant devices are visible.

**Figure 3-3: HA Connection Between Signaling Components**

The screenshot displays the Audiocodes Mediant SW Monitor interface. The top navigation bar includes 'SETUP', 'MONITOR' (selected), and 'TROUBLESHOOT'. The main content area is divided into several sections:

- Device Information Table:**

10.4.220.74 Address	7.20A.204.011 Firmware	Mediant SW Type	Operational HA Status	194943260928673 S/N
------------------------	---------------------------	--------------------	--------------------------	------------------------
- Active Device: Device 1:** A diagram showing a device with three network ports (1, 2, 3) connected to a 'Network'.
- Redundant Device: NA:** A diagram showing a device with three network ports (1, 2, 3) connected to a 'Network'.
- SBC Metrics:** Six circular gauges representing:
  - Active Calls: 0
  - Average Success Ratio (ASR): N/A
  - Average Call Duration (ACD): N/A
  - Calls per Sec.: 0
  - Transactions per Sec.: 0
  - Registered Users: 0

7. Add the cluster IP address to the Signaling Components:
  - a. On the 1<sup>st</sup> Signaling Component (sc-1), open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
  - b. Add an additional (secondary) IP address to the VLAN that is attached to the 3<sup>rd</sup> network interface (eth3).
  - c. Configure the 'Application Type' parameter to **Cluster** for this additional IP address.

Figure 3-4: Network Configuration on Signaling Components

The screenshot shows the Audiocodes Mediant SW configuration interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' tabs, with a 'Save' button highlighted in a red box. The main content area is titled 'IP NETWORK' and shows a network diagram. The diagram includes:

- IP Interfaces:** Four boxes representing interfaces: #0 [eth0] 10.4.220.74, #1 [eth1] 192.168.1.12, #2 [eth2] 192.168.0.107, and #3 [eth2-1] 192.168.0.52.
- VLANs (Eth Devices):** Three boxes representing VLANs: #0 [Vlan 1] VLAN ID = 1 (Untagged), #1 [Vlan 2] VLAN ID = 2 (Untagged), and #2 [Vlan 3] VLAN ID = 3 (Untagged).
- Ethernet Groups:** Three boxes representing groups: #0 [GROUP\_1], #1 [GROUP\_2], and #2 [GROUP\_3].
- Physical Ports:** Three boxes representing ports: #0 [User P... GE\_1], #1 [User P... GE\_2], and #2 [User P... GE\_3].

Lines connect the Ethernet Groups to the Physical Ports. A 'Refresh Network View' button is located at the bottom of the diagram area.

8. Configure Signaling Components to operate in Media Cluster mode:
  - a. On the 1<sup>st</sup> Signaling Component (sc-1), open the Cluster Manager Settings page (**Setup** menu > **IP Network** tab > **Media Cluster** folder > **Cluster Manager Settings**).
    - ◆ Configure the 'Cluster Mode' parameter to **Media Cluster**.
    - ◆ Configure the 'Device Role' parameter to **Signaling Component**.
  - b. Save configuration.
  - c. Restart the device to activate the new operation mode.
9. Configure Media Components (mc-1, mc-2, mc-3) to operate in Media Cluster mode:
  - a. On each Media Component (mc-1, mc-2, mc-3), open the Cluster Manager Settings page (**Setup** menu > **IP Network** tab > **Media Cluster** folder > **Cluster Manager Settings**).
    - ◆ Configure the 'Cluster Mode' parameter to **Media Cluster**.
    - ◆ Configure the 'Device Role' parameter to **Media Component**.
  - b. Refresh the navigation menu, by clicking the browser's Reload button or using the Ctrl+R shortcut key.
  - c. Open the MC Settings page (**Setup** menu > **IP Network** tab > **Media Cluster** folder > **MC Settings**).
    - ◆ Configure the 'Cluster Manager IP Address' parameter to the Cluster IP address of the Signaling Component (added in Step 7).
    - ◆ Configure the 'Media Component Profile' parameter to match the intended operational mode of the Media Components.
  - d. Save configuration.

- e. Restart the device to activate the new configuration.
10. Configure Signaling Components to operate with Media Components:
    - a. On the 1<sup>st</sup> Signaling Component (sc-1), open the Media Components page (**Setup** menu > **IP Network** tab > **Media Cluster** folder > **Media Components**).
    - b. Click **New** to add a new Media Component entry.
    - c. Configure the Media Component name and corresponding OAM IP address (assigned to eth0 interface).
    - d. Repeat the above steps for all Media Components.
    - e. Save configuration.
    - f. Wait until the 'Status' field of all Media Components displays "Connected".

