

Version 7.2 to 7.4 Upgrade Procedure

Mediant 9000/9030/9080 SBC
Mediant Server Edition (SE) SBC
Mediant Virtual Edition (VE) SBC
Mediant Cloud Edition (CE) SBC



Table of Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 7 |
| 1.1 | Supported Versions | 7 |
| 2 | Upgrading Standalone Mediant 9000/9030/9080/SE | 9 |
| 2.1 | Prerequisites | 9 |
| 2.2 | Service Affecting | 9 |
| 2.3 | Upgrade Procedure | 9 |
| 2.4 | Rollback Procedure | 11 |
| 3 | Upgrading High-Availability (HA) Mediant 9000/9030/9080/SE via Hitless Procedure..... | 13 |
| 3.1 | Prerequisites | 13 |
| 3.2 | Service Affecting | 14 |
| 3.3 | Upgrade Summary | 14 |
| 3.3.1 | Upgrading Device in a Media Transcoding Cluster | 14 |
| 3.4 | Upgrade Procedure | 14 |
| 3.5 | Rollback Procedure | 16 |
| 4 | Upgrading High-Availability (HA) Mediant 9000/9030/9080/SE via Non-Hitless Procedure | 17 |
| 4.1 | Prerequisites | 17 |
| 4.2 | Service Affecting | 18 |
| 4.3 | Upgrade Procedure | 18 |
| 4.4 | Rollback Procedure | 20 |
| 5 | Upgrading via Side-By-Side Deployment on VMware, KVM or Hyper-V | 21 |
| 5.1 | Process Overview | 21 |
| 5.2 | Prerequisites | 21 |
| 5.3 | Service Affecting | 21 |
| 5.4 | Detailed Procedure..... | 22 |
| 6 | Upgrading Standalone Mediant VE on VMware | 23 |
| 6.1 | Prerequisites | 23 |
| 6.2 | Service Affecting | 23 |
| 6.3 | Upgrade Summary | 23 |
| 6.4 | Rollback Procedure | 24 |
| 6.5 | Alternative Upgrade Procedure..... | 25 |
| 7 | Upgrading Standalone Mediant VE on KVM | 27 |
| 7.1 | Prerequisites | 27 |
| 7.2 | Service Affecting | 27 |
| 7.3 | Upgrade Procedure | 27 |
| 7.4 | Rollback Procedure | 28 |
| 7.5 | Alternative Upgrade Procedure..... | 29 |
| 8 | Upgrading Standalone Mediant VE on Hyper-V | 31 |
| 8.1 | Prerequisites | 31 |

| | | |
|-----------|--|----|
| 8.2 | Service Affecting | 31 |
| 8.3 | Upgrade Procedure | 31 |
| 8.4 | Rollback Procedure | 32 |
| 8.5 | Alternative Upgrade Procedure..... | 32 |
| 9 | Upgrading High-Availability (HA) Mediant VE on VMware, KVM or Hyper-V33 | |
| 9.1 | Prerequisites | 33 |
| 9.2 | Service Affecting | 33 |
| 9.3 | Upgrade Procedure | 34 |
| 9.4 | Rollback Procedure | 34 |
| 9.5 | Alternative Upgrade Procedure..... | 34 |
| 9.5.1 | Alternative Upgrade Procedure – Hitless Option..... | 35 |
| 9.5.2 | Alternative Upgrade Procedure – Non-Hitless Option..... | 42 |
| 10 | Upgrading Mediant CE on VMware, KVM or Hyper-V.....45 | |
| 10.1 | Prerequisites | 45 |
| 10.2 | Service Affecting | 45 |
| 10.3 | Upgrade Procedure | 46 |
| 10.4 | Rollback Procedure | 46 |
| 11 | Upgrading Mediant VE on Public Clouds (AWS / Azure / Google Cloud).....47 | |
| 12 | Upgrading Mediant CE on Public Clouds (AWS / Azure / Google Cloud).....49 | |

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: September-28-2023

09

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 |
|-------|--|
| 28724 | Initial document release. |
| 28725 | Software rollback procedure; restore HA Ethernet Group; upgrading Mediant CE on VMware, KVM or Hyper-V |
| 28726 | HA upgrade |
| 28727 | Supported software versions; hitless upgrade not supported note |
| 28728 | Intermediate version update |
| 28729 | Intermediate note removed |
| 28731 | HA status "Operational"; upgrade Mediant VE on KVM updated |
| 28736 | Rocky Linux 8 |
| 28737 | 7.20A.259.* added to supported 7.2 versions for upgrade |

Documentation Feedback

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

1 Introduction

This document provides step-by-step instructions on how to upgrade the following AudioCodes session border controllers (SBC) from Version 7.2 to Version 7.4:

- Mediant 9000/9030/9080
- Mediant Server Edition (SE)
- Mediant Virtual Edition (VE) deployed in VMware, Hyper-V and KVM environments
- Mediant Cloud Edition (CE) deployed in VMware, Hyper-V and KVM environments

Both standalone and high-availability (HA) deployment modes are covered in this document.



Note: Upgrade instructions for Mediant VE/CE deployed in public clouds (Azure, AWS, and Google Cloud) are provided in their corresponding Mediant VE/CE Installation Manuals.

Since 7.2 and 7.4 software versions are based on different operating systems (CentOS 6 and CentOS Stream 8 / Rocky Linux 8, respectively), such a software upgrade cannot be performed through the regular Software Upgrade Wizard using the CMP file. Instead, use the procedures described in this document to upgrade the device.

1.1 Supported Versions

Only the following 7.2 software versions can be upgraded to a 7.4 version:

- 7.20A.260.*
- 7.20A.259.*
- 7.20A.258.*
- 7.20A.256.*
- 7.20A.204.549
- 7.20A.204.878

This page is intentionally left blank.

2 Upgrading Standalone Mediant 9000/9030/9080/SE

This chapter describes the upgrade procedure for standalone Mediant 9000/9030/9080/SE.

2.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- ISO file of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8)
- Connection to the iLO server management interface (also referred to as "Remote Console")
- Connection to the Mediant 9000/9030/9080/SE Web interface



Note: The below instructions assume that your server's iLO server management interface provides Remote Console functionality. iLO interface on Mediant 9030/9080 servers includes this functionality. However, iLO interface on Mediant 9000 does not include it.

For Mediant 9000, or if you don't have a remote connection to the iLO server management interface, do the following:


1. Burn the ISO file of the latest 7.4 version to a physical DVD disk.
2. Use a physical VGA terminal and keyboard to perform the installation.

2.2 Service Affecting

Upgrading the device is service affecting. The upgrade process requires manual backup and restore of device configuration. The process takes approximately 30 minutes to complete.

2.3 Upgrade Procedure

➤ **To upgrade standalone Mediant 9000/9030/9080/SE:**

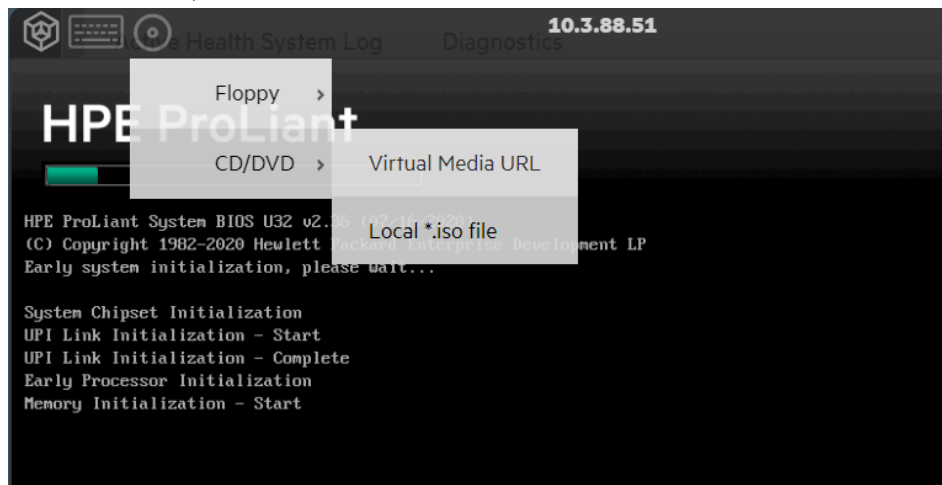
1. Back up configuration and the license key from the currently running software (7.2) so that you can restore them later if you rollback the device from Version 7.4 to 7.2:
 - a. Log in to the SBC's Web interface.
 - b. On the toolbar, click **Actions > Configuration File**, and then click **Save Configuration Package**.
 - c. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**, and then click the **Save License Key to File** icon .
2. Install the latest 7.4 software version from the ISO file using the iLO interface:



Note: If you are using a physical VGA terminal and keyboard, insert the DVD disk into the DVD-ROM drive, reboot the server by pressing **Power** button, and then continue with Step f.

