Hardware Installation Manual

AudioCodes Session Border Controller Series

Mediant 9080C SBC

Version 7.4 and later

audiocodes

Notice

Date Published: December-30-2024

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.

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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.

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.

Stay in the Loop with AudioCodes

Notes and Warnings

A safety, environmental and regulatory booklet ("Safety, Environmental, and Regulatory Information") is included in the device packaging. Before installing the device, make sure to carefully review the safety instructions in the booklet provided with the device.

The device is an INDOOR unit and thus, must be installed ONLY indoors. In addition, Ethernet port interface cabling must be routed only indoors and must not exit the building.

For full environmental specifications, please refer to Dell's documentation.

This device must be installed only in a restricted access location.

Service of the device must be made only by qualified service personnel.

AC powered units must be connected only to a grounded AC mains power socket.

Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Caution Laser: This device contains a Class 1 LED/Laser emitting device, as defined by 21CFR 1040 and IEC825. Do not stare directly into the beam or into fiber optic terminations as this can damage your eyesight.

Caution Electrical Shock: Do not attempt to open or disassemble this device. The device carries high voltage. Contact with internal components may cause electrical shock and bodily harm.

For all service and maintenance issues, contact AudioCodes technical support (see Customer Support above).

Reliable Earthing: Reliable earthing of rack- mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

Related Documentation

Document Name
SBC-Gateway Release Notes for Latest Release (LR) Versions 7.4
Mediant 9000 Series SBC User's Manual

Document Revision Record

LTRT	Description
41701	Initial document release.

Table of Contents

1 Introduction

This document describes the hardware and basic deployment of AudioCodes' carrier-grade Mediant 9080C SBC.

This document describes the Mediant 9080C, which is based on Dell PowerEdge R660xs.

The Mediant 9080C is compatible with Version 7.4.600.203 and later.

The Mediant 9080C model can be identified by running the following CLI command:

```
show system hardware
 CPU: Intel(R) Xeon(R) Silver 4410Y, total 48 cores, avx supported
 Memory: 131072 MB
 Chassis: Mediant 9080-C
```

For installation instructions on the Mediant 9000 Rev B, Mediant 9030, and Mediant 9080 Rev. A/B (Gen 10) models, refer to *Mediant 9000 SBC Hardware Installation Manual Ver. 7.2 and later*.

2 Product Configurations

The following configurations are available for the Mediant 9080C SBC.

Table 2-1: AudioCodes Mediant 9080C SBC Product Configurations

Product Configuration	Description
M9080C Configurations	
M9K80C/AC	Mediant 9080C chassis with dual AC power supplies and 12 x 1GbE RJ-45 ports.
M9K80C/AC/R	HA-pair of Mediant 9080C chassis with dual AC power supply and 12 x 1GbE RJ-45 ports.
M9K80C/AC/10GSR	Mediant 9080C chassis with dual AC power supply, 8 x 1GbE RJ-45 ports and 4 x 10GBase-SR ports (SFP+ transceivers).
M9K80C/AC/10GSR/R	HA-pair of Mediant 9080C chassis with dual AC power supply, 8 x 1GbE RJ-45 ports and 4 x 10GBase-SR ports (SFP+ transceivers).
M9K80C/AC/10GLR	Mediant 9080C chassis with dual AC power supply, 8 x 1GbE RJ-45 ports and 4 x 10GBase-LR ports (SFP+ transceivers).
M9K80C/AC/10GLR/R	HA-pair of Mediant 9080C chassis with dual AC power supply, 8 x 1GbE RJ-45 ports and 4 x 10GBase-LR ports (SFP+ transceivers).
M9080C FRU & Upgrades	
FRU/M9KC/10GSR	Mediant 9080C offers 12 x 1GbE RJ-45 ports and supports an upgrade by adding a single 4 x 10GBase-SR SFP+ NIC in the OCP slot. One standard 4 x 1GbE NIC must be removed or disabled, resulting in 8 x 1GbE and 4 x 10GBase-SR ports.
FRU/M9KC/10GLR	Mediant 9080C offers 12 x 1GbE RJ-45 ports and supports an upgrade by adding a single 4 x 10GBase-LR SFP+ NIC in the OCP slot. One standard 4 x 1GbE NIC must be removed or disabled, resulting in 8 x 1GbE and 4 x 10GBase-LR ports.

3 Specifications

The following table lists the device's specifications.

Table 3-1: Mediant 9080C Specifications

CPU	Memory	Disk	Chassis
2 x 12 Cores 2 GHz 30 MB Cache	128 GB DDR5-4000	Mechanical hard drive 2 TB SATA	■ Chassis type: 1RU ■ Network (max. total 12 ports): ✓ 1 GbE (copper): 12 or 8 ports ✓ 10 GbE (SFP+): 0 or 4 ports ■ Installation interfaces: ✓ VGA monitor and keyboard ✓ Remote access through BMC (iDRAC)

4 Physical Description

This section provides a physical description of the device.

Physical Dimensions

The device's chassis dimensions are shown below.

Figure 4-1: Chassis Dimensions

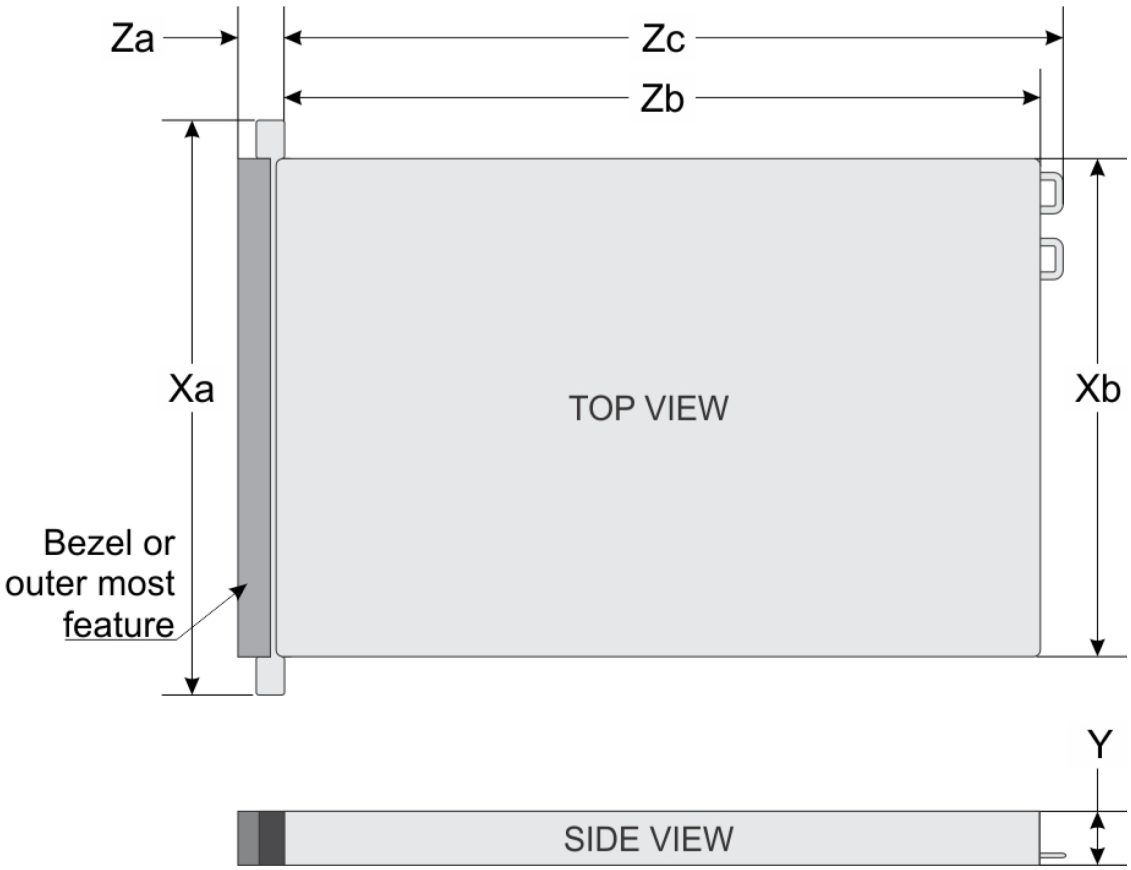


Table 4-1: Chassis Dimensions

Xa	Xb	Y	Za	Zb	Zc
482 mm (18.976 in.)	434 mm (17.08 in.)	42.8 (1.685 in.)	35.84 mm (1.41 in.) with bezel	677.1 mm (26.65 in.) Ear to rear wall	712.95 mm (28.05 in.)

Table 4-2: Physical Dimensions

Item	Description
Physical Dimension	4.28 x 43.4 x 71.3 cm (1.69 x 17.08 x 28.05 in)
Weight (approximate)	19.45 kg (42.88 lb)
Environmental	Operational: 10 to 35°C (50° to 95°F)

LCD Panel

The LCD panel is available only on the front bezel. The optional front bezel is hot pluggable.

