

# HAIVISION



## **StreamHub**

Media Transceiver

VERSION 4.3.1

2024/04/08

Installation & Configuration Guide

[www.haivision.com](http://www.haivision.com)

# StreamHub

## Media Transceiver

VERSION 4.3.1

### Scope of this Document

This content covers the firmware installation and configuration required for Haivision StreamHub server.

- [Hardware Requirements](#)
- [Installing the Firmware](#)
- [Accessing the Settings Menu](#)
- [Configuring the Network Interfaces](#)
- [Configuring Security Settings](#)
- [Configuring System Settings](#)
- [Maintaining the Server Application](#)
- [LiveGuest Configuration](#)

## Hardware Requirements

If you are setting up the software license on your own platform, ensure that your equipment meets the following requirements. Here are the minimal hardware requirements to install and run StreamHub software application on a 1U server for each configuration.



**Note**

Haivision does not guarantee the proper operation, or even start, of the software application installed on hardware platforms which do not comply with these requirements.

Description	Manufacturer	Part Number	Standard			Ultra		
			STD-1S DI	STD-4SDI	STD-ST2110	ULT-4K MHD	ULT-8HD	ULT-ST2110
SuperChassis 514-R400W 1U Chassis	Super micro	CSE-514-R407W	✓			✓		
Power supply	Super micro	PWS-407 P-1R	✓			✓		
Power distributor	Super micro	PDB-PT514-2824	✓			✓		
Super X11SCW-F Motherboard	Super micro	MBD-X11SCW-F	✓					
Super X11SPW-TF Motherboard	Super micro	MBD-X11SPW-TF				✓		
Intel® Xeon® E-2176G	Intel	E-2176G	✓					
Intel Xeon Gold 6226R	Intel	CD8069504449000				✓		

Description	Manufacturer	Part Number	Standard			Ultra		
			STD-1S DI	STD-4SDI	STD-ST2110	ULT-4K MHD	ULT-8HD	ULT-ST2110
1U PASSIVE CPU HS FOR INTEL LGA1156	Supermicro	SNK-P0046P	✓					
1U PASSIVE CPU HS FOR INTEL LGA3647-0	Supermicro	SNK-P0067PS-001				✓		
8GB DDR4-2400 ECC UDIMM CL17 1Rx8	Dataram	DVM24E1T8/8G	(x2)					
8GB 1Rx8 PC4-2666V-R19 Micron	Dataram	DTM68127A				(x6)		
1TB 2.5" 7200RPM SATA3 6Gb/s 128M Internal Hard Drive	Seagate	ST1000NX0423	✓					
1TB Enterprise Capacity 2.5 HDD 4KN SATA	Seagate	ST1000NX0303				✓		
Supermicro 1U Passive Riser Card - 2 PCI-E x8 slots or PCI-E x16 slot	Supermicro	RSC-W-68	✓					
Supermicro 1U Passive Riser Card - 2x PCI-E x16 slots	Supermicro	RSC-R1UW-2E16				✓		
Fan(s)	Supermicro	FAN-0141L4	✓ (x2)			✓ (x2)		
Creative Sound Blaster Audigy Fx	Creative	Audigy Fx	✓			✓		

Description	Manufacturer	Part Number	Standard			Ultra		
			STD-1S DI	STD-4SDI	STD-ST2110	ULT-4K MHD	ULT-8HD	ULT-ST2110
DeckLink Mini Monitor 4K	Black magic Design	DeckLink Mini Monitor 4K	✓					
DeckLink Duo 2	Black magic Design	DeckLink Duo 2		✓				
Deckink 8K Pro	Black magic Design	Deckink 8K Pro				✓		
DeckLink QUAD 2, available on ULT-8HD (not ULT-4KMHD)	Black magic Design	DeckLink QUAD 2				✓		
Mellanox ConnectX-6 Lx	NVidia	ConnectX -6 Lx			✓			✓
Raid Card - MegaRAID SAS 9341-4i SGL	Broadcom	MegaRAID SAS 9341-4i SGL	Option			Option		

## Installing the Firmware

 Tip

The complex process has been broken down into smaller procedures or steps. To avoid complications, be sure to perform these steps in order. Click the table links above to navigate back and forth between steps.


This procedure guides you through the steps of installing an update to your server's firmware using a bootable USB storage device with the ISO.

This complex task involves performing the following procedures:

1. [Preparing a Bootable USB Key.](#)
2. [Performing Backup Precautions.](#)
3. [Installing from the ISO.](#)
4. [Importing the Exported Files.](#)

## Preparing a Bootable USB Key

Installing the Firmware	
Step	Description
1	Step 1: Preparing Bootable USB Key
2	<a href="#">Step 2: Performing Backup Precautions</a>
3	<a href="#">Step 3: Installing from the ISO</a>
4	<a href="#">Step 4: Importing the Exported Files</a>

 **Tip**

The complex process has been broken down into smaller procedures or steps. To avoid complications, be sure to perform these steps in order. Click the table links above to navigate back and forth between steps.

### Prerequisites

You will need:

- Utility software for creating a bootable USB key (e.g., Rufus).
- USB Key with at least 4Gb capacity (FAT32 format).
- ISO File from the Support team.

 **Note**

Once you downloaded the ISO file as indicated by the support team, you can create the bootable USB key that will be used for the installation.

To create a bootable USB key:

 **Important**

During the bootable USB key creation, please make sure to select MBR partition mode. The use of UEFI mode is not supported.