- a. Connect to the iLO server management interface.

- b. Open the Remote Console.
- c. On the toolbar, choose **Virtual Media > CD/DVD > Local *.iso file:**



- d. Browse to the ISO file of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8).
- e. On the toolbar, choose **Menu > Power > Reset**; the server reboots and the Mediant SBC Installation menu is displayed.



- f. Type **upgrade**, and then press Enter to start installation.



Note: During installation from the ISO file / DVD disk, the hard drive is formatted. However, because you typed **upgrade**, the SBC configuration (INI file, auxiliary files and TLS certificates) and the license key will be preserved.

- g. Wait until installation is complete (approximately 10 minutes), and then disable the virtual CD/DVD drive that was selected before the installation.
 - h. Press ENTER to reboot the server.
3. Wait until the server starts. Verify that it is running the latest 7.4 software version, by connecting to its Web interface and checking the version on the MONITOR page. Verify that the SBC configuration is preserved.

2.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Install Version 7.2 from the ISO file or physical DVD disk.
2. Restore the configuration package and license key from the backup.
3. If needed, restore the customized device certificate and/or trusted root certificates.

This page is intentionally left blank.

3 Upgrading High-Availability (HA) Mediant 9000/9030/9080/SE via Hitless Procedure

This chapter describes the upgrade procedure for high-availability (HA) Mediant 9000/9030/9080/SE deployment, which consists of two units running as an active/standby pair.

The procedure is hitless, meaning that during the upgrade process, the SBC service is preserved. For a slightly quicker non-hitless procedure, see Upgrading High-Availability (HA) Mediant 9000/9030/9080/SE via Non-Hitless Procedure.

Hitless upgrade of a High-Availability (HA) Mediant 9000/9030/9080/SE deployment from the 7.2 to 7.4 stream should always be performed via the 7.40A.005.619 version. For example, if you currently have the 7.20A.258.* version installed and want to upgrade to the 7.40A.100.* version, you need to perform the upgrade in two steps:

- First upgrade from 7.20A.258.* to the 7.40A.005.619 version using the special upgrade procedure described below.
- Then upgrade from 7.40A.005.619 to the 7.40A.100.* version using the regular CMP upgrade method.



Note: The 7.40A.005.619 version lacks new features added in the 7.20A.260 stream. If you are currently running the 7.20A.260.* version, you will lose all 7.20A.260 stream specific features when you upgrade to the 7.40A.005.619 version. However, the features will be restored after you complete the upgrade to the 7.40A.100.* or later version.

3.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- ISO file of 7.40A.005.619 version (based on CentOS Stream 8)
- CMP of "intermediate" 7.40A.005.619 version - same version number as above, but based on CentOS 6
- CMP of the latest 7.4 version (e.g., 7.40A.100.*)
- Connection to the iLO server management interface (also referred to as "Remote Console") on both units
- Connection to the Mediant 9000/9030/9080/SE SSH and Web interfaces



Note: The below instructions assume that your server's iLO server management interface provides Remote Console functionality. iLO interface on Mediant 9030/9080 servers includes this functionality. However, the iLO interface on Mediant 9000 does not include it.

For Mediant 9000 product, or if you don't have a remote connection to iLO server management interface, do the following:

1. Burn the ISO file of the 7.40A.005.619 version to a physical DVD disk.
2. Use a physical VGA terminal and keyboard to perform the installation.

3.2 Service Affecting

Upgrading the device is not service affecting. Device configuration is preserved during the upgrade. The process takes approximately two hours to complete.

3.3 Upgrade Summary

The upgrade procedure consists of the following main steps:

1. Install the "intermediate" 7.40A.005.619 version (based on CentOS 6) on both units.
 - The upgrade is performed through the regular Software Upgrade Wizard using the CMP file.
 - Note that "intermediate" software version is intended for a temporary use during software upgrade only; it should not be used for a regular deployment in production.
2. Install the "final" 7.40A.005.619 software version, based on CentOS Stream 8, on the redundant unit from the ISO file, using the iLO interface. Installation is performed in **upgrade** mode, which preserves all existing configuration and the license key.
3. Perform an HA switchover.
4. Install the "final" 7.40A.005.619 software version, based on CentOS Stream 8, on the remaining (currently redundant) unit from the ISO file, using the iLO interface. Installation is also performed in **upgrade** mode.
5. Upgrade to the latest 7.4 version (e.g., 7.40A.100.*) using the regular CMP upgrade method.

3.3.1 Upgrading Device in a Media Transcoding Cluster

If the Mediant 9000/9030/9080/SE device is part of a Media Transcoding Cluster, perform the following steps *prior* to starting the upgrade:

1. Log in to the SBC's Web interface.
2. Navigate to **MONITOR > Device Information** page.
3. Check if **vMC Firmware File** is listed under **LOADED FILES**.
4. If the file is listed, delete it by clicking **Delete**.


Upgrade the Media Transcoding Cluster as follows:

1. Upgrade the Mediant 9000/9030/9080/SE device to the 7.40A.005.619 version. Make sure that the device is fully upgraded (to "final" 7.40A.005.619 version based on CentOS Stream 8) prior to proceeding to the next step.
2. Upgrade the Media Components to the 7.40A.005.619 version, as described in the 'Upgrading the Cluster Software Version' section in the [Mediant 9000 SBC Series User Manual](#).
3. Upgrade the Mediant 9000/9030/9080/SE device and Media Components to the latest 7.4 version (e.g., 7.40A.100.*) using the regular CMP upgrade method.

3.4 Upgrade Procedure

➤ **To upgrade HA Mediant 9000/9030/9080/SE via hitless procedure:**

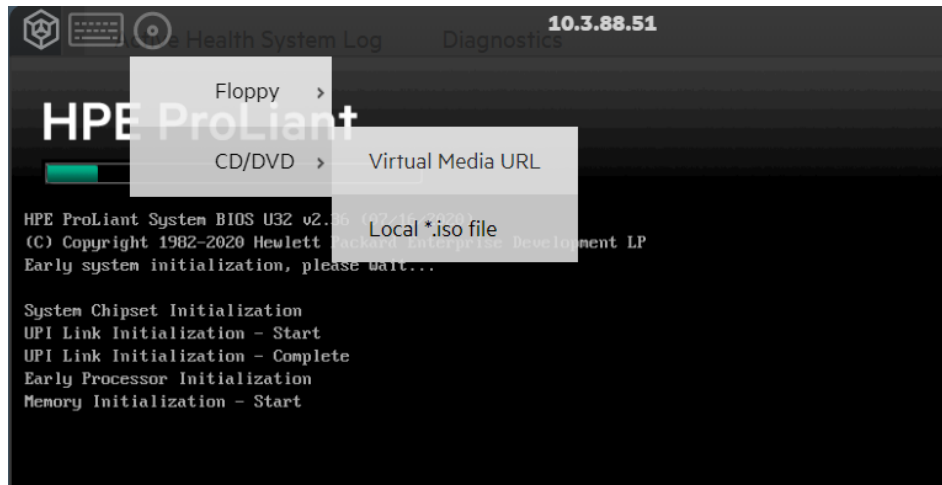
1. Back up configuration and the license key from the currently running software (7.2) so that you can restore them later if you rollback the device from Version 7.4 to 7.2:
 - a. Log in to the SBC's Web interface.

- b. On the toolbar, click **Actions > Configuration File**, and then click **Save Configuration Package**.
 - c. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**, and then click the **Save License Key to File** icon  .
2. Install the "intermediate" 7.40A.005.619 version (same baseline as the "final" 7.40A.005.619 version, but based on CentOS 6) through the regular Software Upgrade wizard. The upgrade is performed using the CMP file and installs the "intermediate" 7.40A.005.619 software on both units.
 3. Install the "final" 7.40A.005.619 version (based on CentOS Stream 8) on the redundant unit:



Note: If you are using a physical VGA terminal and keyboard, insert the DVD disk into the DVD-ROM drive, reboot the server by pressing the **Power** button, and then continue with Step f.