The LCD panel provides system information, status, and error messages to indicate if the system is functioning correctly or requires attention. The LCD panel is used to view the iDRAC IP address of the system.

The status and conditions of the LCD panel are outlined here:

- The LCD backlight is white during normal operating conditions.
- If there is an issue, the LCD backlight turns amber and displays an error code followed by descriptive text.

> If the system is connected to a power source and an error is detected, the LCD turns amber regardless of whether the system is powered on or off.

- When the system powers off and there are no errors, the LCD enters the standby mode after five minutes of inactivity. Press any button on the LCD to power it on.
- If the LCD panel stops responding, remove the bezel and reinstall it. If the problem persists, see Getting help.
- The LCD backlight remains off if LCD messaging is powered off using the iDRAC utility, the LCD panel, or other tools.

Figure 4-2: LCD Panel Features

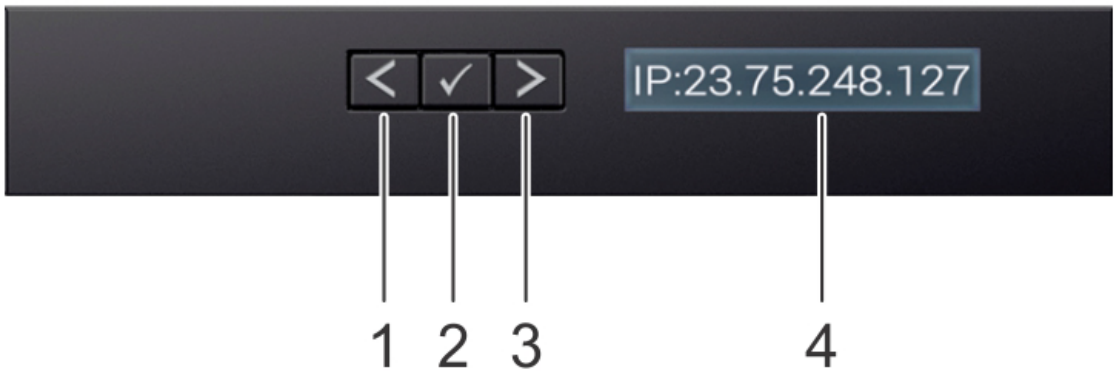


Table 4-3: LCD Panel Features

Item	Button or display	Description
1	Left	Moves the cursor back in one-step increments.
2	Select	Selects the menu item highlighted by the cursor.
3	Right	Moves the cursor forward in one-step increments. During message scrolling: ■ Press and hold the right button to increase scrolling speed. ■ Release the button to stop.
4	LCD display	Displays the system information, status, and error messages or iDRAC IP address. For information about the event and error messages generated by the system firmware and agents that monitor system components, go to the Error and Event Messages Reference Guide.

Front Panel

The device features a 4 x 3.5-inch drive system for standard internal storage hard drives. The device's front panel is shown in the figures below and described in the subsequent table.

Figure 4-3: Front Panel

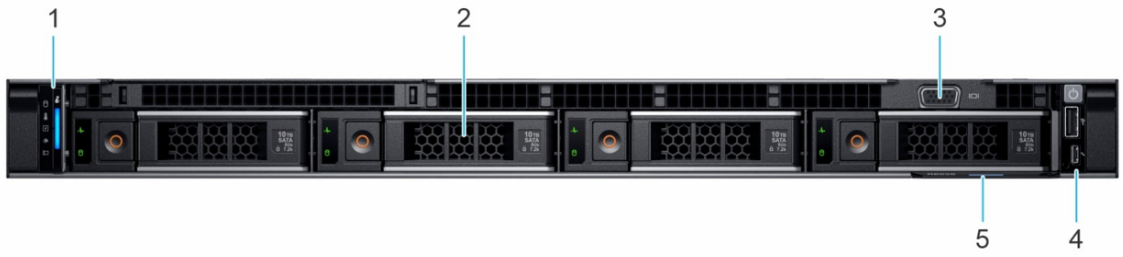


Table 4-4: Front Panel

Item #	Ports, Panels, and Slots	Icon	Description
1	Left control panel	-	Contains the system health, system ID and status LED. Status LED: Enables you to identify any failed hardware components. There are up to five status LEDs and an overall system health LED (Chassis health and system ID) bar. For more information, see the Status LED indicators section.

Item #	Ports, Panels, and Slots	Icon	Description
2	Drive	-	2-TB SATA drive.
3	VGA port		Enables you to connect a display device to the system.
4	Right control panel	-	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
5	Express service tag	-	The Express Service Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. The Information tag also contains the iDRAC secure default password.

Left Control Panel

The left control panel is displayed below and described in the subsequent figure.

Figure 4-4: Left Control Panel

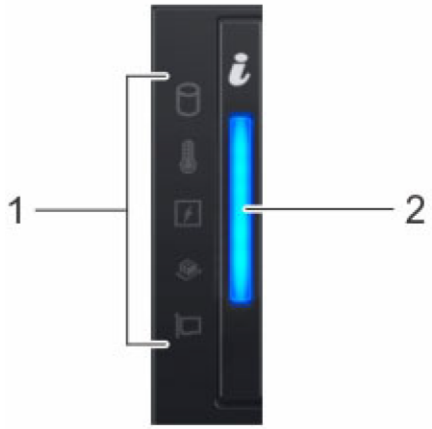


Table 4-5: Left Control Panel

Item #	Indicator, Button, or Connector	Icon	Description
1	Status LED indicators - Indicates the status of the system		Drive indicator. The indicator turns solid amber if there is a drive error. **Corrective action:** ■ Check the System Event Log to determine if the drive has an error.

Item #	Indicator, Button, or Connector	Icon	Description
			■ Run the appropriate Online Diagnostics test. Restart the system and run embedded diagnostics (ePSA). ■ Please contact AudioCodes support.
			Temperature indicator. The indicator turns solid amber if the system experiences a thermal error (for example, the ambient temperature is out of range or there is a fan failure). **Corrective action:** Ensure that none of the following conditions exist: ■ A cooling fan has been removed or has failed. ■ System cover, air shrouds, or back filler bracket has been removed. ■ Ambient temperature is too high. ■ External airflow is obstructed. ■ If the problem persists, contact AudioCodes support.
			Electrical indicator. The indicator turns solid amber if the system experiences an electrical error (for example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator). **Corrective action:** ■ Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reset the PSU. ■ If the problem persists, contact AudioCodes support.

Item #	Indicator, Button, or Connector	Icon	Description
			Memory indicator. The indicator turns solid amber if a memory error occurs. **Corrective action:** ■ Check the System Event Log or system messages for the location of the failed memory. Reset the memory module. ■ If the problem persists, contact AudioCodes support.
			PCIe indicator. The indicator turns solid amber if a PCIe card experiences an error. **Corrective action:** ■ Restart the system. ■ If the problem persists, contact AudioCodes support.
2	System health and system ID indicator		Indicates the status of the system. **Solid blue:** Indicates that the system is powered on, is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode. **Blinking blue:** Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode. **Solid amber:** Indicates that the system is in fail-safe mode. If the problem persists, see the Getting help section. **Blinking amber:** Indicates that the system is experiencing a fault. Check the System Event Log for specific error messages. For information about the event and error messages generated by the system firmware and agents that monitor system components, go to the

Item #	Indicator, Button, or Connector	Icon	Description
			Error and Event Messages Reference Guide.

Right Control Panel

The right control panel is shown below.

Figure 4-5: Right Control Panel

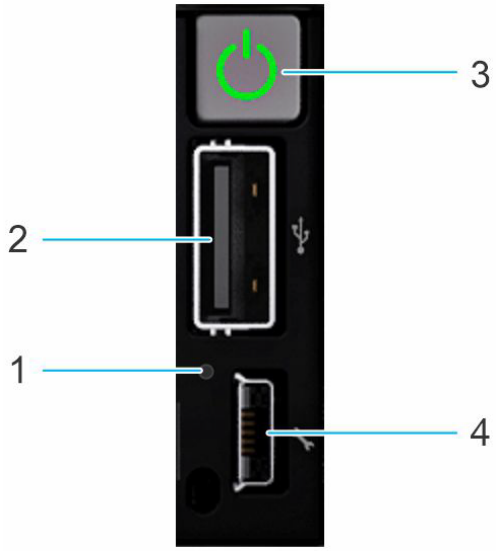


Table 4-6: Right Control Panel

Item	Indicator or button	Icon	Description
1	iDRAC Direct LED indicator	n/a	The iDRAC Direct LED indicator lights up to indicate that the iDRAC Direct port is actively connected to a device
2	USB 2.0-compliant port		Not used.
3	Power button		Indicates if the system is powered on or off. Press the power button to manually power on or off the system. **Note:** Press the power button to gracefully shut down the device.