1. Make sure that you have installed on a utility software (such as Rufus) to create a bootable USB key (FAT32 format).
2. Insert the USB key (minimum capacity: 4Gb).
3. Open the utility software.
4. Choose USB key as the destination device.
5. Browse and select the provided ISO file.
6. Start flashing.

The ISO file is copied on the USB key. You can now install the firmware.



## Backup Precautions

Installing the Firmware	
Step	Description
1	<a href="#">Step 1: Preparing Bootable USB Key</a>
2	Step 2: Backup Precautions
3	<a href="#">Step 3: Installing from the ISO</a>
4	<a href="#">Step 4: Importing the Exported Files</a>



**Tip**

The complex process has been broken down into smaller procedures or steps. To avoid complications, be sure to perform these steps in order. Click the table links above to navigate back and forth between steps.



**Important**

As this firmware installation requires use of an ISO file, all current configuration and local files will be deleted.

Consequently, before installing the firmware, make sure that:

- You saved / exported the license settings.
- You exported the configuration.
- You saved the IP settings.

Additionally, you might want to save screenshots of various settings:

- IP inputs
- Encoder profiles
- FTP settings

- Physical outputs
- Streaming outputs...

Use the following as a checklist and click the ► item to expand/collapse the listing to display instructions as needed:

### Exporting License Settings

On a StreamHub v3.x, you can export the license settings from the Web User Interface of the server.

1. In the menu bar, click on **admin**.
2. Click on **License**.

### Exporting the Configuration

The procedure varies slightly depending upon your current firmware version. Make a selection from the following tabs based upon your firmware version.

#### Prior Migration from a 3.x to a 4.x Firmware Version

To export the StreamHub configuration (application settings):

1. In the menu bar, click on **admin**.
2. Click on **Export Config** button. The StreamHub configuration is saved as a `.awj` file.

#### From 4.x Firmware Version

To export the StreamHub configuration:

1. In the menu bar, click on **Settings**.
2. In the sidebar, click on **General**.
3. Click on the **Export Config** button. The StreamHub configuration is saved as a `.awj` file.

### Saving IP Settings

To save IP settings to the server, you can:

- **On-Premise:** Connect a VGA monitor and a USB keyboard directly to the server.
- **Remote:** Connect a computer to the server using the Ethernet port 2 and a secure shell (ssh) session.

#### On-Premise: Via a Monitor and Keyboard Attached to the Server

To save the IP settings using a monitor and keyboard:

1. Plug a VGA display monitor to the server.
2. Plug a keyboard to an USB interface on the server.
3. Power on the server.

- When prompted, follow the directions to log in to the server. The default credentials depend upon your firmware version:

Firmware Version	Prior v3.1	From v3.1	From 4.0
Username	user	config	config
Password	user	config	Password as defined during installation. <div style="border: 2px solid orange; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>On a newly delivered unit, the password is defined by Haivision and provided in the plastic label available on the front panel of the server.</p> </div>

The settings menu appears.

```

=====
== 1 - IPMI Settings ==
== 2 - IP Settings ==
== 3 - Password Settings ==
== 4 - Security Settings ==
== 5 - System Settings ==
== S - Restart services ==
== B - Reboot Device ==
== H - Halt Device ==
== E - Exit ==
=====
=> choice : _
    
```

- Use the arrow keys to select **IP Settings** menu (option 2).
- Select **Interface 1**.
- When the current IP Address is displayed, take a picture of the screen being sure to include the network settings (local IP, netmask, and gateway).
- Press **R**, then select **Interface 2**.


- Take a picture of the screen being sure to include the network settings (local IP, netmask, and gateway).

### Remote: Via an Ethernet and Secure Shell (SSH) Session with the Server

This method requires use of an:

- Ethernet cable (not included)
- Secure Shell (ssh) :
  - On Mac or UNIX, use a terminal window to initiate the secure shell (SSH) session.
  - On Windows, you need the Remote Desktop Protocol (RDP) or to install a utility such as PuTTY or Tera Term.

*To save the IP settings using an Ethernet port on the Computer:*

- Plug the computer to the server on the Ethernet Port 2.
- On your computer, open the  panel and select the **Ethernet Settings** menu.
- Enter the following static **IP Address**: 192.168.10.200
- Open an `ssh` client application on the computer or a terminal window and enter the following information:
  - Static IP address of the server: 192.168.10.11
  - Port: 5322
  - Connection type (or service): ssh
- When prompted, follow the directions to log in to the server. The default credentials depend upon your firmware version:

Firmware Version	Prior v3.1	From v3.1	From 4.0
Username	user	config	config

Password	user	config	Password as defined during installation. <div style="border: 2px solid orange; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>On a newly delivered unit, the password is defined by Haivision and provided in the plastic label available on the front panel of the server.</p> </div>
----------	------	--------	--

The settings menu appears.

```

=====
== 1 - IPMI Settings ==
== 2 - IP Settings ==
== 3 - Password Settings ==
== 4 - Security Settings ==
== 5 - System Settings ==
== S - Restart services ==
== B - Reboot Device ==
== H - Halt Device ==
== E - Exit ==
=====
=> choice : _
    
```

6. Use the arrow keys to select **IP Settings** (option 2).
7. Next, select **Interface 1**.
8. When the current IP Address is displayed, from the `ssh` interface, save a screenshot that includes the network settings for: local IP, netmask, and gateway.
9. Press **R**, then select **Interface 2**.
10. The current IP Address is displayed.