- a. Connect to the iLO server management interface of the redundant unit.
- b. Open the Remote Console.
- c. On the toolbar, choose **Virtual Media > CD/DVD > Local *.iso file**:



- d. Browse to the ISO file of the "final" 7.40A.005.619 version (based on CentOS Stream 8).
- e. On the toolbar, choose **Menu > Power > Reset**; the server reboots and the Mediant SBC Installation menu is displayed.



- f. Type **upgrade**, and then press Enter to start installation.



Note: During the installation from the ISO file / DVD disk, the hard drive is formatted. However, because you typed **upgrade**, the SBC configuration (INI file, auxiliary files and TLS certificates) and the license key will be preserved

- g. Wait until installation is complete (approximately 10 minutes), and then disable the virtual CD/DVD drive that was selected before the installation.
- h. Press ENTER to reboot the server.
- 4. Wait until the redundant unit completes the reboot and synchronizes with the active unit:
 - a. Log in to the SBC's Web interface.
 - b. Navigate to the **MONITOR** page.
 - c. Wait until both units are displayed and the HA status is "Operational".
- 5. Make the redundant unit (that has "final" 7.40A.005.619 software version) active:
 - a. On the **MONITOR** page, check which unit is active.
 - b. If the first unit (that wasn't upgraded to "final" 7.40A.005.619 version yet) is active, perform a switchover, by clicking **Actions > Switch Over** on the toolbar.
- 6. Repeat steps 3-4 on the remaining unit (which is currently the redundant unit).
- 7. Upgrade to the latest 7.4 version (e.g., 7.40A.100.*) via the regular **Software Upgrade Wizard**, using the corresponding CMP file.

3.5 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Install Version 7.2 from the ISO file or physical DVD disk, on both units.
2. Restore the HA network setting on both units and make sure that they are properly connected and operate as an HA pair.
3. Restore the configuration package and license key from the backup.
4. If needed, restore the customized device certificate and/or trusted root certificates.

4 Upgrading High-Availability (HA) Mediant 9000/9030/9080/SE via Non-Hitless Procedure

This chapter describes the upgrade procedure for high-availability (HA) Mediant 9000/9030/9080/SE deployment, which consists of two units running as an active/standby pair.

The procedure is non-hitless, meaning that during the upgrade, the SBC service is **not available**. Compared to the hitless procedure, described in the previous section, this procedure is slightly quicker and requires less configuration steps.

4.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- ISO file of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8)
- Connection to the iLO server management interface (also referred to as "Remote Console") on both units
- Connection to the Mediant 9000/9030/9080/SE Web interface



Note: The below instructions assume that your server's iLO server management interface provides Remote Console functionality. The iLO interface on Mediant 9030/9080 servers includes this functionality. However, the iLO interface on Mediant 9000 does not include it.

For Mediant 9000, or if you don't have a remote connection to iLO server management interface, do the following:


1. Burn the ISO file of the latest 7.4 version to a physical DVD disk.
2. Use a physical VGA terminal and keyboard to perform the installation.

4.2 Service Affecting

Upgrading the device is service affecting. The upgrade process requires manual backup and restore of device configuration. The process takes approximately one hour to complete.

4.3 Upgrade Procedure

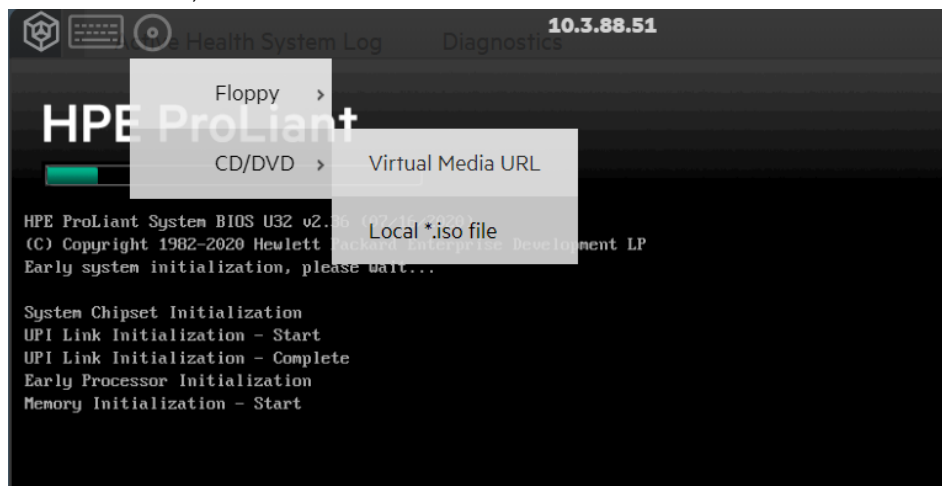
- **To upgrade HA Mediant 9000/9030/9080/SE via non-hitless procedure:**

 1. Back up configuration and the license key from the currently running software (7.2) so that you can restore them later if you rollback device from Version 7.4 to 7.2:
 - a. Log in to the SBC's Web interface.
 - b. On the toolbar, click **Actions > Configuration File**, and then click **Save Configuration Package**.
 - c. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**, and then click the **Save License Key to File** icon  .
 2. Install the latest 7.4 software version on the redundant unit:



Note: If you are using a physical VGA terminal and keyboard, insert the DVD disk into the DVD-ROM drive, reboot the server by pressing **Power** button, and then continue with Step f.

- a. Connect to the iLO server management interface.
- b. Open the Remote Console.
- c. On the toolbar, choose **Media > CD/DVD > Local *.iso file**:



- d. Browse to the ISO file of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8).

- e. On the toolbar, choose **Menu > Power > Reset**; the server reboots and the Mediant SBC Installation menu is displayed.

```

Mediant SBC
-----
Mediant SBC
ver 7.40A.005.314
-----
- To start installation, press <ENTER> key.
- To start installation from RS-232 serial console, type rs232 <ENTER>.
- To boot from local disk, type local <ENTER>.
boot: upgrade
    
```

- f. Type **upgrade**, and then press Enter to start installation.



Note: During installation from the ISO file / DVD disk, the hard drive is formatted. However, because you typed **upgrade**, the SBC configuration (INI file, auxiliary files and TLS certificates) and the license key will be preserved.

- g. Wait until installation is complete (approximately 10 minutes), and then disable the virtual CD/DVD drive that was selected before the installation.
- h. Power off the active unit.
- i. Press Enter to reboot the redundant unit.



Note: It is imperative to power off the active unit prior to rebooting the redundant unit, because it still has the 7.2 software version installed.

3. Wait until the redundant unit starts. Verify that it is running the latest 7.4 software version, by connecting to its Web interface and checking the version on the MONITOR page. Verify that the SBC configuration is preserved.
4. Repeat Step 2 on the remaining unit (which is currently powered off). When the installation completes, do not power off the active unit because it's already running the latest 7.4 software version.
5. Wait until both units become synchronized:
 - a. Log in to the SBC's Web interface.
 - b. Navigate to the **MONITOR** page.
 - c. Wait until both units are displayed and the HA status displays "Operational".

4.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Install Version 7.2 from the ISO file or physical DVD disk, on both units.
2. Restore the HA network setting on both units and make sure that they are properly connected and operate as an HA pair.
3. Restore the configuration package and license key from the backup.
4. If needed, restore the customized device certificate and/or trusted root certificates.

5 Upgrading via Side-By-Side Deployment on VMware, KVM or Hyper-V

This chapter describes the procedure for upgrading from Version 7.2 to 7.4, Mediant VE deployed on VMware, KVM or Hyper-V, via side-by-side deployment of the 7.4 version along the existing 7.2 version.

5.1 Process Overview

The process consists of the following steps:

1. Deploy a new Mediant VE instance from the latest 7.4 version image (OVF / QCOW2 / VHD).
2. Switch live traffic from the old Mediant VE instance to the new one.
3. Delete the old Mediant VE instance when it's no longer needed.

Compared to the in-place upgrade process described in subsequent sections (6, 7, 8 and 9), the side-by-side process has the following advantages and disadvantages:

- Advantages:
 - If any problems are experienced with the new 7.4 version, software roll-back to the old 7.2 version is quick and simple.
 - Traffic may be gradually moved to a new instance (assuming that VoIP equipment that sent the traffic to the SBC supports such functionality), thereby providing better control over the upgrade process.
- Disadvantages:
 - Requires the use of additional virtual machines for the duration of the upgrade.
 - Requires a change of the IP addresses and therefore, requires reconfiguration of VoIP equipment that communicates with the SBC.