Figure 3-5: Media Components Configuration and Status Table

The screenshot displays the Audiocodes Mediant SW interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' tabs, with 'SETUP' selected. The main menu shows 'IP NETWORK' selected under 'SIGNALING & MEDIA'. The left sidebar contains a 'NETWORK VIEW' menu with 'MEDIA CLUSTER' selected. The main content area shows 'Media Components (3)' with a table listing three components (mc-1, mc-2, mc-3). Below the table, the configuration details for '#0[mc-1]' are shown, including device settings, device information, and device status.

INDEX	NAME	OAMP IP ADDRESS	ADMIN STATE	VERSION	STATUS	MEDIA UTILIZATION (LEGS)	DSP UTILIZATION (LEGS)	ALARM SEVERITY
0	mc-1	10.4.220.69	Unlocked	7.20A.204.011	Connected	0% (0)	0% (0)	None
1	mc-2	10.4.220.72	Unlocked	7.20A.204.011	Connected	0% (0)	0% (0)	None
2	mc-3	10.4.220.75	Unlocked	7.20A.204.011	Connected	0% (0)	0% (0)	None

**#0[mc-1]**

DEVICE SETTINGS		DEVICE INFORMATION	
Name	mc-1	Media Component Type	vMC
OAMP IP Address	10.4.220.69	Version	7.20A.204.011
Cluster Manager IP Address	192.168.0.52	Serial Number	149070522145563
Admin State	Unlocked		
Media Utilization (Legs)	0% (0)		
DEVICE STATUS		DSP INFORMATION	
Status	Connected	DSP SW Name	SOFTDSP
Device Up Time	00:00H:21M:06S	DSP Count	0
Alarm Severity	None	DSP SW Version	00.00
		DSP Utilization (Legs)	0% (0)

11. Configure Remote Media Interfaces on Signaling Components:
  - a. On the 1<sup>st</sup> Signaling Component (sc-1), open the Remote Media Interfaces page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Remote Media Interfaces**).
  - b. Click **New** to add a new Remote Media Interface.
  - c. Enter the name of the network interface on Media Components that is capable of handling media traffic (e.g., "eth0" or "eth1" in our example).

- d. Repeat the above steps for all network interfaces on the Media Components that are capable of handling media traffic.
- e. Verify that the 'Number of MCs' for each configured interface matches the actual number of Media Components (three in our example).

**Figure 3-6: Remote Media Interfaces Configuration**

The screenshot shows the Audiocodes Mediant CE web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' tabs, with a 'Save' button highlighted. The main navigation bar shows 'SIGNALING & MEDIA' as the active tab. The left sidebar contains a 'TOPOLOGY VIEW' section with 'Remote Media Interfaces (2)' selected. The main content area displays a table of Remote Media Interfaces:

INDEX	NAME	NUMBER OF MCS
0	eth0	3
1	eth1	3

Below the table, the configuration details for the selected interface '#0[eth0]' are shown. The 'GENERAL' section includes:

- Name: eth0
- Number of MCs: 3

12. Update Media Realms configuration on Signaling Components:
  - a. On the 1<sup>st</sup> Signaling Component (sc-1), open the Media Realms page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
  - b. Click **Edit** to edit the default Media Realm.
  - c. Configure 'Remote IPv4 Interface Name' to reference one of the Media Component's network interfaces, configured as Remote Media Interfaces in Step 12.

All traffic associated with this Media Realm is sent/received via the corresponding network interface on one of the Media Components. If you need to define additional Media Realms, configure them in a similar manner. In other words, configure 'Remote IPv4 Interface Name' or 'Remote IPv6 Interface Name' to associate the Media Realm with the corresponding network interface on one of the Media Components. Mediant CE automatically distributes calls across available Media Components, choosing the proper network interface and port range as configured for the Media Realm.

Figure 3-7: Media Realms Configuration

The screenshot shows the Audiocodes Mediant CE web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT' tabs, with a 'Save' button highlighted. The main menu on the left is under 'CORE ENTITIES' and includes 'Media Realms (1)'. The main content area shows a table of Media Realms with one entry: 'DefaultRealm' (Index 0, Port Range Start 6000, Port Range End 65534, Number of Media Session Legs 11907, Default Media Realm Yes). Below the table, the configuration details for '#0[DefaultRealm]' are displayed in a form with sections for GENERAL and QUALITY OF EXPERIENCE.