Item	Indicator or button	Icon	Description
4	iDRAC Direct port (Micro-AB USB)		The iDRAC Direct port (Micro-AB USB) enables you to access the iDRAC direct Micro-AB USB features. For more information, refer to the *Integrated Dell Remote Access Controller 9 User's Guide*. **Note:** You can configure iDRAC Direct by using a USB to micro USB (type AB) cable, which you can connect to your laptop or tablet. Cable length should not exceed 3 feet (0.91 meters). Performance could be affected by cable quality.

iDRAC Direct LED Indicator Codes

Table 4-7: iDRAC Direct LED Indicator Codes

iDRAC Direct LED indicator code	Condition
Solid green for two seconds	Indicates that the laptop or tablet is connected.
Blinking green (on for two seconds and off for two seconds)	Indicates that the laptop or tablet connected is recognized.
LED Indicator off	Indicates that the laptop or tablet is unplugged.

Rear Panel

The rear panel is displayed in the following figure and described in the subsequent table.

Figure 4-6: Rear Panel

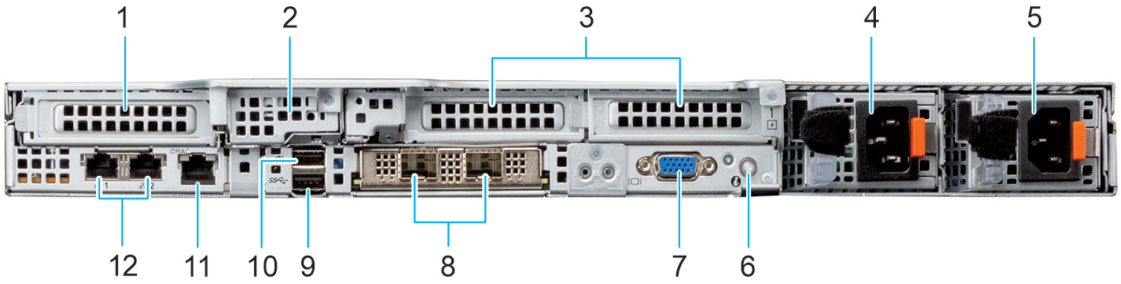


Table 4-8: Rear Panel

Item #	Description	
	Mediant 9080 12 x 1GbE	**Mediant 9080 8 x 1GbE and 4 x 10GbE**

Item #	Description	
		SFP+
1	Slot 1: Quad 1-GbE copper ports	Slot 1: Quad 1-GbE copper ports
2	Optional storage: Not used	Optional storage: Not used
3	Slot 2: Quad 1-GbE copper ports	Slot 2: Quad 1-GbE copper ports
	Slot 3: Quad 1-GbE copper ports	Slot 3: Not Used
4	Power supply 1 (PS1)	Power supply 1 (PS1)
5	Power supply 2 (PS2)	Power supply 2 (PS2)
6	System identification button	System identification button
7	Video port (VGA)	Video port (VGA)
8	OCP slot: Not used	OCP slot: Quad 10-GbE SFP+ ports
9	USB 3.0 port: Not used	USB 3.0 port: Not used
10	USB 2.0 port: Not used	USB 2.0 port: Not used
11	iDRAC dedicated management port	iDRAC dedicated management port
12	Unsupported NIC ports (dust covered)	Unsupported NIC ports (dust covered)

Power Supply Unit Indicator Codes

AC power supply units (PSUs) have an illuminated translucent handle that serves as an indicator. The indicator shows if power is present or if a power fault has occurred.

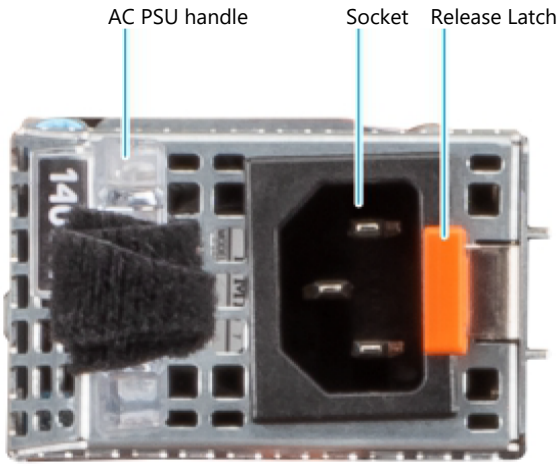
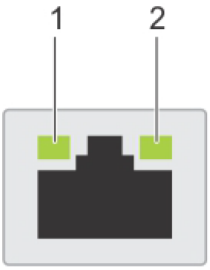


Table 4-9: AC PSU Status Indicator Codes

Power indicator codes	Condition
Green	Indicates that a valid power source is connected to the PSU and the PSU is operational.
Blinking amber	Indicates an issue with the PSU.
Not powered on	Indicates that the power is not connected to the PSU.
Blinking green	Indicates that the firmware of the PSU is being updated. **Warning:** Do not disconnect the power cord or unplug the PSU when updating firmware. If firmware update is interrupted, the PSUs will not function.
Blinking greens and powers off	When hot-plugging a PSU, it blinks green five times at a rate of 4 Hz and powers off. This indicates a PSU mismatch due to efficiency, feature set, health status, or supported voltage. **Warning:**: ■ If two PSUs are installed, both the PSUs must have the same type of label; for example, Extended Power Performance (EPP) label. Mixing PSUs from previous generations of PowerEdge servers is not supported, even if the PSUs have the same power rating. This results in a PSU mismatch condition or failure to power on the system. ■ If two PSUs are used, they must be of the same type and have the same maximum output power. ■ When correcting a PSU mismatch, replace the PSU with the blinking indicator. Swapping the PSU to make a matched pair can result in an error condition and an unexpected system shutdown. To change from a high output configuration to a low output configuration or vice versa, you must power off the system. ■ AC PSUs support both 240 V and 120 V input voltages with the exception of Titanium PSUs, which support only 240 V. When two identical PSUs receive different input voltages, they can output different wattages, and trigger a mismatch.

NIC Indicator Codes

Each NIC on the rear panel has indicators that provide information about the activity and link status. The activity LED indicator indicates if data is flowing through the NIC, and the link LED indicator indicates the speed of the connected network.



1 = Link LED indicator

2 = Activity LED indicator

Table 4-10: NIC Indicator Codes

Power indicator codes	Condition
Link and activity indicators are off.	Indicates that the NIC is not connected to the network.
Link indicator is green, and activity indicator is blinking green.	Indicates that the NIC is connected to a valid network at its maximum port speed, and data is being sent or received.
Link indicator is amber, and activity indicator is blinking green.	Indicates that the NIC is connected to a valid network at less than its maximum port speed, and data is being sent or received.
Link indicator is green, and activity indicator is off.	Indicates that the NIC is connected to a valid network at its maximum port speed, and data is not being sent or received.
Link indicator is amber, and activity indicator is off.	Indicates that the NIC is connected to a valid network at less than its maximum port speed, and data is not being sent or received.
Link indicator is blinking green, and activity is off.	Indicates that the NIC identity is enabled through the NIC configuration utility.

5 Deploying the Device

This chapter describes how to deploy the device. The following sections are described:

- Deploying the Rail Kit
- Connecting to Power and Replacing Power Supply
- Connecting Display and Keyboard
- Connecting Device to IP Network for 1-GbE Copper
- Connecting Device to IP Network with SFP
- Viewing Network Port Status

Deploying the Rail Kit

The type of Rail that are providing is “A11 Drop-in/Stab-in 4-Post Rail”.

This section provides information about the mounting features and key dimensions of the rack rails used for mounting the devicein a rack enclosure. This section also provides a compatibility summary for racks as well as some common third-party racks. Note that the product list is not all inclusive and updates will be made as needed.

The dimensions provided in this document are for reference only. Some minor deviations due to manufacturing tolerances and variances should be expected.

The rail kits may not be compatible with racks from other vendors, however, all rail kits are designed for compliance with all EIA-310-D and later revision specifications for 19-inch racks.

For instructions for deploying the rail system, refer to the printed instructions "Quick Deploy Rail System Installation Instructions".

Rack Mount Safety Instructions: When installing the chassis in a rack, implement the following safety instructions:

- Elevated Operating Temperature: If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_A) of 35°C (95°F).
- Reduced Air Flow: Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

- Two people are required to mount the device in the 19-inch rack.

- When attaching the chassis to the rack, it is mandatory to connect it using both the front-mounting brackets and the rear-mounting brackets (supplied).