5.2 Prerequisites

Prior to implementing the procedure, make sure the following prerequisites are met:

- Image file of the latest 7.4 version for specific virtual environment – OVF / QCOW2 / VHD
- Connection to the virtual environment's management interface
- Credentials on virtual environment that allow creation of new virtual machines
- Connection to the Mediant VE Web interface

5.3 Service Affecting

The process is not service affecting. However, SBC IP addresses are changed and therefore, VoIP equipment that communicates with the SBC must be updated accordingly. The process takes approximately one hour to complete.

5.4 Detailed Procedure

- To upgrade Mediant VE on VMware, KVM or Hyper-V from 7.2 to 7.4 version via side-by-side installation:
1. Deploy a new Mediant VE instance from the latest 7.4 version image. Refer to Mediant Virtual Edition (VE) Installation Manual for detailed instructions.
 2. Download the configuration file (.ini) from the existing Mediant VE instance (**Actions > Configuration File > Save INI File**).
 3. Remove all networking configuration from the downloaded file, using one of the following methods:
 - Using ini_cleanup.py script from the *Mediant VE Installation Kit*, which is available on www.audiocodes.com portal.

```
# python ini_cleanup.py old.ini new.ini
```
 - Manually: Open the file in a text editor (e.g. Notepad++), and then delete the following elements:
 - ◆ Configuration tables: PhysicalPortsTable, EtherGroupTable, DeviceTable, InterfaceTable, MtcEntities
 - ◆ Configuration parameters: HARemoteAddress, HAUnitldName, HARemoteUnitldName, HAPriority, HARemotePriority, HALocalMAC, HARemoteMAC
 4. Obtain, activate and apply the license to the new Mediant VE instance. Refer to section Licensing the Product in Mediant Virtual Edition (VE) SBC Installation Manual for detailed description.
 5. Switch live traffic from the old Mediant VE instance to the new one. This typically requires a change in the SBC's IP address in the VoIP equipment that communicates with the SBC. Consider performing gradual traffic migration if your VoIP equipment supports it. For example, first switch 10% of your live traffic to the new Mediant VE instance, verify that it is processed as expected, and only then switch the rest of the traffic.
 6. After all live traffic is switched to the new Mediant VE instance and service operates normally, delete the old Mediant VE instance.

6 Upgrading Standalone Mediant VE on VMware

This chapter describes the upgrade procedure for standalone Mediant VE on VMware.

6.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- "OVF archive" of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8)
- Connection to the VMware Web interface (vSphere or vCenter)
- Connection to the VMware host through SSH interface
- VMware credentials that allow creation and modification of virtual resources as described in the upgrade procedure below
- At least 40 GB of storage space available in the VMware datastore
- Connection to the Mediant VE Web interface

6.2 Service Affecting

Upgrading the device is service affecting. Device configuration is preserved during the upgrade. The process takes approximately 30 minutes to complete.

6.3 Upgrade Summary

The recommended upgrade procedure described below includes the following steps:

1. Create a new virtual disk with the latest 7.4 software from the "OVF archive".
2. Stop the virtual machine.
3. Mount the new virtual disk (with 7.4 version) as the primary disk and the old disk (with 7.2 version) as the secondary disk.
4. Start the virtual machine; the new SBC software automatically copies all existing configuration and the license key from the secondary disk.
5. Detach the secondary disk.

➤ **To upgrade Mediant VE on VMware:**

1. Enable SSH access to the VMware host:
 - a. Log in to the VMware Web interface. The instructions below use vSphere UI, but you may perform similar operations using vCenter UI instead.
 - b. Navigate to **Host > Actions > Services**, and then turn on **Enable Secure Shell (SSH)**.
2. Upload the disk image (VMDK) of the latest 7.4 version to the VMware datastore:
 - a. Extract the VMDK file from the latest 7.4 version "OVF archive".
 - b. Log in to the VMware Web interface. The instructions below use vSphere UI, but you may perform similar operations using vCenter UI instead.
 - c. Open the Datastore browser (**Storage > datastore1 > Datastore browser**).
 - d. Create a directory where the 7.4 image (VMDK) will be stored (e.g., "images").
 - e. Upload the extracted VMDK file to the created directory.

3. Create a copy of the 7.4 disk image (VMDK) file for the specific virtual machine and convert it into native ESXi format:
 - a. Connect to the VMware host via SSH interface.
 - b. Run the following commands:

```
cd /vmfs/volumes/datastore1/<vm-name>/  
vmkfstools -i ../images/<image-name>.vmdk new-disk.vmdk
```
4. Stop the VM (**Virtual Machines > VM > Actions > Shut down**).
5. Attach a new disk to the VM as the primary disk, keeping the old one as secondary:
 - a. Open the VM settings (**Virtual Machines > VM > Actions > Edit settings**).
 - b. Add the new disk to the VM:
 1. Click **Add hard disk > Existing hard disk**.
 2. Navigate to the VM folder, and select the `new-disk.vmdk` file created in the previous step.
 - c. Swap hard disks so that the new hard disk becomes the primary disk and the old hard disk becomes secondary:
 1. Open "New Hard disk" settings, and then change 'Virtual Device node' from **SCSI (0:1)** to **SCSI (0:0)**.
 2. Open (old) "Hard disk 1" settings, and then change 'Virtual Device node' from **SCSI (0:0)** to **SCSI (0:1)**.
 - d. Under VM Options, change 'General Options' > 'Guest OS Version' to **CentOS 8 (64-bit)**. If such an option is unavailable, choose **CentOS 7 (64-bit)** instead.
 - e. Click **Save** to apply the changes.
6. Start the VM (**Virtual Machines > VM > Actions > Power on**).
7. Wait until the VM completes the boot and displays the CLI prompt. During this process, VM copies all configuration and the license key from the secondary disk.
8. Verify that the VM is running the latest 7.4 software version, by connecting to its Web interface and checking the version on **MONITOR** page. Verify that SBC configuration is preserved.
9. Stop the VM (**Virtual Machines > VM > Actions > Shut down**).
10. Remove the secondary disk:
 - a. Navigate to **Virtual Machines > VM > Actions > Edit settings**.
 - b. Locate the hard disk that is connected as "SCSI (0:1)" (typically, it is named "Hard disk 2"), and then delete it.
 - c. Click **Save** to apply the changes.
11. Start the VM (**Virtual Machines > VM > Actions > Power on**).



Note: It's recommended to keep the old disk in case you need to rollback to the old software version (for whatever reason).

6.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Stop the VM.
2. Detach the new disk (with Version 7.4) and attach the old disk (with Version 7.2).
3. Start the VM.

6.5 Alternative Upgrade Procedure

Some VMware deployments may lack the ability to attach a secondary hard disk and/or swap the virtual machine's primary hard disk. This may happen, for example, if you are using some "private cloud" solution on top of VMware that doesn't support virtual machine configuration via standard vSphere / vCenter interface.

If, for whatever reason, the above-described recommended procedure cannot be implemented, use the following alternative procedure instead:

1. Back up the device configuration, by downloading the configuration package from it.
2. Check if some customization was done for the device certificate and/or trusted root certificates.

The default device configuration is as follows:

- Device certificate has a Common Name that starts with "**ACL_**" and is self-signed.
- Trusted Root Certificates list is empty.

If the device certificate was customized or some certificates were added to the Trusted Root list, make sure that you have the means to restore them (e.g., generate a new device certificate) as they are deleted during the upgrade.

3. Delete the current virtual machine, and then create a new one from the latest 7.4 version "OVF archive". Alternatively, you may keep the current virtual machine shut down because you will be using the same network IP addresses on the new virtual machine.
4. Configure the new virtual machine to use the same network IP address as the old one.
5. Obtain and activate the license for the new virtual machine.
6. Restore the configuration package from the backup.
7. If your device is connected to OVOC, enable the SNMP protocol, by setting the **Disable SNMP** parameter to **No** (parameter's default value was changed in 7.4 version).
8. If your device had the Telnet server enabled prior to the upgrade and you want to keep it enabled, configure the **Embedded Telnet Server** parameter (parameter's default value was changed in 7.4 version).
9. Restore the device certificate and/or trusted certificates if needed.

This page is intentionally left blank.

7 Upgrading Standalone Mediant VE on KVM

This chapter describes the upgrade procedure for standalone Mediant VE on KVM.

7.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- QCOW2 image of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8)
- Connection to the KVM host via SSH interface
- KVM credentials that allow creation and modification of virtual resources, as described in the upgrade procedure below
- At least 40 GB of storage space available on the KVM host
- Connection to the Mediant VE Web interface

7.2 Service Affecting

Upgrading the device is service affecting. Device configuration is preserved during the upgrade. The process takes approximately 30 minutes to complete.