## Installing from the ISO

Installing the Firmware	
Step	Description
1	<a href="#">Step 1: Creating Bootable USB Key</a>
2	<a href="#">Step 2: Performing Prerequisites</a>
3	Step 3: Installing from the ISO
4	<a href="#">Step 4: Importing the Exported Files</a>



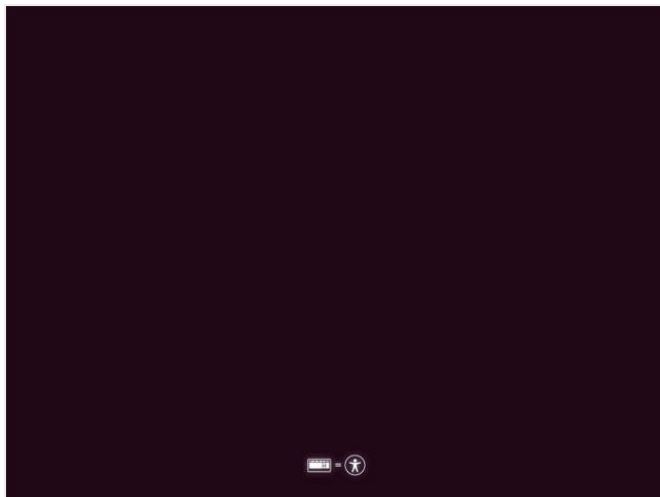
**Tip**

The complex process has been broken down into smaller procedures or steps. To avoid complications, be sure to perform these steps in order. Click the table links above to navigate back and forth between steps.

1. Insert the USB key (that you created in [Step 1: Creating Bootable USB Key](#)).
2. Power the server ON.
3. Press **F11** to enter the Boot menu.



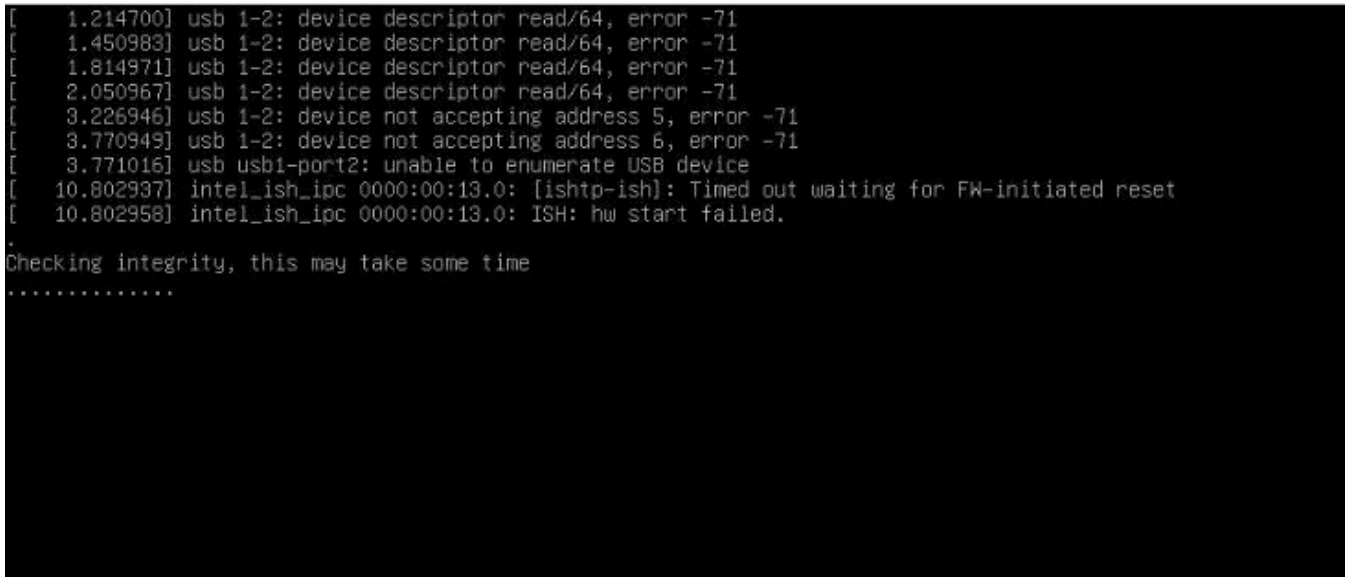
4. Press **Enter** to start the procedure.



5. Select **English** as the installation language and press **Enter**.

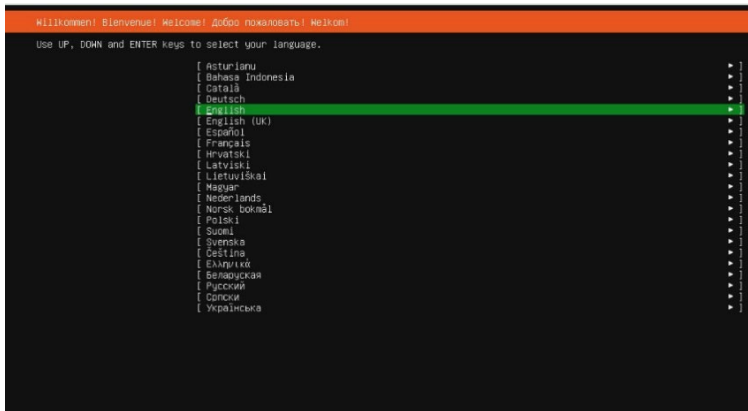


6. Select StreamHub as the type of server to be installed and press **Enter**.
7. Wait until integrity is checked and initialization is over.