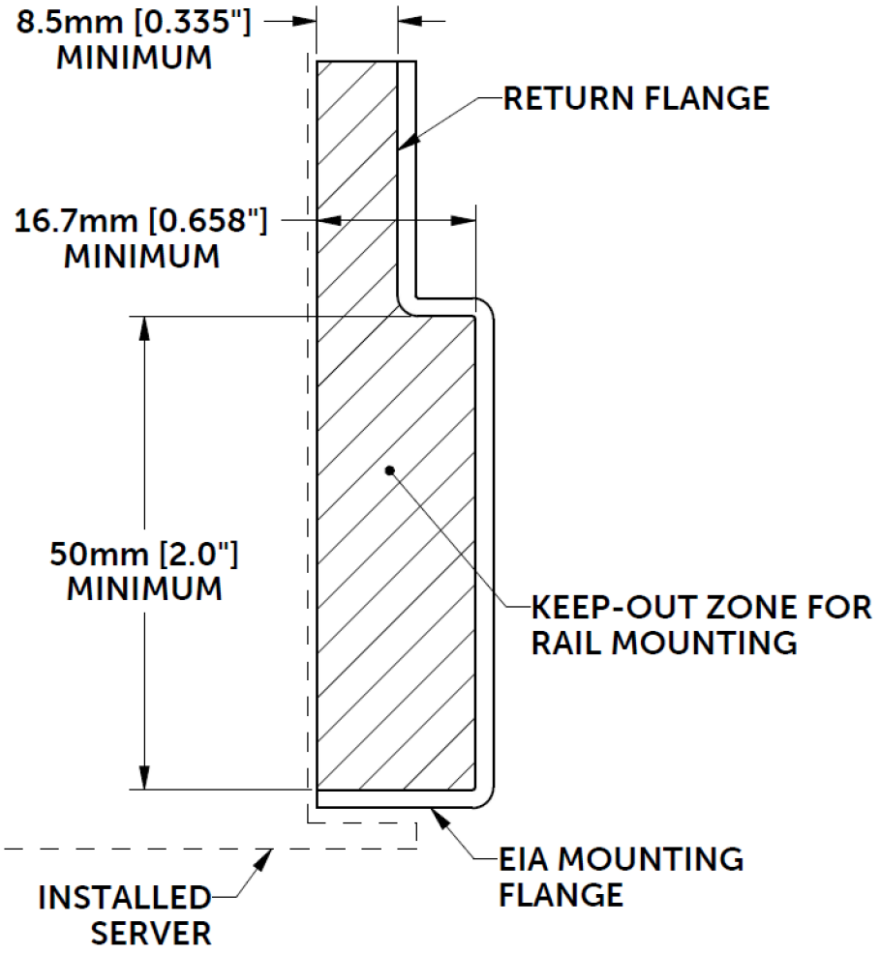
Considerations

Please pay attention to the footnotes indicated in the tables because they provide important information on using the rails in different racks and circumstances.

It is assumed that rack mount peripherals and cable bundles do not protrude into the space directly behind the systems.

Note that rail kits with a Rail Identifier code have been designed to be compliant with the Server System Infrastructure (SSI) Specification for Computer Server Cabinet Enclosures & Racks, which specifies a minimum offset distance for return flanges on the rack mounting flanges to allow sufficient room for mounting the rail kits, as indicated in the following figure.

Figure 5-1: Top View of Right-Front EIA Mounting Flange



Some third-party racks may not meet this requirement; it's not feasible to provide a solution for every circumstance.

Rack Type - 4 Post

The rail kits install in 4-post rack types, which contain vertical mounting flanges with either square-hole, unthreaded round-hole, or threaded round-hole designs as part of the rack and rail interface.

For more information, see Rail (A11) Technical Specifications below.

Mounting Interface

Refer to the Dell Technologies Enterprise Systems Rail Sizing and Rack Compatibility Matrix for detailed information on the following:

- Specific rail types
- Rail adjustability ranges for different rack mounting flange types
- Rail depth with and without cable management accessories
- Supported rack types for various rack mounting flange types

Rail Type - System Installation Method

Drop-in/Stab-in rails (Combo Rail) are a feature rich rail solution that allows a system to be fully extended out of the rack for service and the user has the option to install the system into the rail using a drop-in method like the ReadyRails sliding rails, or a stab-in method like the ReadyRails static rails. Drop-in/Stab-in rails support CMA or SRB applications. CMA and SRB applications must be detached in order to remove the inner member from the rails.

A “drop-in” design means that the system is installed vertically into the rails by inserting the standoffs on the sides of the system into the “J-slots” in the inner rail members with the rails in the fully extended position. The recommended method of installation is to first insert the rear standoffs on the system into the rear J-slots on the rails to free up a hand and then rotate the system down into the remaining J-slots while using the free hand to hold the rail against the side of the system.

A “stab-in” design means that the inner (chassis) rail members must first be attached to the sides of the system and then inserted into the outer (cabinet) members installed in the rack.

Rail (A11) Technical Specifications

The technical specifications of this Rail (A11) is shown below:

Parameter	Value
Product	R660xs (4-HDD/10-HDD)
Rail identifier	A11
Mounting interface	Generic Tool-less

Parameter	Value		
Rail type	Drop-in / Stab-in		
Rack types supported	4-Post	Square	√
		Round	√
		Thread	√[1]
Rail adjustability range (mm)	Square	Min	609[2]
		Max	931
	Round	Min	609[2]
		Max	931
	Threaded	Min	609[2]
		Max	931
Rail depth (mm)	without CMA/SRB	770[3]	
	with CMA(SRB)	89 (811/833)	

Connecting to Power and Replacing Power Supply

This section lists the various warnings, cautions and notes regarding connecting to the power supply and replacing power supply units.

To view a video on replacing the Power Supply, click here.

To reduce the risk of electric shock or energy hazards:

- This equipment must be installed by trained service personnel, as defined by the NEC and IEC 60950-1, Second Edition, the standard for Safety of Information Technology Equipment.
- Connect the equipment to a reliably grounded Secondary circuit source. A Secondary circuit has no direct connection to a Primary circuit and derives its power from a transformer, converter, or equivalent isolation device.

[1]The hole diameter of the threaded hole rack flange equal or greater than 10-32UNF-2B.

[2]Chassis type utilizes the Self-Adjusting Rail Feature to install properly into rack.

[3]With CMA brackets removed.

- Both Power Supply modules (1 and 2) must be connected. Ensure that you connect each one to a different AC power supply source. Two Power Supplies provide 1+1 power load-sharing and redundancy. The AC power sockets are located on the device's rear panel.
- The two AC power sources must have the same ground potential.
- The device must be connected (by service personnel) to a socket-outlet with a protective earthing connection.
- Use only a certified 3-conductor power cord, supplied with the unit.

To reduce the risk of personal injury from hot surfaces, allow the power supply or power supply blank to cool before touching it.

The device must be connected (by service personnel) to a socket-outlet with a protective earthing connection

- Before extracting the Power Supply module, disconnect the power cord from the module.
- Before extracting the Power Supply module (after you have disconnected the power cord), wait at least three seconds for the capacitors to discharge.

When connecting both Power Supply modules, the two AC power sources must have the same ground potential.

Power Specifications

AC power specifications are shown in the table below:

PSU	Class	Heat dissipation (maximum) (BTU/hr)	Frequency (Hz)	AC Voltage			Current (A)
				100–120 V	200–240 V	277 V	
800 W mixed mode	Platinum	3000	50/60	800 W	800 W	N/A	9.2 A - 4.7 A

Connecting Display and Keyboard

To connect to the CLI console, perform the cable connections:

- Connect the display to the 15-pin HD D-Sub (HD-15) VGA port.

- Connect the keyboard to the USB port.

Connecting Device to IP Network for 1-GbE Copper

This section shows how to connect the device to the IP network using the copper 1-GbE ports.

Intra-building connections of the device require the use of shielded cables grounded at both ends.