7.3 Upgrade Procedure

The recommended upgrade procedure described below includes the following steps:

1. Create a new virtual disk with the latest 7.4 software from the QCOW2 image.
2. Stop the virtual machine.
3. Mount the new virtual disk (with 7.4 version) as the primary disk and the old disk (with 7.2 version) as the secondary disk.
4. Start the virtual machine; the new SBC software automatically copies all existing configuration and the license key from the secondary disk.
5. Detach the secondary disk.

➤ To upgrade Mediant VE on KVM:

1. Upload the latest 7.4 QCOW2 image to the KVM host:
 - a. Connect to the KVM host from the SCP/SFTP client (e.g., WinSCP).
 - b. Upload the QCOW2 image file. The correct QCOW2 image extension is **.qcow2**. If you received a ZIP file, extract the QCOW2 file from it prior to uploading it.
2. Create a copy of the 7.4 QCOW2 image for the specific virtual machine:
 - a. Connect to the KVM host via the SSH interface.
 - b. Run the following commands:

```
DIR=/var/lib/libvirt/images
sudo cp <image>.qcow2 $DIR/<vm-name>-disk.qcow2
```

3. Stop the VM:

```
sudo virsh shutdown <vm-name>
```

4. Attach the new disk to the VM as the primary disk, keeping the old one as secondary:
 - a. Attach the new disk to the VM:

```
sudo virsh attach-disk <vm-name> \  
$DIR/<vm-name>-disk.qcow2 hdb --config --subformat qcow2
```
 - b. Open the VM settings editor:

```
virsh edit <vm-name>
```
 - c. Change the target device names for <disk> elements:
 - ◆ For the new disk, set the target device name to `hda`.
 - ◆ For the old disk, set the target device name to `hdb`.
5. Start the VM:

```
sudo virsh start <vm-name>
```
6. Wait until the VM completes the boot and displays the CLI prompt. During this process, VM copies configuration and the license key from the secondary disk.
7. Verify that the VM is running the latest 7.4 software version, by connecting to its Web interface and checking the version on the **MONITOR** page. Verify that SBC configuration is preserved.
8. Detach the secondary disk:

```
sudo virsh shutdown <vm-name>  
sudo virsh detach-disk <vm-name> hdb --config  
sudo virsh start <vm-name>
```



Note: It's recommended to keep the old disk in case you need to rollback to the old software version (for whatever reason).

7.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Stop the VM.
2. Detach the new disk (with Version 7.4) and attach the old disk (with Version 7.2).
3. Start the VM.

7.5 Alternative Upgrade Procedure

Some KVM deployments may lack the ability to attach a secondary disk and/or swap the virtual machine's primary disk. This may happen, for example, if you are using some "private cloud" solution on top of KVM (e.g., OpenStack that doesn't support virtual machine configuration via the **virsh** command).

If, for whatever reason, the above-described recommended procedure cannot be implemented, use the following alternative procedure instead:

1. Back up device configuration, by downloading the configuration package from it.
2. Check if some customization was done for device certificate and/or trusted root certificates:

Default device configuration is as follows:

- Device certificate has a Common Name that starts with "**ACL_**" and is self-signed.
- Trusted Root Certificates list is empty.

If the device certificate was customized or some certificates were added to the Trusted Root list, make sure that you have the means to restore them (e.g., generate a new device certificate) as they are deleted during the upgrade.

3. Delete the current virtual machine, and then create a new one from the QCOW2 image. Alternatively, you may keep the current virtual machine shut down because you will be using the same network IP addresses on the new virtual machine.
4. Configure the new virtual machine to use the same network IP address as the old one.
5. Obtain and activate the license for the new virtual machine.
6. Restore the configuration package from the backup.
7. If your device is connected to OVOC, enable the SNMP protocol by setting the **Disable SNMP** parameter to **No** (parameter's default value was changed in 7.4 version).
8. If your device had the Telnet server enabled prior to the upgrade and you want to keep it enabled, configure the **Embedded Telnet Server** parameter (parameter's default value was changed in 7.4 version).
9. Restore the device certificate and/or trusted root certificates, if needed.

This page is intentionally left blank.

8 Upgrading Standalone Mediant VE on Hyper-V

This chapter describes the upgrade procedure for standalone Mediant VE on Hyper-V.

8.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- VHD image of the latest 7.4 version (based on CentOS Stream 8 / Rocky Linux 8)
- Connection to the Hyper-V host
- Hyper-V credentials that allow creation and modification of virtual resources, as described in the upgrade procedure below
- At least 20 GB of storage space available on the Hyper-V host
- Connection to the Mediant VE Web interface

8.2 Service Affecting

Upgrading the device is service affecting. Device configuration is preserved during the upgrade. The process takes approximately 30 minutes to complete.

8.3 Upgrade Procedure

The recommended upgrade procedure described below includes the following steps:

1. Create a new virtual disk with the latest 7.4 software from the VHD image.
2. Stop the virtual machine.
3. Mount the new virtual disk (with 7.4 version) as the primary disk and the old disk (with 7.2 version) as the secondary disk.
4. Start the virtual machine; the new SBC software automatically copies all existing configuration and the license key from the secondary disk.
5. Detach the secondary disk.

➤ **To upgrade Mediant VE on Hyper-V:**

1. Copy the latest 7.4 VHD image to the Hyper-V host. Place it in the same folder where the existing VM disk is located (e.g., C:\Hyper-V\Virtual Hard Disks). Provide a unique name for the copied image (e.g., <vm-name>-disk.vhdx).
2. Stop the VM (**VM > Actions > Shut down**).
3. Open VM Settings (**VM > Actions > Settings**).
4. Under **IDE Controller 0**, add a new hard drive, click **Browse**, choose the copied image, and then click **Apply**.
5. Make the new hard drive the primary one, by setting its **Location** to **0**.
6. Make the old hard drive the secondary one, by setting its **Location** to **1**.
7. Click **Apply** to apply the changes.
8. Start the VM (**VM > Actions > Start**).
9. Wait until the VM completes the boot and displays the CLI prompt. During this process, VM copies configuration and the license key from the secondary disk.

10. Verify that the VM is running the latest 7.4 software version, by connecting to its Web interface and checking the version on the **MONITOR** page. Verify that SBC configuration is preserved.
11. Stop the VM (**VM > Actions > Shut down**).
12. Remove the old hard drive.
13. Start the VM (**VM > Actions > Start**).



Note: It's recommended to keep the old hard drive in case you need to rollback to the old software version (for whatever reason).

8.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Stop the VM.
2. Detach the new hard drive (with Version 7.4) and attach the old hard drive (with Version 7.2).
3. Start the VM.

8.5 Alternative Upgrade Procedure

Some Hyper-V deployments may lack the ability to attach a secondary disk and/or swap the virtual machine's primary disk. This may happen, for example, if you are using some "private cloud" solution on top of Hyper-V that doesn't support virtual machine configuration via standard Hyper-V management interface.

If, for whatever reason, the above-described recommended procedure cannot be implemented, use the following alternative procedure instead:

1. Back up device configuration, by downloading the configuration package from it.
2. Check if some customization was done for the device certificate and/or trusted root certificates:

Default device configuration is as follows:

- Device certificate has a Common Name that starts with "**ACL_**" and is self-signed.
- Trusted Root Certificates list is empty.

If the device certificate was customized or some certificates were added to the Trusted Root list, make sure that you have the means to restore them (e.g., generate a new device certificate) as they are deleted during the upgrade.

3. Delete the current virtual machine, and then create a new one from the latest 7.4 VHD image. Alternatively, you may keep the current virtual machine shut down because you will be using the same network IP addresses on the new virtual machine.
4. Configure the new virtual machine to use the same network IP address as the old one.
5. Obtain and activate the license for the new virtual machine.
6. Restore the configuration package from the backup.
7. If your device is connected to OVOC, enable the SNMP protocol by setting the **Disable SNMP** parameter to **No** (parameter's default value was changed in 7.4 version).
8. If your device had Telnet server enabled prior to the upgrade and you want to keep it enabled, configure the **Embedded Telnet Server** parameter (parameter's default value was changed in 7.4 version).
9. Restore the device certificate and/or trusted root certificates if needed.