INDEX	NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	DefaultRealm	6000	11907	65534	Yes

**#0[DefaultRealm]** [Edit](#)

GENERAL		QUALITY OF EXPERIENCE	
Name	DefaultRealm	QoE Profile	# [-] <a href="#">View</a>
Topology Location	Down	Bandwidth Profile	# [-] <a href="#">View</a>
Remote IPv4 Interf...	# [eth0] <a href="#">View</a>		
Remote IPv6 Interf...	# [-] <a href="#">View</a>		
Port Range Start	6000		
Number Of Media ...	11907		
Port Range End	65534		
Default Media Realm	Yes		

13. If one of your subnets resides behind the NAT device, configure NAT translation as follows:
  - For each Media Component (mc-1, mc-2, and mc-3):**
    - a. Open the NAT Translation page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).
    - b. Click **New** to create a new NAT Translation rule, and then configure it as follows:
      - ◆ Configure the 'Source Interface' parameter to reference the corresponding network interface (e.g. eth1).
      - ◆ Configure the 'Source Start Port' parameter to **1**.
      - ◆ Configure the 'Source End Port' parameter to **65535**.
      - ◆ Configure the 'Target IP Address' parameter to match the public IP address of the NAT device (e.g., 10.6.2.101).
      - ◆ Configure the 'Target Start Port' parameter to **1**.
      - ◆ Configure the 'Target End Port' parameter to **65535**.
    - c. Restart the Media Component to activate the new configuration.
    - d. Repeat the above steps for all Media Components.



**On the 1st Signaling Component (sc-1):**

- a. Open the Media Components page (**Setup** menu > **IP Network** tab > **Media Cluster** folder > **Media Components**).
- b. For each entry that corresponds to the specific Media Component, click the **Network Interfaces** link at the bottom of the page, and then verify that the Public IP Address is properly detected for relevant interfaces.

**Figure 3-8: Verifying Public IP Address of the Media Component**

The screenshot shows the Audiocodes Mediant CE web interface. The top navigation bar includes 'SETUP', 'MONITOR', and 'TROUBLESHOOT'. The main menu is 'IP NETWORK', with sub-menus for 'SIGNALING & MEDIA' and 'ADMINISTRATION'. The left sidebar contains various configuration categories, with 'MEDIA CLUSTER' expanded to show 'Media Components (3)'. The main content area displays 'Media Components [#2] > Network Interfaces (2)'. A table lists the network interfaces:

INDEX	INTERFACE NAME	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS	NETWORK GROUP	APPLICATION TYPE	VLAN ID
0	eth0	10.4.220.75		GROUP_1	O+M+C	1 (Native Vlan)
1	eth1	192.168.1.6	10.6.2.101	GROUP_2	MEDIA+CONTROL	2 (Native Vlan)

Below the table, the details for the selected interface (#1) are shown in the 'GENERAL' section:

Interface Name	eth1
Private IP Address	192.168.1.6
Public IP Address	10.6.2.101
Network Group	GROUP_2
Application Type	MEDIA+CONTROL
Vlan ID	2 (Native Vlan)

14. Open the NAT Translation page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).

15. Click **New** to create a new NAT Translation rule, and then configure it as follows:

- Leave the 'Source Interface' parameter empty.
- Configure the 'Remote Interface Name' parameter to reference the corresponding Media Component's network interface (e.g., eth1).
- Configure the 'Source Start Port' parameter to **1**.
- Configure the 'Source End Port' parameter to **65535**.
- Configure the 'Target IP Mode' parameter to **Automatic**.
- Configure the 'Target Start Port' parameter to **1**.
- Configure the 'Target End Port' parameter to **65535**.

Mediant CE automatically performs NAT Translation, using the Public IP address of the Media Component that handles the specific call.

16. Your basic Mediant CE configuration is complete. You should now configure the SIP application, as described in the *Mediant VE/CE User's Manual* and perform some basic calls to verify correct system operation.

## 4 Managing Mediant CE

Mediant CE management is performed through the Web, CLI, and REST management interfaces provided by the active Signaling Component. These management interfaces are accessible via:

- **OpenStack:** via "eth1" private or public IP addresses assigned to the active signaling component
- **Private cloud environments (e.g., VMware):** via "eth0" private or public IP addresses assigned to the active signaling component

All Mediant CE management operations are performed through the above described management interface. There is no need to access management interfaces on other components (e.g., on media components).