> The intra-building ports of the equipment are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building ports of the equipment must not be metallically connected to interfaces that connect to the Outside Plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports, as described in GR-1089–CORE, Issue 4) and requires isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring

The device's management interface uses special string names to represent the Ethernet ports, as shown in the following figure:

Figure 5-2: Management Name per Physical Ethernet Port – Mediant 9080C with 12 x GbE Port Configuration

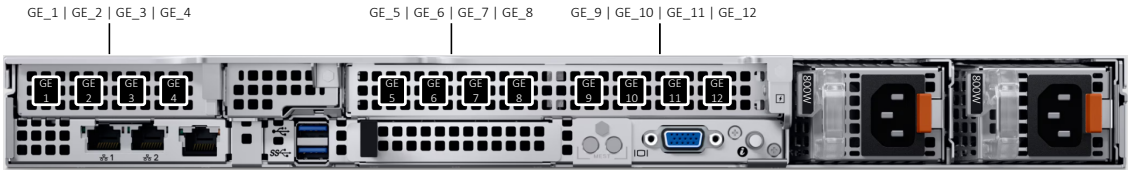
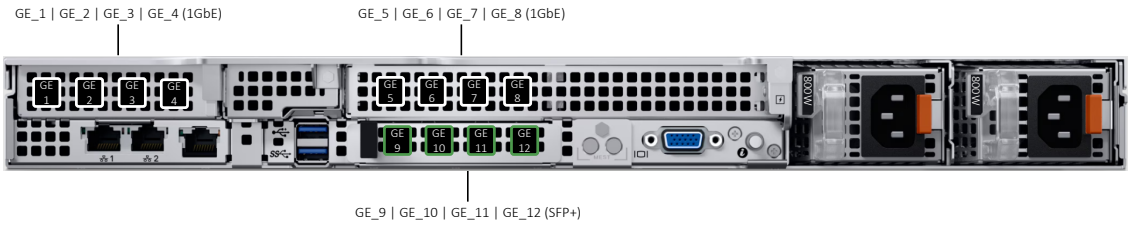


Figure 5-3: Management Name per Physical Ethernet Port – Mediant 9080C with 8 x 1GbE + 4 x 10GbE Port Configuration



➢ **To connect the device to the IP network:**

- Use an Ethernet cable to connect the GE-1 RJ-45 network port on the server's rear panel to the LAN.

Connecting Device to IP Network with SFP+

The following procedure describes how to cable the device to the network, using the 10 Gbps optical Small Form-Factor Pluggable (SFP+) transceiver modules.

Caution Laser: This device contains a Class 1 LED/Laser emitting device, as defined by 21CFR 1040 and IEC825. Do not stare directly into the beam or into fiber optic terminations as this can damage your eyesight.

Care in Handling Fiber Optic Cabling:

1. Excessive bending of the Fiber Optic Cable can cause distortion and signal losses.
2. Ensure the minimum bending radius recommended by the Fiber Optic Cable supplier.
3. Incoming optic cabling from the network infrastructure can originate from the top of the rack or from another shelf within the rack. Preserve the minimum-bending ratio indicated by the cable manufacturer.
4. To ensure full high-availability capabilities, the configuration of the interface to the IP backbone must include certain redundant features from which two separate fiber optic cables are entering the device.

➢ **To connect to the network using SFP+:**

1. Remove the protective dust plug from the SFP+ transceiver module.
2. Connect a cable with LX-type or SX-type plugs to the SFP+ transceivers:

Figure 5-4: Cabling Network using SFP+

Viewing Network Port Status

Use the CLI command `show network physical-port` to view network port status (up/down) and MAC address:

```
# show network physical-port

Port Num  Port Name  MAC Address       Speed Duplexity Link Status Native VLAN  Driver Info
--------  ---------  -----------       ----- --------- ----------- -----------  -----------
1          GE_1      20:3a:43:a5:3f:98  1Gbps FULL     UP           1           igb-zc
2          GE_2      20:3a:43:a5:3f:99                 DOWN         1           igb-zc
3          GE_3      20:3a:43:a5:3f:9a                 DOWN         1           igb-zc
4          GE_4      20:3a:43:a5:3f:9b                 DOWN         1           igb-zc
5          GE_5      20:3a:43:a5:4f:98                 DOWN         1           igb-zc
6          GE_6      20:3a:43:a5:4f:99                 DOWN         1           igb-zc
7          GE_7      20:3a:43:a5:4f:9a                 DOWN         1           igb-zc
8          GE_8      20:3a:43:a5:4f:9b                 DOWN         1           igb-zc
9          GE_9      20:3a:43:a5:a4:40                 DOWN         1           igb-zc
10         GE_10     20:3a:43:a5:a4:41                 DOWN         1           igb-zc
11         GE_11     20:3a:43:a5:a4:42                 DOWN         1           igb-zc
12         GE_12     20:3a:43:a5:a4:43                 DOWN         1           igb-zc
```

For 10G SFP+ ports, the 'Driver Info' column displays "ice-zc" instead of "igb-zc", but the port name remains the same (i.e., "GE_*n*").

6 Fiber Network Card Support

This section describes the device's fiber network card support.

Supported Configurations

The network cards located in PCIe slot 3 (as shown in Rear Panel on page 11), can be replaced with SFP+ cards in any of the following supported configurations:

Table 6-1: Supported Configurations with SFP Network Cards

Slot 1-3	OCP Slot	Total Network Ports
Slot 1: Quad 1 GbE Copper **Slot 2:** Quad 1 GbE Copper **Slot 3:** Not Used	Quad SFP+ 10G with LR transceivers	8 x 1 GbE Copper + 4 x 10G SFP+ LR
Slot 1: Quad 1 GbE Copper **Slot 2:** Quad 1 GbE Copper **Slot 3:** Not Used	Quad SFP+ 10G with SR transceivers	8 x 1 GbE Copper + 4 x 10G SFP+ SR

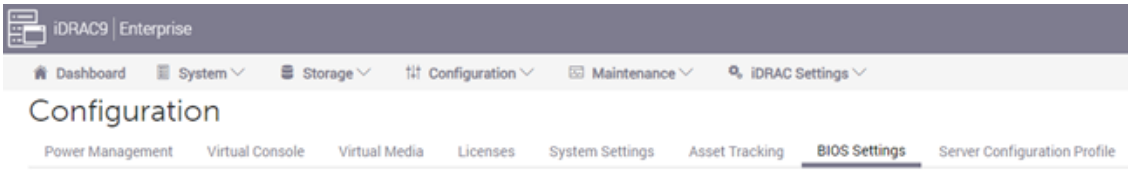
Fiber Network cards must be ordered from AudioCodes.

Replacing Copper NIC with Fiber Network Card

Mediant 9080C supports 12 network interfaces. Therefore, the 4 x 1GbE located in Slot 3 should be disabled and a new network card with 4 x SFP+ ports will be added to the OCP slot and indexed as GE_9 through to GE_12.

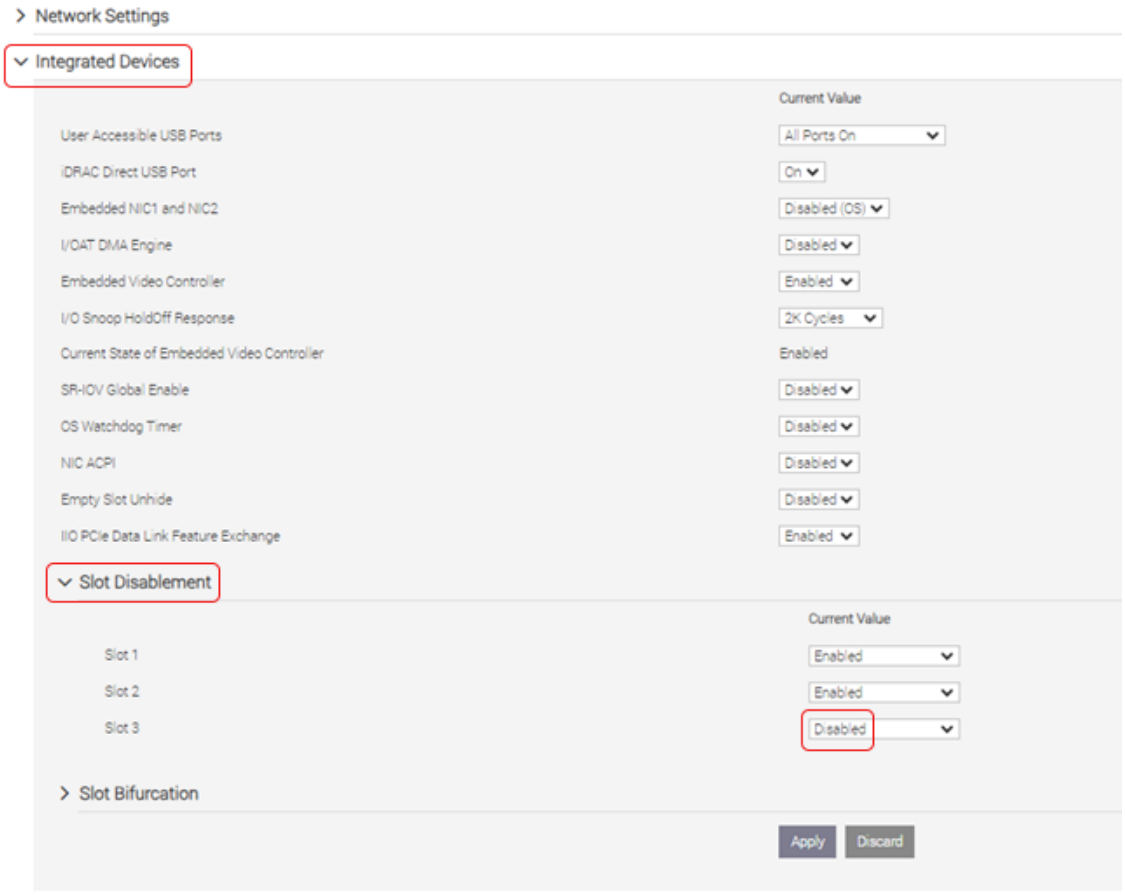
➢ **To replace the copper NIC with Fiber Network Card:**

1. Disconnect the network cables from the slot to be removed (Slot 3).
2. Disable the PCIe card in Slot 3 in the BIOS:
   a. Access the iDRAC web management, as described in Connecting to Remote Management (iDRAC) on page 25.
   b. Select the **Configuration** menu, and then click the **BIOS Settings** tab:



c. Expand **Integrated Devices** > **Slot Disablement.**

d. Change Slot 3 to **Disabled**:



e. Click **Apply**.

f. Scroll down to the bottom of the page and select **At Next Reboot**.