9 Upgrading High-Availability (HA) Mediant VE on VMware, KVM or Hyper-V

This chapter describes the upgrade procedure for high-availability (HA) Mediant VE deployment on VMware, KVM or Hyper-V, which consists of two virtual machines running in an active/standby pair.

Hitless upgrade of a High-Availability (HA) Mediant VE deployment from 7.2 to 7.4 stream should always be performed via the 7.40A.005.619 version. For example, if you currently have the 7.20A.258.* version installed and want to upgrade to the 7.40A.100.* version, you need to perform the upgrade in two steps:

- First upgrade from 7.20A.258.* to the 7.40A.005.619 version using the special upgrade procedure described below.
- Then upgrade from 7.40A.005.619 to the 7.40A.100.* version via the regular CMP upgrade method.



Note: The 7.40A.005.619 version lacks new features added in the 7.20A.260 stream. If you are currently running the 7.20A.260.* version, you will lose all 7.20A.260 stream specific features when you upgrade to the 7.40A.005.619 version. However, the features will be restored after you complete the upgrade to the 7.40A.100.* version or later.

9.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- Image file of 7.40A.005.619 version (based on CentOS Stream 8) for specific virtual environment – OVF / QCOW2 / VHD
- CMP of "intermediate" 7.40A.005.619 version - same version number as above, but based on CentOS 6
- CMP of the latest 7.4 version (e.g., 7.40A.100.*)
- Connection to the virtual host's management interface
- Connection to the Mediant VE Web interface

9.2 Service Affecting

Upgrading the device is not service affecting. Device configuration is preserved during the upgrade. The process takes approximately 1 hour to complete.

9.3 Upgrade Procedure

The recommended upgrade procedure described in this section is built upon the recommended upgrade procedure for standalone Mediant VE on VMware, KVM or Hyper-V environments, described in the corresponding sections above.

This recommended procedure preserves complete SBC configuration and the license key of the upgraded Mediant VE instance, which greatly simplifies upgrade of the high-availability (HA) deployment. If you are unable to upgrade your Mediant VE instances via the recommended procedure, refer to the alternative upgrade procedure described in Alternative Upgrade Procedure.

➤ To upgrade HA Mediant VE on VMware, KVM or Hyper-V:

1. Install the "intermediate" 7.40A.005.619 version (same baseline as "final" 7.40A.005.619 version, but based on CentOS 6) via the regular Software Upgrade wizard.
2. Install the "final" 7.40A.005.619 version (based on CentOS Stream 8) on the redundant unit. Use the recommended upgrade procedure as described in the sections above for standalone Mediant VE deployment in your environment.
3. Wait until the redundant unit properly connects to the active one:
 - a. Log in to the SBC's Web interface.
 - b. Open the MONITOR page and verify that both units are displayed and the HA status is "Operational".
4. Make the redundant unit (which has the "final" 7.40A.005.619 software version) active:
 - a. Log in to the SBC's Web interface.
 - b. Open the MONITOR page.
 - c. Check which unit is active. If the first unit (that wasn't upgraded to "final" 7.40A.005.619 version yet) is active, perform a switchover by clicking **Actions > Switch Over** on the toolbar.
5. Repeat Steps 2-3 on the remaining unit (which is currently redundant).
6. Upgrade to the latest 7.4 version (e.g., 7.40A.100.*) via the regular **Software Upgrade Wizard**, using the corresponding CMP file.

9.4 Rollback Procedure

If you need to rollback software from Version 7.4 to 7.2, do the following:

1. Stop both VMs.
2. Detach the new disk (with Version 7.4) and attach the old disk (with "intermediate" 7.40A.005.619 version).
3. Start the VMs.
4. Install Version 7.2 via the regular Software Upgrade Wizard, using the corresponding CMP file.

9.5 Alternative Upgrade Procedure

This chapter describes the alternative upgrade procedure for high-availability (HA) deployment of Mediant VE on VMware, KVM or Hyper-V environments. This procedure is relevant **only** when you cannot upgrade Mediant VE instances via the recommended upgrade procedure, as described in the previous section. This may happen, for example, if you are using some "private cloud" solution on top of VMware, KVM or Hyper-V environments (e.g., OpenStack that doesn't support swapping of virtual machine's primary disk).

The procedure is built upon the alternative upgrade procedure for standalone Mediant VE on VMware, KVM or Hyper-V environments, described in the corresponding sections above.


This procedure doesn't preserve configuration and the license key of the upgraded Mediant VE instance and therefore, is more complicated and takes longer to complete than the recommended procedure.

You have two options for implementing the alternative upgrade procedure:

- **Hitless upgrade:** This option preserves SBC service during the upgrade, but takes longer and is more complicated.
- **Non-hitless upgrade:** With this option SBC service is down during the upgrade. However, the procedure is faster and simpler to implement.

9.5.1 Alternative Upgrade Procedure – Hitless Option

➤ **To upgrade HA Mediant VE on VMware, KVM or Hyper-V via alternative upgrade procedure while preserving SBC service:**

1. Ensure that SSH server is enabled in SBC configuration:
 - a. Log in to the SBC's Web interface.
 - b. Navigate to **SETUP > ADMINISTRATION > WEB & CLI > CLI Settings**.
 - c. Ensure that the **Enable SSH Server** parameter value is set to **Enable**.
2. Install the "intermediate" 7.40A.005.619 version (same baseline as the "final" 7.40A.005.619 version, but based on CentOS 6) through the regular Software Upgrade wizard. The upgrade is performed using the CMP file and installs the "intermediate" 7.40A.005.619 software on both units.
3. Back up the current license key of both units:
 - a. Log in to the SBC's Web interface.
 - b. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**, click **Save License Key to File** icon  , and then save the downloaded file.
4. Enable SSH connection to the redundant unit:
 - a. Log in to the SBC's CLI interface via SSH protocol.

```
putty.exe <sbci_ip> -l <username> -pw <password>
```
 - b. Enable SSH proxy to redundant unit, by configuring some port for it (e.g., 1022):

```
configure system
  cli-settings
    ssh-red-device-port 1022
  exit
```



Note: Your SSH session may stop responding after running the **exit** command. If this happens, close the current SSH session and proceed to the next step.

5. Connect to the CLI interface of the redundant unit via SSH proxy on the active unit:
 - a. Establish a new SSH connection to the SSH proxy port configured above:

```
putty.exe <sbci_ip> -P 1022 -l <username> -pw <password>
```
 - b. Use the following command to check that you are logged into the redundant unit:

```
show high-availability status
```

The output should contain "Unit HA state is: Redundant".
6. Back up HA configuration on the redundant unit.
 - a. Capture configuration of the HA network interface:
 - i. Run the following command:

```
show running-config | between network-if exit
```

The command outputs a list of all network interfaces and their configuration, for example:

```
interface network-if 0
  ip-address 10.3.88.52
  prefix-length 16
  gateway 10.3.0.1
  name "O+M+C"
  underlying-dev "vlan 1"
  exit

interface network-if 1
  application-type maintenance
  ip-address 10.44.88.52
  prefix-length 16
  name "ha"
  underlying-dev "ha"
  exit
```

- ii. Identify the network interface with `application-type maintenance` and copy/paste its configuration to a local file on your PC for future use.

b. Capture configuration of the HA network device:

- i. Run the following command:

```
show running-config | between network-dev exit
```

The command outputs a list of all network devices and their configuration, for example:

```
network-dev 0
  underlying-if "GROUP_1"
  name "vlan 1"
  tagging untagged
  exit

network-dev 1
  vlan-id 4
  underlying-if "GROUP_4"
  name "ha"
  tagging untagged
  exit
```

- ii. Identify the network device whose name matches the `underlying-dev` name of the HA network interface and copy/paste its configuration to a local file on your PC for future use.

c. Capture configuration of the HA Ethernet Group:

- i. Run the following command:

```
show network ether-group
```

The command outputs a list of Ethernet groups, for example:

| G. Num | Group Name | Mode | State |
|--------|------------|----------------------|-------|
| 0 | GROUP_1 | GROUP_TYPE_SINGLE/1 | Up |
| 1 | GROUP_2 | GROUP_TYPE_SINGLE/1 | Up |
| 2 | GROUP_3 | GROUP_TYPE_NON/0 | Up |
| 3 | GROUP_4 | GROUP_TYPE_2RX_1TX/3 | Up |

- ii. Identify the Ethernet Group by name that matches the `underlying-if` name of the HA network device. This is the HA Ethernet Group. Its index is displayed in the first column (`G. Num`).