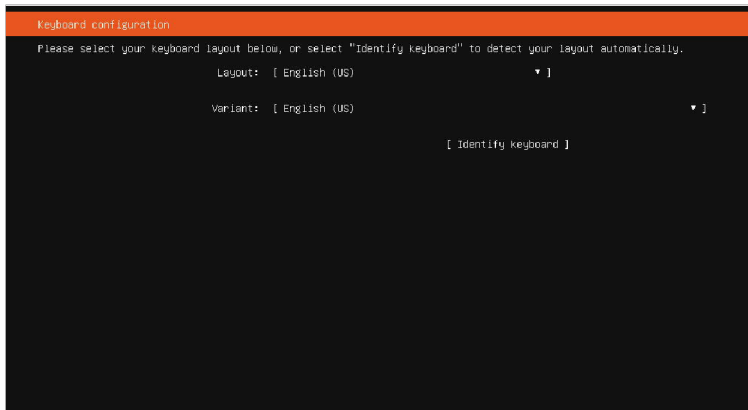


8. Select "English" as the operating language.

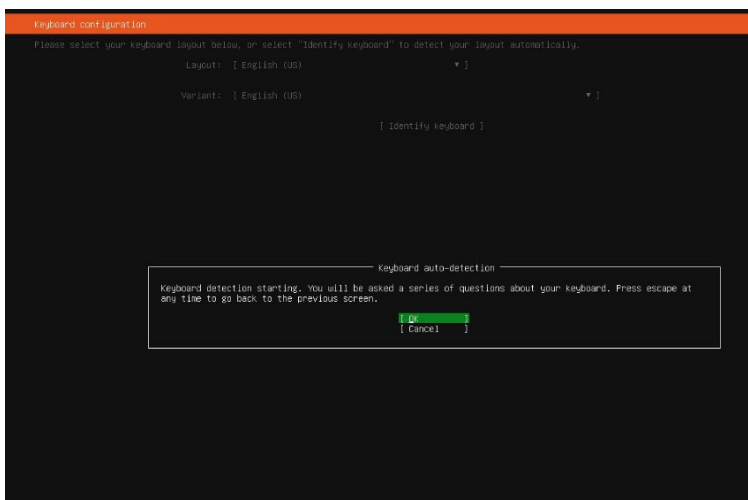




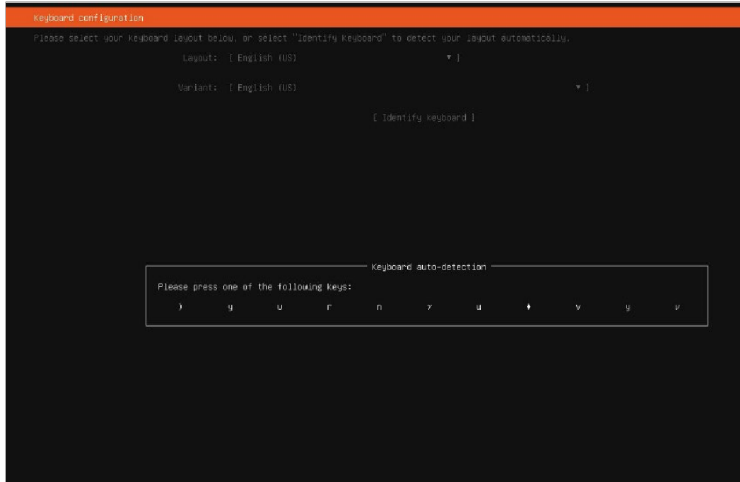
9. Use the arrow keys to select **Identify Keyboard** and press **Enter**.



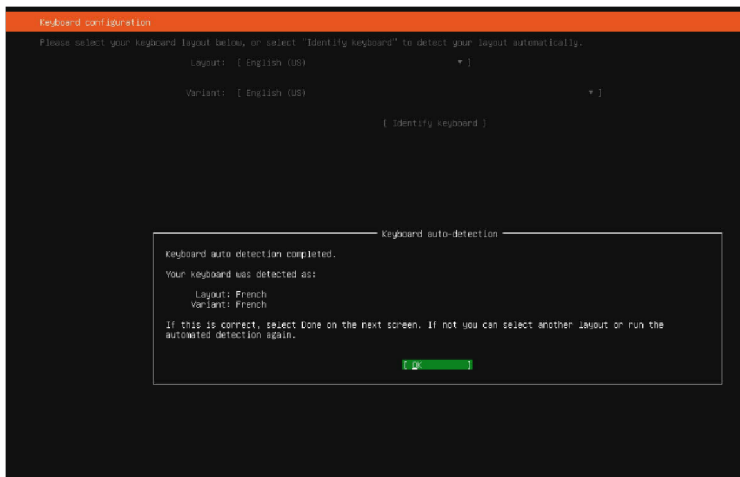
10. Select **OK**, and press **Enter** to start keyboard identification.