3. Power off the server and disconnect it from the power source.
4. Install the OCP SFP+ network card, as described in Dell's documentation.
5. Connect the optic cables, as described in Connecting Device to IP Network with SFP+ on page 20.
6. Power on the server. When the device completes loading, the new SFPs are labeled "GE_9" through "GE_12".

7 Connecting to Remote Management (iDRAC)

The device allows remote management using Dell's iDRAC controller. The iDRAC is used for remote virtual console, monitoring the server components, and updating the server firmwares.

The complete guide for the iDRAC interface can be found here.

By default, the server is provided with the following iDRAC parameters:

- The iDRAC network port is configured to DHCP.
- iDRAC credentials:
  - Username: **root**
  - Password: The password is shown on the Information tag, located on the bottom-right of the front panel (Item #5 in Front Panel on page 6). You need to pull the tag out. The password is written on the downside of the tag.

➢ **To connect to the iDRAC web management:**

1. Make sure that the iDRAC network port is connected to the LAN.
2. When connected, the DHCP IP address is displayed on the LCD screen.
3. Use a web browser to access the iDRAC web management site using this iDRAC IP address.
4. Use the iDRAC credentials to log in to the web management interface.

8 SBC Initial Configuration

This chapter describes the procedures for the initial configuration of the device.

- After completing the steps in this section, it's recommended to change the default Admin user login passwords to prevent unauthorized access.
- For security-related recommendations to follow during device installation, see Security Recommendations on page 35.

Reconfiguring Default IP Address to Match Customer Network Settings

The device is supplied with software preinstalled. By default, the device is assigned with a default IP address that will most likely be inaccessible from the customer's network.

Figure 8-1: Default IP Address

Parameter	Value
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

Reconfigure the IP address to connect to the Device's Web-based management tool (hereafter referred to as Web interface).

➢ **To reconfigure the IP address using CLI:**

1. Use the VGA monitor and keyboard to connect to the CLI management interface. Alternatively, you can access the device's CLI through iDRAC virtual console.
2. At the prompt, type the username (default is Admin - case sensitive):

```
Username: Admin
```

3. At the prompt, type the password (default is Admin - case sensitive):

```
Password: Admin
```

4. At the prompt, run the following command:

```
> enable
```

5. At the prompt, type the password again:

```
Password: Admin
```

6. At the prompt, type the following commands to access the network interface configuration:

```
# configure network
(config-network)# interface network-if 0
```

Use the Tab key to auto-complete partially entered commands.

7. At the prompt, type the following commands to configure the IP address, prefix length and default gateway:

```
(network-if-0)# ip-address 10.4.212.155
(network-if-0)# prefix-length 16
(network-if-0)# gateway 10.4.0.1
(network-if-0)# exit
```

8. At the prompt, type the following command to complete the network configuration:

```
(network-if-0)# exit
```

9. If the device is connected to the IP network that uses VLAN ID (for example, VLAN ID 10), type the following commands to configure it in the Ethernet Device table (otherwise skip to step 10):

```
(config-network)# interface network-dev 0
(network-dev-0)# vlan-id 10
(network-dev-0)# tagging tagged
(network-dev-0)# exit
```

10. At the prompt, type the following command to complete the configuration:

```
(network-dev-0)# exit
```

11. At the prompt, make sure that Port #1 is connected (Link is UP) using the `show network physical-port` CLI command, as described in Viewing Network Port Status,
By default, Port #1 (GE_1) is mapped to network-if-0.

12. At the prompt, type the following command to save the configuration, reset the device, and activate the new configuration:

```
# reload now
```

After the device restarts, connect to its Web interface to continue provisioning. Change the default Admin user login passwords to prevent unauthorized access. For more information, see the device's *User's Manual*.

Licensing the Device

The device is supplied with a pre-installed software and License Key. Use the pre-installed License Key to enable the call capacity and features that you ordered. To upgrade your License Key, refer to the device's User's Manual.

9 Device Software Upgrade and Re-installation

This chapter describes device software upgrade and re-installation.

Installing an HA System

You can set up two devices to function in a High Availability (HA) configuration.

For details on upgrading the device software in an HA setup without causing service interruptions (Hitless Upgrade), please consult the device's *User Manual*.

Upgrading

You can update the device's software, for example, to implement software fixes. For more information, refer to the device's User's Manual.

Reinstalling Device Software from an ISO Image

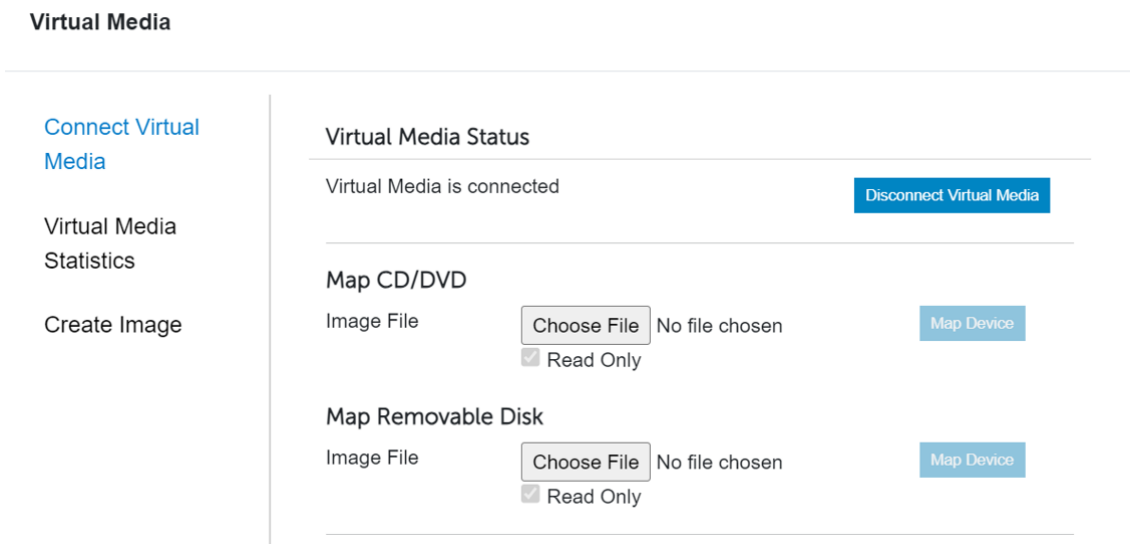
The device is pre-installed on the device's server. In case a clean installation of the device's software is required, you should download the latest installation image from the AudioCodes website and install the software from the iDRAC Virtual Media.

> A clean installation deletes any user configuration, data or snapshots that were previously resident on the device.