- iii. Run the following command:

```
show running-config | between ether-group exit
```

The command outputs a list of all Ethernet Groups and their configuration, for example:

```
ether-group 0
  mode single
  member1 "GE_1"
  exit
ether-group 1
  mode single
  member1 "GE_2"
  exit
ether-group 2
  exit
ether-group 3
  mode 2rx-1tx
  member1 "GE_3"
  member2 "GE_4"
  exit
```

- iv. Identify the HA Ethernet Group by its index, and then copy-paste its configuration to a local file on your PC for future use.

- d. Capture generic HA settings:

- i. Run the following command:

```
show running-config | between high-availability exit
```

The command outputs a list of HA parameters, for example:

```
high-availability settings
  unit-id-name "Device 2"
  remote-address 10.44.88.54
  redundant-unit-id-name "Device 1"
  exit
```

- ii. Copy/paste configuration of the following parameters: `remote-address`, `unit-id-name` and `priority` (if present) to a local file on your PC for future use.

7. Delete the existing virtual machine that corresponds to the redundant unit and create a new virtual machine from the 7.40A.005.619 image file (that contains the "final" 7.40A.005.619 version based on CentOS Stream 8). Provision a new virtual machine in the same way as the old one (use the same number of vCPUs / RAM, connect to the same virtual networks, use the same IP addresses, etc.).



Notes:

- The size of the 7.2 version image (based on CentOS 6) is 10 GB. The size of the 7.4 version image (based on CentOS Stream 8 / Rocky Linux 8) is 20 GB. Therefore, virtual disk size changes after the virtual machine rebuild.
- Instead of deleting the existing virtual machine, you may stop it and postpone deletion until after the upgrade is finished. However, keep in mind that the new virtual machine will be provisioned with the same IP addresses as the old one; therefore, you can't have both old and new virtual machines running at the same time.

8. Configure the redundant unit so that it's CLI interface can be accessed from the active unit:

- a. Connect to the redundant unit's CLI interface via the virtual console provided by you virtual environment.
- b. Wait until the server reboots and the Mediant SBC command line interface (CLI) login prompt is displayed, and then log in using the following default credentials:

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

c. Enter the configuration mode

```
enable
Admin
```

d. Change the application type of the default network interface to **media**:

```
configure network
interface network-if 0
application-type media
exit
exit
```

e. If **vlan-id** of the HA network device (captured in Step 6) equals 1, change the **vlan-id** of the default network device to **2**:

```
configure network
network-dev 0
vlan-id 2
exit
exit
```

f. Restore the HA network device and interface configuration, but make the following changes:

- ◆ If the HA network interface's ID is 0 (zero), change it to 1.
- ◆ Change the HA interface's **application-type** to **oamp** instead of **maintenance**.



Notes:

- The below commands are used as an example; use the data captured in Step 6 instead. **DO NOT** restore generic HA settings (e.g., `remote-address`) at this stage.
- Since virtual consoles typically lack copy/paste capabilities, you need to manually type the commands. Use CLI auto-completion capabilities (via Tab or '?' character) while typing the commands.

```

configure network
  network-dev 1
    vlan-id 4
    underlying-if "GROUP_4"
    name "ha"
    tagging untagged
    exit
  interface network-if 1
    application-type oamp
    ip-address 10.44.88.52
    prefix-length 16
    name "ha"
    underlying-dev "ha"
    exit
  exit

```

g. Restore the HA Ethernet group configuration:

i. Run the following command:

```
show network ether-group
```

The command outputs a list of Ethernet groups, for example:

| G. Num | Group Name | ... | Group Members |
|--------|------------|-----|---------------|
| 0 | GROUP_1 | ... | GE_1 , |
| 1 | GROUP_2 | ... | GE_2 , |
| 2 | GROUP_3 | ... | GE_3 , |
| 3 | GROUP_4 | ... | GE_4 , |

ii. Identify groups to which HA Ethernet ports (listed as `member1 / member2` in HA Ethernet group configuration captured in Step 6) are currently attached.

iii. If HA Ethernet ports are not attached to the correct groups:

- Detach the HA Ethernet ports from their current groups; for example:

```

configure network
  ether-group 2
    member1 ""
    exit
  ether-group 3
    member1 ""
    exit
  exit

```

- Restore HA Ethernet group configuration; for example:

```

configure network
  ether-group 3
    mode 2rx-1tx
    member1 "GE_3"
    member2 "GE_4"
    exit
  exit

```

- h. Reboot the redundant unit:

```
reload now
```
- i. Wait until the redundant unit completes the reboot and displays the CLI login prompt.

9. Configure License Key on the redundant unit:

- a. Connect to the CLI interface of the redundant unit via SSH proxy on the active unit:

```
putty.exe <sbci_ip> -P 1022 -l <username> -pw <password>
```



Notes:

- The above command uses port 1022 configured for SSH proxy in Step 4. If you used a different port, then change the command accordingly.
- Connection to the CLI interface via SSH proxy on the active unit supports copy/paste functionality that greatly simplifies license key configuration, as described in the following steps.

- b. Use the following command to check that you are logged into the redundant unit:

```
show high-availability status
```

The output should contain "Unit HA state is: NotInit".

- c. Enter the configuration mode:

```
enable
  Admin
```

- d. Determine the redundant unit's serial number, by running the following command:

```
show system version
```
- e. Open the License Key file backed up in Step 2 and determine the license key that corresponds to the redundant unit's serial number. The license key file looks as follows:

```
[LicenseKeys]
S/N<serial-number-1>=<license-key-1>
S/N<serial-number-2>=<license-key-2>
```

- f. Restore the license key. Use the redundant unit's license key instead of <license-key> in the below command. Place the value in double quotation marks to ensure that it is properly configured:

```
configure system
  feature-key "<license-key>"
exit
```



Note: It is imperative to put the <license-key> value in double quotation marks as it may contain special symbols (e.g., question mark) that may be interpreted by CLI shell as commands and result in wrong license key configuration.

10. Restore HA configuration on the redundant unit:

- a. Use the connection to the CLI interface of redundant unit via virtual console, as in Step 8.



Note: Do not use the connection via SSH proxy established in Step 9 because you will be changing network configuration of the redundant unit and this connection will be lost.

- b. Log in using the following default credentials:
 - ◆ Username: **Admin**
 - ◆ Password: **Admin**
- c. Enter the configuration mode:


```
enable
Admin
```
- d. Enter the network configuration mode:


```
configure network
```
- e. Change the application type of HA network interface to **maintenance**. Use the ID of the HA network interface configured in Step 8 instead of <ha-interface-id> (in the above example, ha-interface-id is 1):


```
interface network-if <ha-interface-id>
  application-type maintenance
exit
```
- f. Change the application type of the default network interface to **oamp**:


```
interface network-if 0
  application-type oamp
exit
```
- g. Configure generic HA settings:



Note: The below commands are used as an example; use the data captured in Step 6 instead.

```
high-availability settings
  unit-id-name "Device 2"
  remote-address 10.44.88.54
exit
```

- h. Exit the network configuration mode:


```
exit
```
- i. Reboot the redundant unit:


```
reload now
```
11. Wait until the redundant unit completes the reboot and synchronizes with the active unit.
 - a. Log in to the SBC's Web interface.
 - b. Navigate to the **MONITOR** page.
 - c. Wait until both units are displayed and the HA status is "Operational".
12. Make the redundant unit (that has "final" 7.40A.005.619 software version) active:
 - a. On the **MONITOR** page, check which unit is active.
 - b. If the first unit (that wasn't upgraded to "final" 7.40A.005.619 version yet) is active, perform a switchover, by clicking **Actions** > **Switch Over** on the toolbar.
13. Repeat steps 5 through 10 on the remaining unit (which is currently the redundant unit).
14. Disable the SSH connection to the redundant unit (enabled in Step 4):

- a. Log in to the SBC's CLI interface via SSH protocol:


```
putty.exe <sbci_ip> -l <username> -pw <password>
```
- b. Disable SSH proxy to the redundant unit, by configuring port 0 for it:

```
configure system
  cli-settings
    ssh-red-device-port 0
  exit
```

- 15. Upgrade to the latest 7.4 version (e.g. 7.40A.100.*) via the regular **Software Upgrade Wizard**, using the corresponding CMP file.