11. Press the keys as appropriate.



12. Once the keyboard is properly detected, press **Enter** to confirm.

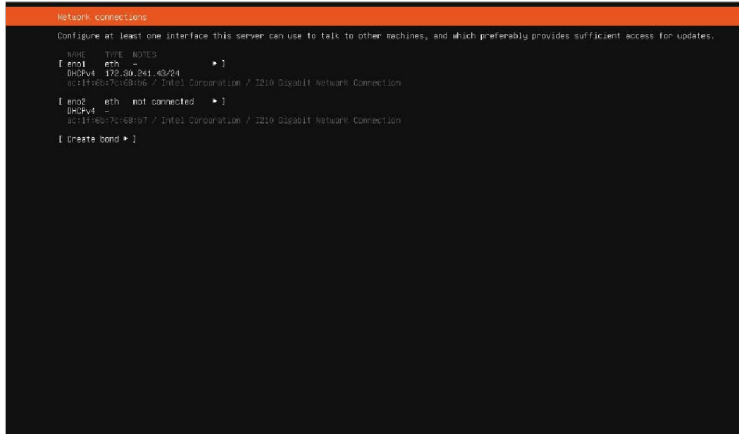


13. Press **Enter**.

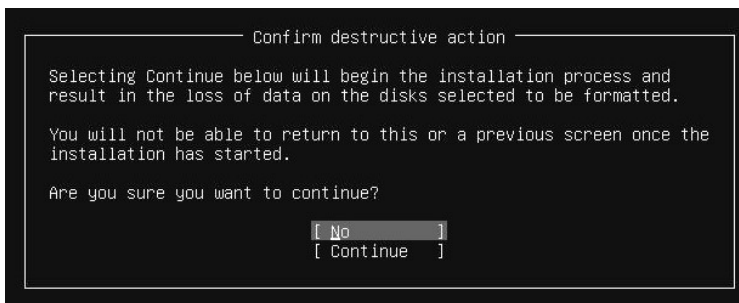


### Tip

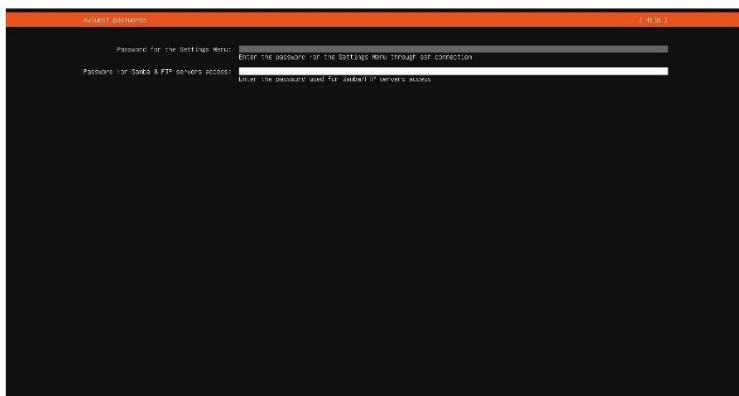
It is highly recommended that you disconnect from the public internet to ensure good operation.



14. Select **Continue** and press **Enter**.



15. Define access passwords for the SSH settings menu and for FTP/Samba servers as appropriate.



- When new passwords are defined, make note and keep them safely.



**Important**

If you lose the SSH settings password, you will need to contact Haivision support team, or to fully reinstall the application.