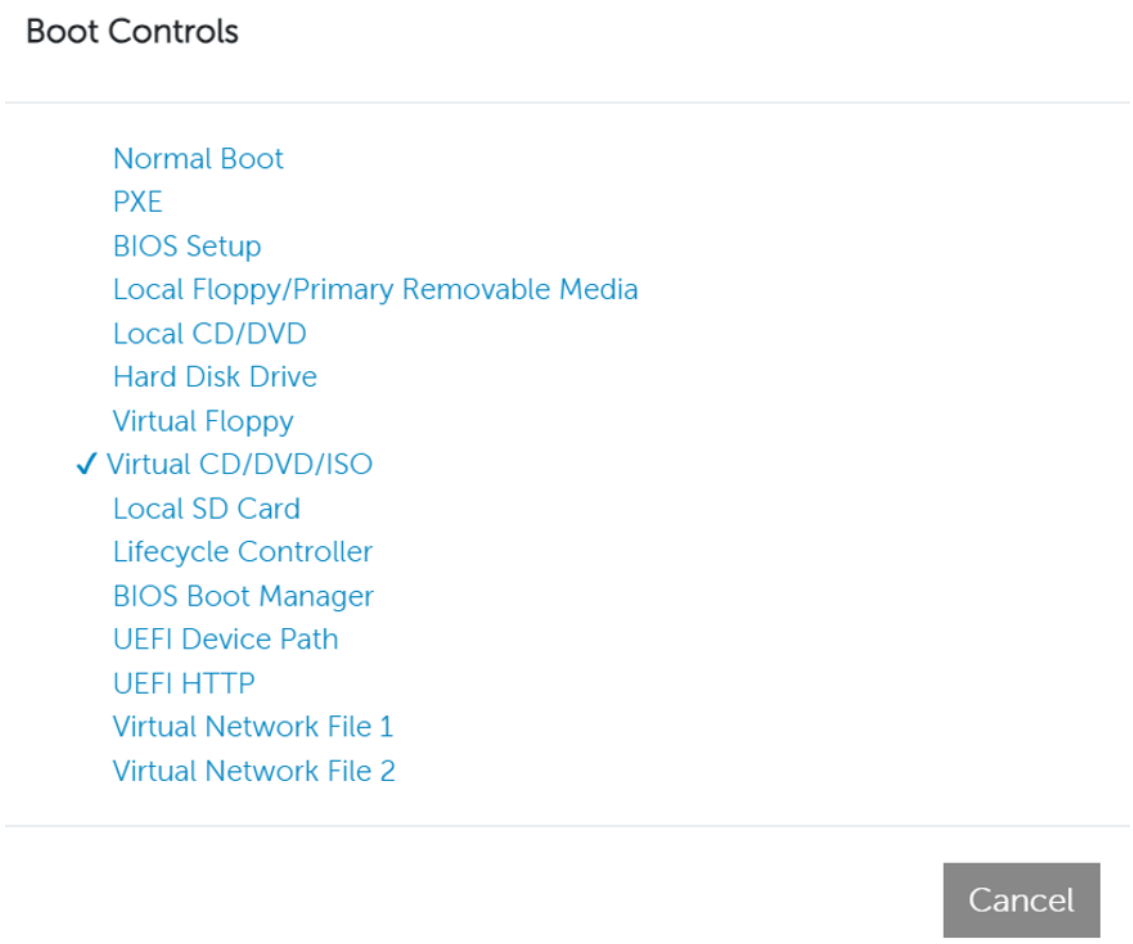
➢ **To install Mediant SBC:**

1. Download the latest ISO file containing the device's software from AudioCodes website.
2. In the iDRAC web management dashboard, start the Virtual Console.
3. In the Virtual Console menu, choose **Virtual Media** > **Connect Virtual Media** > **Map CD/DVD** > **Choose File** (see following figure).
4. Browse to the device's software ISO file that you downloaded from AudioCodes website, and then click **Open**.
5. Click **Map Device**.

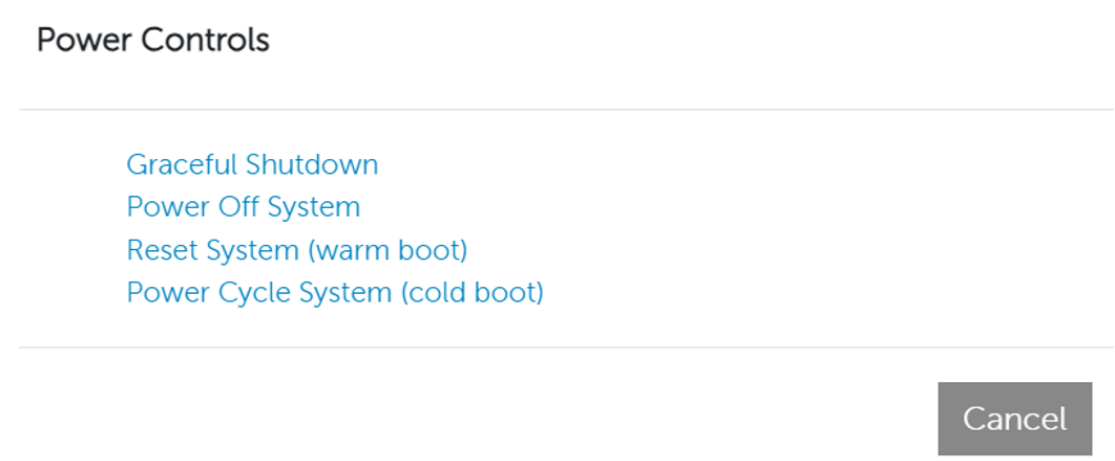
Figure 9-1: Mounting ISO Image from Virtual Console



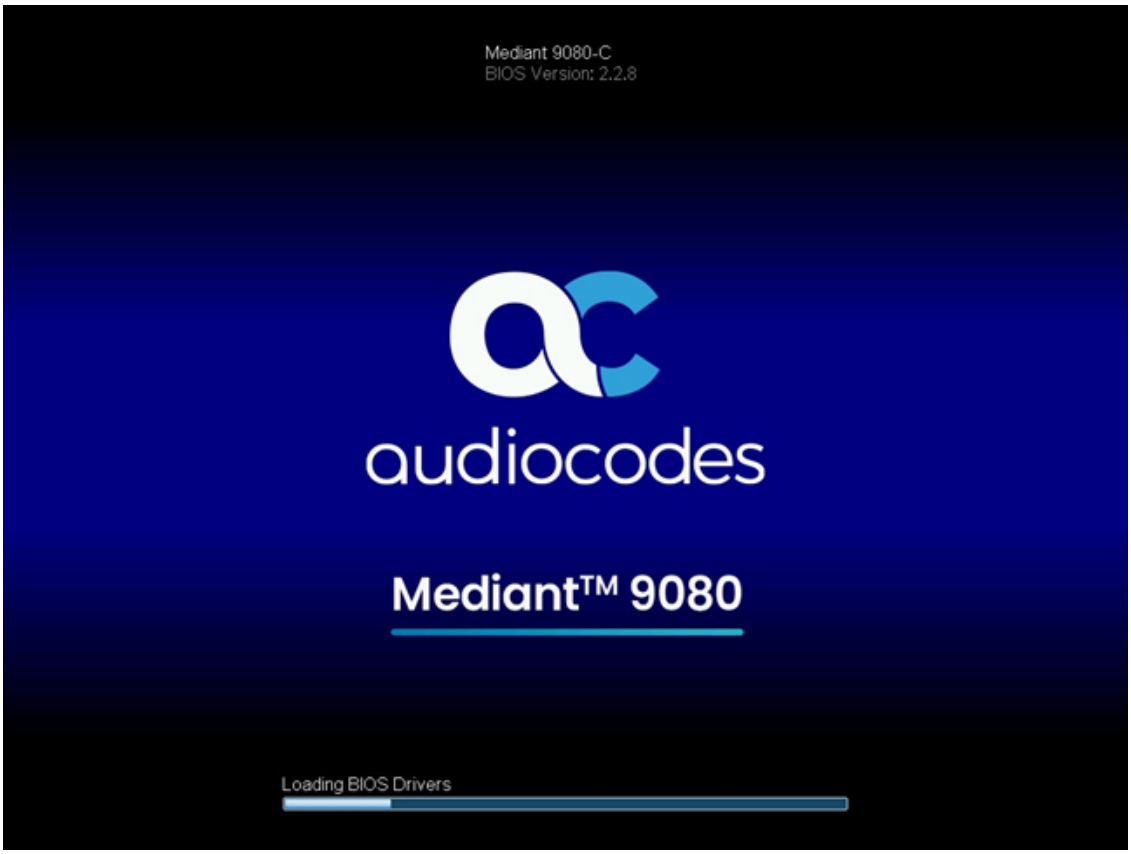
6. Click the **Boot on the Virtual Console** menu, and then choose **Virtual CD/DVD/ISO**:



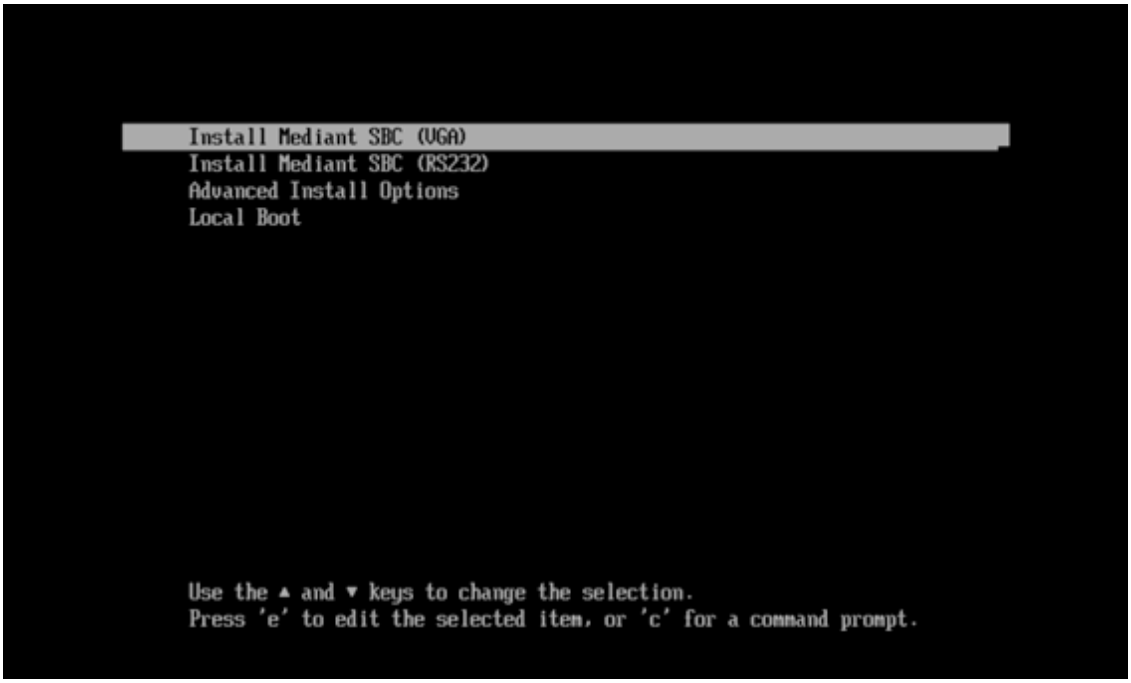
7. Click the **Power on the Virtual Console** menu, and then choose **Reset System** (warm boot):



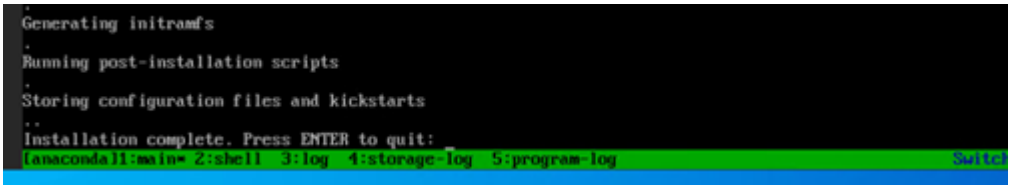
The server boots from the Virtual Console and then the Mediant SBC Installation Menu is displayed:



Installation Start Prompt:



8. Press the ENTER key to Install Mediant SBC (VGA); installation commences from the ILO virtual drive.
9. Wait for the 'Complete' prompt. Installation takes approximately 40 minutes:



10. Press ENTER to reboot the server; after rebooting, the server boots from the local disk to the newly installed device software.

10 Rescue Options

The device features a System Snapshots mechanism that provides the capability of returning the system to a previous state. The mechanism may be used as a rescue option if a system malfunction occurs. For more information, refer to the device's User's Manual.

11 Firmware Upgrades

The device uses several types of firmware to ensure optimal performance, security, and functionality. Regularly updating your server's firmware is best practice to maintain security, performance, and reliability. Some of the firmware components might affect the performance and functionality of the device and therefore, must first get approval from AudioCodes.

Refer to AudioCodes Services Portal for a list of the latest approved firmware components and for instructions on how to install them. You need to have an active support contract to access the Services Portal. After logging in, navigate to the Mediant 9080C product page.

Key Firmware Components:

- **BIOS:** Initializes hardware during boot and provides runtime services. Updates improve compatibility, stability, and performance.
- **iDRAC:** Enables remote server management. Updates enhance management features, security, and reliability.
- **Lifecycle Controller:** Simplifies server deployment and maintenance. Updates add features and improve efficiency.
- **NIC Firmware:** Controls network hardware. Updates enhance performance, security, and compatibility.
- **PSU Firmware:** Manages server power supply. Updates improve efficiency and reliability.

To ensure optimal performance and security, it is recommended to regularly check for firmware updates on AudioCodes Services Portal. Apply critical updates immediately to address any security vulnerabilities or major bugs.

12 Security Recommendations

AudioCodes advises the below recommendations during device installation to ensure optimal security for your Mediant 9080C SBC. By following these recommendations, you can significantly enhance the security of your Mediant 9080C SBC. For additional recommendations, refer to the *Recommended Security Guidelines* document.

If you have any questions or need further assistance, please refer to the product's *Release Notes* or contact AudioCodes Support.

Table 12-1: Security Recommendations

Description	Recommended Action
Network Security	
Dedicated Management Network	Connect the iDRAC to a separate, isolated management network. This network should be physically and logically isolated from the production network using firewalls and VLANs.
Avoid Direct Internet Connection	Do not connect the iDRAC directly to the internet.
Access Control and Authentication	
Change Default iDRAC Password	Change the default iDRAC password located on the pull-out service tag. Choose a strong, unique password that meets the complexity requirements. **Keep the new password in a safe and known place for remote service support**.
iDRAC IP Range Filtering	Limit access to authorized management stations only. Define specific IP ranges or subnets allowed to access the iDRAC.
Use TLS Secured Versions for iDRAC	Ensure all iDRAC network communications are encrypted using TLS 1.2 or higher to protect data in transit.
Directory Service Integration	Integrate with Microsoft Active Directory or LDAP to manage user accounts, roles, and permissions centrally. Configure iDRAC to use LDAPS (LDAP over SSL) for secure communication with the directory server.
Multi-Factor Authentication	Enable MFA using supported methods such as RSA SecurID or Smartcards (CAC/PIV). Configure iDRAC to require an additional authentication factor beyond the password for login.

Description	Recommended Action
System Integrity	
Setup Password	You can enable the Setup password option to prevent access to the device BIOS settings. It is recommended to use a strong password of at least 8 characters. **Keep the new password in a safe and known place for service support**.
Secure Boot / Digitally signed Software Upgrades	**Do not Enable Secure Boot** in the BIOS settings as it is not compatible with the SBC software installation. When upgrading the device software, all CMP files are digitally signed. This digital signature ensures that only files that have been verified and approved by AudioCodes can be loaded to the device. During the update process, the device verifies the digital signature of the CMP file. If the file is not signed or the signature does not match, the update is rejected. This ensures that only authentic and unaltered files are used.
Chassis Intrusion Detection	Enable chassis intrusion detection in the iDRAC settings. Configure alerts to notify administrators of any detected intrusion attempts. This provides an additional layer of security by alerting personnel to potential physical tampering with the server.
User Accessible USB Ports	USB Port Management is a security feature that allows administrators to selectively enable or disable USB ports on the device. This helps prevent unauthorized use of USB devices, which can be a potential security risk. It is recommended to disable the User Accessible USB Ports.
Front Bezel Lock	Lock the front bezel to prevent unauthorized access to the server's hard drives.
Secure Rack Installation	Ensure the server is securely mounted in a locked rack or cabinet to prevent unauthorized access.
Firmware Management	
Regular Firmware Updates	Regularly check for firmware updates on the AudioCodes Support website and install them promptly. For non-HA deployments, schedule these updates during maintenance windows.
Device Recycling	
System Erase	Before discarding the device, use System Erase to securely wipe data from storage drives. This ensures data is irrecoverable and protects against unauthorized access.

Description	Recommended Action
Secure SBC Management Access	
Change Default Admin User Login Passwords	Change the default Admin user login passwords immediately upon setup to prevent unauthorized access.
Use Strong Authentication Passwords	Ensure strong passwords for authentication.
Implement LDAP-based User Authentication	Use LDAP for centralized user authentication and authorization.
Implement Two-Way Authentication with X.509 Certificates	Use X.509 certificates for two-way authentication.
Secure Access using HTTPS	Ensure all management access is secured using HTTPS.
Use TLS Secured Versions for Management	Ensure all management network communications are encrypted using TLS 1.2 or later to protect data in transit.
Secure Telnet Sessions	Avoid using Telnet; if necessary, secure sessions.
Secure CLI Sessions by SSH	Use SSH for securing CLI sessions.
Define Web, Telnet, and SSH Authorized Access List	Define an authorized access list.
Secure SNMP Interface Access	Prefer SNMPv3 over SNMPv2 for secure SNMP interface access
Secure SIP using TLS (SIPS)	
Use TLS for SIP Interfaces and	Use TLS for SIP interfaces and block unnecessary TCP/UDP ports.

Description	Recommended Action
Block TCP/UDP Ports	
Implement X.509 Certificates for SIPS (TLS) Sessions	Use X.509 certificates for securing SIPS (TLS) sessions.
Use TLS Secured Versions for SIP	Ensure all network communications are encrypted using TLS 1.2 or later to protect data in transit.
Use an NTP Server	Configure an NTP server on the SBC application (not on iDRAC settings) to ensure accurate time synchronization.

This page is intentionally left blank.

International Headquarters

6 Ofra Haza Street

Naimi Park

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/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-41701