9.5.2 Alternative Upgrade Procedure – Non-Hitless Option

- **To upgrade HA Mediant VE on VMware, KVM or Hyper-V via alternative upgrade procedure without SBC service preservation:**

1. Back up configuration and the license key from the currently running software (7.2):
 - a. Log in to the SBC's Web interface.
 - b. On the toolbar, click **Actions > Configuration File**, and then click **Save Configuration Package**.
 - c. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**, and then click the **Save License Key to File** icon  .
2. Check if the device has customized certificates and ensure that they can be restored after the upgrade:
 - a. Navigate to **SETUP > IP NETWORK > SECURITY > TLS Contexts**.
 - b. For each configured TLS Context, select its row and then click **Certificate Information** and **Trusted Root Certificates** at the bottom of the screen.
 - c. Check if some customization was done for the device certificate and/or trusted root certificates.
 Default device configuration is as follows:
 - ◆ Device certificate has a Common Name that starts with "ACL_" and is self-signed
 - ◆ Trusted Root Certificates list is empty
 - d. If the device certificate was customized or some certificates were added to the Trusted Root list, make sure that you have the means to restore them (e.g., generate a new device certificate) because they are deleted during the upgrade.
3. Delete the existing virtual machines for both active and redundant units and create new virtual machines from the latest 7.4 image file. Provision new virtual machines in the same way as the old ones (use the same number of vCPUs / RAM, connect to the same virtual networks, use the same IP addresses, etc.).



Notes:

- The size of the 7.2 version image (based on CentOS 6) is 10 GB. The size of the 7.4 version image (based on CentOS Stream 8 / Rocky Linux 8) is 20 GB. Therefore, virtual disk size changes after the virtual machine rebuild.
- Instead of deleting existing virtual machines, you may stop them and postpone deletion until after the upgrade is finished. Keep in mind however, that new virtual machines will be provisioned with the same IP addresses as the old ones and therefore, you may not have both old and new virtual machines running at the same time.

4. Power off the second unit and leave only the first unit running.
5. Configure the management IP address on the first unit, as described in the section "Changing Default IP Address to Suit your Network Addressing Scheme" of [Mediant Software SBC User Manual](#). Use the same management IP address that was assigned to the SBC prior to the upgrade.
6. Restore configuration from the backup:
 - a. Log in to the SBC's Web interface.
 - b. On the toolbar, click **Actions > Configuration File**.
 - c. Click **Load Configuration Package** and then choose the configuration package backed up in Step 1; the device automatically reboots.
 - d. Wait until the device completes the reboot.
7. Power off the first unit and power on the second unit.
8. Repeat steps 5 through 6.
9. Power on the first unit.
10. Wait until both units become synchronized:
 - a. Log in to the SBC's Web interface.
 - b. Navigate to the **MONITOR** page.
 - c. Wait until both units are displayed and the HA status is "Operational".
11. Restore the license from the backup:
 - a. Navigate to **SETUP > ADMINISTRATION > LICENSE > License Key**,
 - b. Click **Load File** and then choose the license key backed up in Step 1.
 - c. Click **Apply License Key** and then choose **Non-Hitless Upgrade** to apply the license in the fastest possible way.
12. Enable SNMP if your device is connected to OVOC:
 - a. After you upgrade to version 7.4, the SNMP protocol is disabled (because the default value of the **Disable SNMP** parameter was changed to **Yes**).
 - b. If your device is connected to OVOC – for management or licensing – navigate to **SETUP > ADMINISTRATION > SNMP > SNMP Community** and then change the **Disable SNMP** parameter to **No**. Reset the device to apply the new configuration.
13. Enable Telnet server (if needed):
 - a. After you upgrade to version 7.4, the Telnet server is disabled (because the default value of the **Embedded Telnet Server** parameter was changed to **Disable**).
 - b. If your device had Telnet server enabled prior to the upgrade and you want to keep it enabled, navigate to **SETUP > ADMINISTRATION > WEB & CLI > CLI Settings** and then change the **Embedded Telnet Server** parameter to **Enable Unsecured**.
14. If needed, restore the customized device certificate and/or trusted root certificates.

This page is intentionally left blank.

10 Upgrading Mediant CE on VMware, KVM or Hyper-V

This chapter describes the upgrade procedure for Mediant CE deployment on VMware, KVM or Hyper-V, which consists of multiple virtual machines:

- Two Signaling Components, running as an active/standby pair
- Multiple Media Components

Hitless upgrade of the Mediant CE deployment on VMware, KVM or Hyper-V from 7.2 to 7.4 stream should always be performed via the 7.40A.005.619 version. For example, if you currently have the 7.20A.258.* version installed and want to upgrade to the 7.40A.100.* version, you need to perform the upgrade in two steps:

- First upgrade from 7.20A.258.* to the 7.40A.005.619 version using the special upgrade procedure described below.
- Then upgrade from 7.40A.005. 509 to the 7.40A.100.* version via the regular CMP upgrade method.



Note: The 7.40A.005.619 version lacks new features added in the 7.20A.260 stream. If you are currently running the 7.20A.260.* version, you will lose all 7.20A.260 stream specific features when you upgrade to the 7.40A.005.619 version. However, the features will be restored after you complete the upgrade to the 7.40A.100.* version or later.

10.1 Prerequisites

Prior to upgrading the device, make sure the following prerequisites are met:

- Image file of Version 7.40A.005.619 (based on CentOS Stream 8) for the specific virtual environment (OVF / QCOW2 / VHD)
- CMP file of "intermediate" 7.40A.005.619 version (same version number as above, but based on CentOS 6)
- CMP of the latest 7.4 version (e.g., 7.40A.100.*)
- Connection to the virtual host's management interface
- Connection to the Signaling Component's Web interface

10.2 Service Affecting

Upgrading the device is not service affecting. Device configuration is preserved during the upgrade. The process takes approximately 2 hours to complete.

10.3 Upgrade Procedure

- **To upgrade Mediant CE on VMware, KVM or Hyper-V:**
1. Delete **vMC Firmware File** from the Signaling Components:
 - a. Log in to the Signaling Component's Web interface.
 - b. Navigate to **MONITOR > Device Information** page
 - c. Check if **vMC Firmware File** is listed under **LOADED FILES**.
 - d. If the file is listed, delete it by clicking **Delete**.
 2. Install the "intermediate" 7.40A.005.619 version (same baseline as "final" 7.40A.005.619 version, but based on CentOS 6) on Signaling Components' VMs, using the regular Software Upgrade wizard. There is no need to install the "intermediate" 7.40A.005.619 version on Media Components' VMs.
 3. Install the "final" 7.40A.005.619 version (based on CentOS Stream 8) on the Signaling Components' VMs. Use the upgrade procedure as described in the previous sections for HA Mediant VE deployment in your environment.
 4. Install the "final" 7.40A.005.619 version (based on CentOS Stream 8) on the Media Components' VMs. Use the upgrade procedure as described in the previous sections for standalone Mediant VE deployment in your environment.
 5. Upgrade the Signaling Components to the latest 7.4 version (e.g. 7.40A.100.*) via the regular **Software Upgrade Wizard**, using the corresponding CMP file.
 6. Upgrade the Media Components to the latest 7.4 version (e.g., 7.40A.100.*) via the regular **Cluster Manager Settings** screen, using the corresponding CMP file.

10.4 Rollback Procedure

Refer to the rollback procedure in the previous sections for upgrading Signaling Components and Media Components.

11 Upgrading Mediant VE on Public Clouds (AWS / Azure / Google Cloud)

If you are running software version from the 7.20CO stream (based on CentOS 8), you can upgrade to 7.4 version (based on CentOS Stream 8 / Rocky Linux 8) using a CMP file and the regular Software Upgrade Wizard or other SBC management interfaces (e.g., **copy firmware** CLI command).

If you are running software version from the 7.20A stream (based on CentOS 6), the upgrade requires a rebuild of existing Mediant VE instances from the latest 7.4 image. Refer to the section 'Upgrading the Software Version' in the Mediant VE Installation Manual for specific public cloud environment for detailed instructions.

This page is intentionally left blank.

12 Upgrading Mediant CE on Public Clouds (AWS / Azure / Google Cloud)

If you are running software version from 7.20CO stream (based on CentOS 8) you can upgrade to 7.4 version (based on CentOS Stream 8 / Rocky Linux 8) using CMP file and regular Software Upgrade Wizard or other SBC management interfaces (e.g. **copy firmware** CLI command).

If you are running software version from 7.20A stream (based on CentOS 6) the upgrade will require rebuild of existing Mediant CE instances from the latest 7.4 image. Refer to the Mediant CE Installation Manual for detailed instructions.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

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

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

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

©2023 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, VocaNom, 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-28736