## 5 Default Security Rules

Stack Manager creates security groups during Mediant CE deployment that enable only relevant traffic for each component and subnet. These security rules are assigned to network interfaces on both signaling components and media components.

The following table lists inbound rules for default security rules. You may change signaling and media rules by updating the 'Signaling ports' and 'Media ports' fields described previously.

**Table 5-1: Inbound Rules for Default Security Groups**

Component	Traffic	Subnet	Protocol	Port
<b>Signaling Component</b>	SSH	Main	TCP	22
	HTTP	Main	TCP	80
	HTTPS	Main	TCP	443
	SIP over UDP	<ul style="list-style-type: none"> <li>■ Main</li> <li>■ Additional1</li> <li>■ Additional2</li> </ul>	UDP	5060
	SIP over TCP/TLS	<ul style="list-style-type: none"> <li>■ Main</li> <li>■ Additional1</li> <li>■ Additional2</li> </ul>	TCP	5060, 5061
<b>Media Component</b>	RTP, RTCP	<ul style="list-style-type: none"> <li>■ Main</li> <li>■ Additional1</li> <li>■ Additional2</li> </ul>	UDP	6000-65535
<b>All</b>	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 the virtual machines that belong to the same security group / virtual network only. Therefore, there is no need to further adjust them.

Outbound security rules in all subnets are configured by default to allow all traffic. You may adjust them as per your needs.

If you performed Mediant CE deployment via manual installation and configuration, consider creating similar or equivalent security rules in virtual environment specific network configuration.

## 6 Upgrading the 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 6-1: Upgrading Mediant CE via Stack Manager**



Make sure that the Signaling Components have the same or later version as the Media Components.

Upgrade to the 7.6 stream (7.60A.xxx.yyy versions) can be performed only from a 7.4 stream (7.40A.xxx.yyy versions).



If you have an earlier version installed (e.g., from 7.2 stream), first upgrade to a 7.4 stream. Only afterwards, upgrade to a 7.6 stream. Refer to 7.4 version documentation for detailed upgrade instructions.

## 7 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)".



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.

## 8 Licensing Mediant CE

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



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

### 8.1 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.



- 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 8-1: Software License Activation Tool

Home > Software License Activation

### 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](mailto:support@audiocodes.com)  
\*Supports CloudBond 365 version 7.2 and above.

Product Key \*

Fingerprint \*

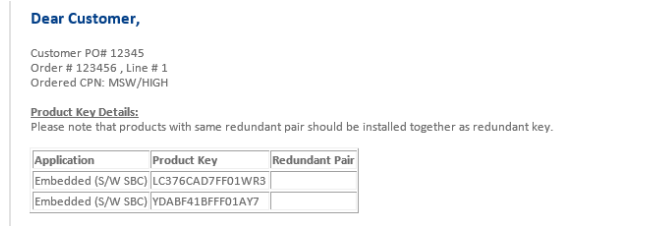
For instructions on how to locate your product's fingerprint, please read the documentation relevant to your product

Email \*

I'm not a robot

SUBMIT

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 8-2: Product Key in Order Confirmation E-mail**

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.



Do **not** modify the contents of the License Key file.

## 8.2 Installing the License Key

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



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.

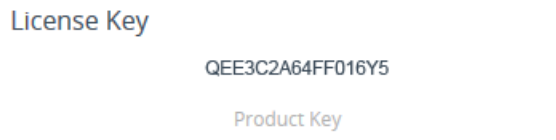
## 8.3 Product Key

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 8-3: Viewing Product Key**

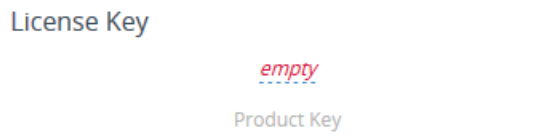


- Device Information page.

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:

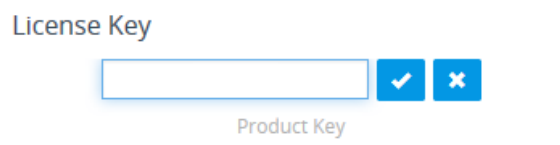
1. Open the License Key page.
2. Locate the Product Key group:



**Figure 8-4: Empty Product Key Field**



3. Click "empty"; the following appears:

**Figure 8-5: 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-11030