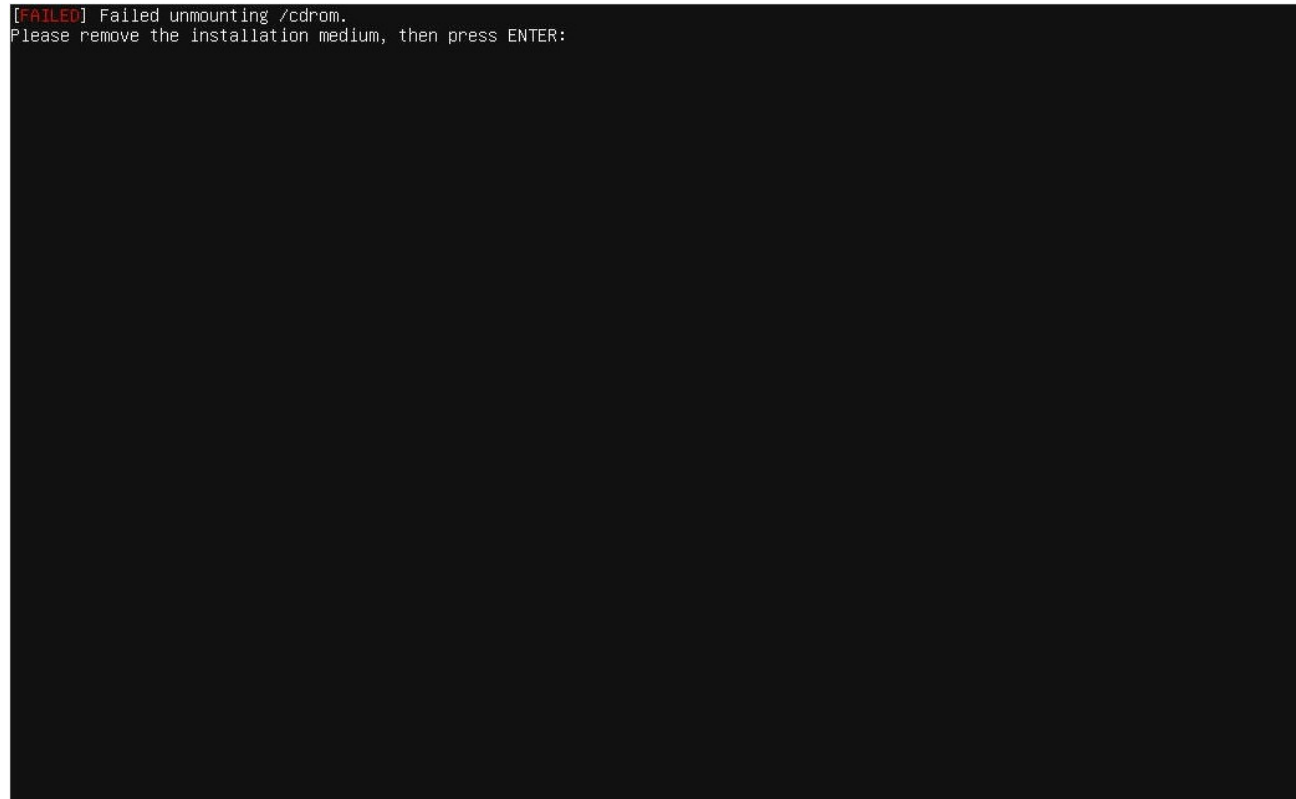
```

Install complete! [ Help ]

setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
finalizing installation
running 'curtin hook'
curtin command hook
executing late commands
final system configuration
configuring cloud-init
installing openssh-server
downloading and installing security updates
restoring apt configuration
subiquity/late/run
subiquity/late/run/command_0: curtin in-target --target=/target -- bash -c 'source /opt/avivest/scripts/postinstall.sh; runLVMPosts'
subiquity/late/run/command_1: curtin in-target --target=/target -- timedatectl set-timezone UTC
subiquity/late/run/command_2: curtin in-target --target=/target -- timedatectl set-ntp true
subiquity/late/run/command_3: curtin in-target --target=/target -- bash -c 'cd /aurepo/archives; dpkg --unpack *.deb; apt-get install --no-download -yf
|| apt-get install -y'
subiquity/late/run/command_4: curtin in-target --target=/target -- bash /opt/avivest/scripts/rootfs_postinstall.sh
subiquity/late/run/command_5: curtin in-target --target=/target -- bash -c 'source /opt/avivest/scripts/postinstall.sh; runCommonPosts'
subiquity/late/run/command_6: curtin in-target --target=/target -- bash /opt/avivest/SuperDoctor5/Install_SuperDoctor.sh
subiquity/late/run/command_7: curtin in-target --target=/target -- systemctl disable sd5.service
subiquity/late/run/command_8: curtin in-target --target=/target -- systemctl disable snmpd.service
subiquity/late/run/command_9: curtin in-target --target=/target -- bash -c 'for file in $(ls /*.deb); do echo "installing $file"; dpkg --install
$(basename $file); rm -f $file; done'
subiquity/late/run/command_11: curtin in-target --target=/target -- bash -c 'export DEBIAN_FRONTEND=noninteractive; apt install --assume-yes
--fix-broken'
subiquity/late/run/command_12: cp /cdrom/app1/desktopvideo*.deb /target/
subiquity/late/run/command_13: curtin in-target --target=/target -- bash -c 'for file in $(ls /desktopvideo*.deb); do dpkg -i $(basename $file); done'
subiquity/late/run/command_14: cp /cdrom/app1/streamhub*.deb /target/
subiquity/late/run/command_15: curtin in-target --target=/target -- bash -c 'for file in $(ls /*streamhub*.deb); do dpkg -i $(basename $file); rm -f
$file; done'
subiquity/late/run/command_16: curtin in-target --target=/target -- dpkg -l > /var/log/installer/dpkg-llist
subiquity/late/run/command_17: curtin in-target --target=/target -- chown syslog:adm /var/log/syslog
subiquity/late/run/command_18: curtin in-target --target=/target -- update-rc.d smbd disable || true
subiquity/late/run/command_19: curtin in-target --target=/target -- update-rc.d vsftpd disable || true
subiquity/late/run/command_20: curtin in-target --target=/target -- systemctl enable avahi-daemon || true
subiquity/late/run/command_21: curtin in-target --target=/target -- systemctl enable avinstalljanus.service || true
subiquity/late/run/command_22: curtin in-target --target=/target -- bash /opt/avivest/scripts/StreamHubTestPerf.sh' || true;
subiquity/late/run/command_23: echo "INSTALLATION DONE. You can reboot now."

[ View full log ]
[ Reboot Now ]
    
```

- Wait until the message, "INSTALLATION DONE" appears at the bottom of the screen.
- Select **Reboot Now** and press **Enter**.


A terminal window with a black background and white text. The text reads: "[FAILED] Failed unmounting /cdrom. Please remove the installation medium, then press ENTER:". The word "FAILED" is in red. The rest of the text is in white.

```
[FAILED] Failed unmounting /cdrom.  
Please remove the installation medium, then press ENTER:
```

19. Remove the installation USB key, then press **Enter**.
20. Enter your user credentials to log in (username should be "config" and the password should be the one you configured previously for the SSH Settings menu).
21. Configure the IP Settings (as indicated in [Configuring the Network Interfaces](#)).

## Importing the Exported Files

Installing the Firmware	
Step	Description
1	<a href="#">Step 1: Creating Bootable USB Key</a>
2	<a href="#">Step 2: Performing Precautions</a>
3	<a href="#">Step 3: Installing from the ISO</a>
4	Step 4: Importing Exported Files

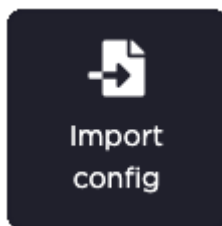
 **Tip**

The complex process has been broken down into smaller procedures or steps. To avoid complications, be sure to perform these steps in order. Click the table links above to navigate back and forth between steps.

When installing a new version of the firmware, you can import the files that you exported and saved previously (see [Step 2: Performing Backup Precautions](#)).

*To import the StreamHub configuration, proceed as follows:*

1. In the menu bar, click on **Settings**.
2. In the sidebar, click on **General**.
3. Click the **Import Config** button.



## Accessing the Settings Menu

You have two possibilities to access the **Settings** menu:

- **On-Premise** – Connecting a screen and a monitor directly to the server.
- **Remote** – Using the SSH connection (provided that the service has been previously enabled in the Security Settings menu).

```

=====
== 1 - IPMI Settings ==
== 2 - IP Settings ==
== 3 - Password Settings ==
== 4 - Security Settings ==
== 5 - System Settings ==
== S - Restart services ==
== B - Reboot Device ==
== H - Halt Device ==
== E - Exit ==
=====
-> choice : _
    
```


Choose a method appropriate to your needs.

### Accessing Settings Menu with a Monitor and a Keyboard

1. Plug a VGA display monitor to the server.
2. Plug a keyboard to an USB interface.
3. Power ON the server.


When the server prompts you, log in to the server to view the server’s **Settings** Menu. User credentials vary depending upon your firmware:

Firmware Version	Prior v3.1	From v3.1	From 4.0
Login	user	config	config

<p>Password</p>	<p>user</p>	<p>config</p>	<p>Password as defined during installation.</p> <div style="border: 2px solid orange; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>On a newly delivered unit, the password is defined by Haivision and provided in the plastic label available on the front panel of the server.</p> </div>
-----------------	-------------	---------------	---

4. Use the arrow keys to select **IP Settings** menu.

### Accessing Settings Menu with Secure Shell (ssh) Session

 **Important**

Prior to this connection:

- Ensure that the ssh service is enabled (please refer to [Configuring Security Settings](#)).
- You have the IP address of the server if connecting to the server on the same LAN.

To access the server's **Settings** menu through ssh connection, you have two options:

- **Static IP** – Connecting the computer directly to the server using the Ethernet port 2. In this case, both the server and the computer have a static IP address.
- **LAN (DHCP)** – Connecting the computer and the server to the same LAN. In this case, the network interfaces of both the server and the computer are configured on DHCP (server's Ethernet 1 interface default configuration). You need to know the IP address of the server.

Choose the appropriate method below:


#### Static IP address

Using Static IP addresses to access the server's **Settings** menu:

1. Plug an Ethernet cable from one of the **Ethernet** interface of the server configured with a static IP address to a computer.
2. Set the computer IP address to the IP: 192.168.10.200.



3. Open PuTTY or Tera Term on the computer or another `ssh` client application (MAC and Unix operating systems usually include an `ssh` terminal).
4. In the **Host** box, enter the static IP address of the server: 192.168.10.11
5. In the **Port** box, enter 5322.
6. For the connection type (or service), tick **ssh**.
7. Click the **Open** (or **OK**) button.
8. Log in to the server to view the server's **Settings** Menu. User credentials vary depending upon your firmware:


Firmware Version	Prior v3.1	From v3.1	From 4.0
Login	<code>user</code>	<code>config</code>	<code>config</code>
Password	<code>user</code>	<code>config</code>	Password as defined during installation. <div style="border: 2px solid orange; padding: 10px; margin-top: 10px;"> <p> <b>Note</b> On a newly delivered unit, the password is defined by Haivision and provided in the plastic label available on the front panel of the server.</p> </div>

## LAN (DHCP)

Using LAN (DHCP) to access the server's Settings menu:

1. Open PuTTY or Tera Term on the computer or another `ssh` client application (MAC and Unix operating systems usually include an `ssh` terminal).
2. In the **Host** box, type the server IP address.
3. In the **Port** box, enter 5322.
4. For the connection type (or service), tick **ssh**.
5. Click the **Open** (or **OK**) button.

- Log in to the server to view the server's **Settings** Menu. User credentials vary depending upon your firmware:

Firmware Version	Prior v3.1	From v3.1	From 4.0
Login	user	config	config
Password	user	config	<p>Password as defined during installation.</p> <div style="border: 2px solid orange; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>On a newly delivered unit, the password is defined by Haivision and provided in the plastic label available on the front panel of the server.</p> </div>

## Configuring the Network Interfaces

To configure the server's network interfaces:

- [Using the Default Configuration](#)
- [Configuring an Ethernet Interface](#)
- [Network Port Requirements](#)
- [Configuring IP Routes](#)
- [Deleting IP Routes](#)

## Using the Default Configuration

The default configuration for the Ethernet interfaces of the server is:

- Interface 1 (LAN1): **DHCP**  
You can connect the Ethernet interface 1 of the server directly to a 1Gb router with a DHCP Server using an Ethernet cable (RJ45).
- Interface 2 (LAN 2): **static**  
Its default IP address is 192.168.10.11.



AW-SH1



AW-SH2 / AW-SH3

Once the server has an IP address, you can connect it to a router or firewall and configure the network settings. See [Network Port Requirements](#).

## Configuring an Ethernet Interface

From the server's **Settings** menu, you can configure the IP settings of the Ethernet interfaces.

**Important**

Make sure *not* to modify the configuration of the Ethernet interface used for the ssh connection.

To configure an Ethernet interface:

1. Plug an Ethernet cable in the Ethernet interface 1 or 2 of the server, according to your needs, and connect it to a router.
2. Access the server's **Settings** menu (see [Accessing Settings Menu](#)).
3. Press the number corresponding to **IP Settings** menu.
4. Press the key corresponding to the Ethernet interface that you want to configure.  
The command prompt shows the current configuration of the selected Ethernet interface.  
Default configuration is DHCP.

```
=====
==          Interface 1 IP Setting          ==
=====
Is using DHCP      : Yes
Current IP address : 10.130.8.228
Current Netmask    : 255.255.254.0
Current Gateway    : 10.130.8.1
Current DNS        : 10.130.0.10

=====
== E - Edit          ==
== R - Return       ==
=====
=> choice : █
```

5. Select the configuration mode according to your needs:
  - If you want to use a DHCP server, simply press the backspace key.
  - If you want to configure a static IP address, press **N** and **Enter**. You can then perform the following steps.
6. Type the local **IP address** and press **Enter**.

7. Type the **Netmask** and press **Enter**.
8. Type the **Gateway**.

**Note**

If a gateway is already configured on one of the Ethernet interfaces of the server, it is mentioned. If you don't need to use a gateway, skip this step.

9. Type the DNS. The default DNS is 8.8.8.8.
10. Press **Enter** on your keyboard.
11. When prompted to confirm your changes, press **Y** to confirm (or **N** to cancel) and then press **Enter** on your keyboard.
12. Restart the server services (see [Restarting the Server Services](#)).
13. Once the server has an IP address, you can connect it to a router or firewall and configure the network settings. See [Network Port Requirements](#).

## Network Port Requirements

To operate, the server uses specific UDP and TCP ports. You need to add rules on your router or firewall to enable inbound and outbound rules on specific ports.

In the tables that follow, ports that must be accessible from the public internet are marked in green.



### Important

- The other port ranges are generally used for communication on your LAN network.
- **It is recommended to close access to these ports from the outside.**

## Mandatory IP Ports to Open

### UDP

Protocol	Destination Port	Traffic direction	Use
UDP	7900* - 79xx**	Inbound/Outbound	<p>Connection of Haivision devices to the server's IP inputs.</p> <p>*This default setting can be changed in the Base Port field from the Settings/Network menu.</p> <p>**Here, you must open a port range starting from the base port (as defined above) and equal to the number of IP inputs (as defined by the license) + 1. For instance, if the server has 16 IP inputs, you must open the port range 7900 to 7916.</p>

### TCP

Protocol	Destination Port	Traffic direction	Use
TCP	7900*	Inbound/Outbound	<p>Connection between the StreamHub and the Manager and connection initialization from other StreamHub servers (using SST IP outputs).</p> <p>*This default setting can be changed in the Base Port field from the Settings/Network menu.</p>

## Optional IP Ports to Open

When using RTSP inputs, RTMP inputs/outputs, SST outputs, TS over IP inputs/outputs, or SRT inputs/outputs, some additional ports may need to be open. These ports will depend on the respective IP profiles configuration defined through the StreamHub.

### UDP

Protocol	Destination Port	Traffic direction	Use
UDP	5000 - 5160*	Inbound	<p>Video Return for MoJoPro.</p> <p>*This default setting can be changed in the <b>Settings/Network/Advanced</b> menu.</p>
	5353	Inbound/Outbound	NDI Discovery protocol
	6960 - 69xx*	Inbound	<p>NDI input streams.</p> <ul style="list-style-type: none"> <li>Here, you must open a port range equal to the number of NDI inputs streams (as defined by the license).</li> </ul>
	7690 - 79xx*	Outbound	<p>NDI output streams.</p> <ul style="list-style-type: none"> <li>Here, you must open a port range equal to the number of NDI outputs stream (as defined by the license).</li> </ul>
	19302	Outbound	STUN server used for Live Guest



Protocol	Destination Port	Traffic direction	Use
	20000 - 20100*	Inbound/Outbound	Live Guest video and audio streams *This default setting can be changed in the <b>Settings/Network/Advanced</b> menu.
	20400* - 204xx**	Inbound/Outbound	SIP Intercom with MoJoPro (for StreamHub V3.5 and next versions). *This default setting can be changed in the UDP Port Range field in the <b>Settings/Intercom</b> menu. **Here, you must open a port range equal to twice the number of IP inputs (as defined by the license) + 1. For instance, if the server has 16 IP inputs, you must open the port range 20400 to 20432.

## TCP

Protocol	Destination Port	Traffic direction	Use
TCP	20	Inbound	Access to the FTP server running on StreamHub, port used for FTP server command.
	21	Inbound	Access to the FTP server running on StreamHub, port used for FTP server data. FTP
	21	Outbound	Default port for access to external FTP servers from the StreamHub. Used for FTP server data.
	53	Inbound/Outbound	DNS resolution.

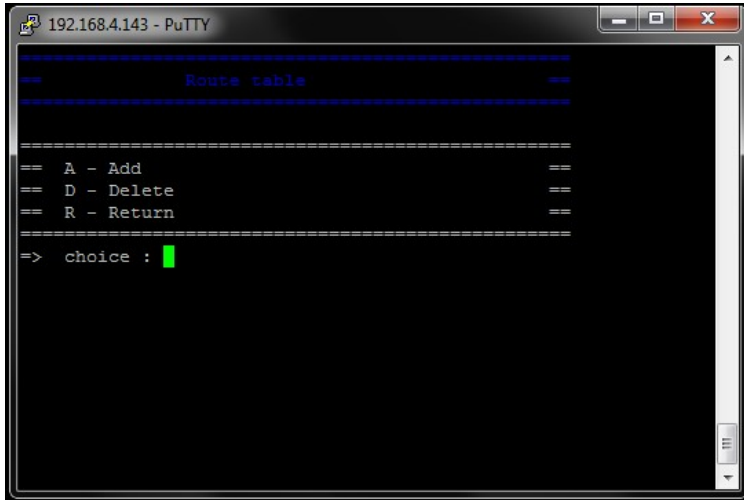
Protocol	Destination Port	Traffic direction	Use
	80	Inbound/ Outbound	Internet access for Databridge (when access to public internet is needed).
	443	Outbound	Connectivity to Haivision HUB. Get public IP address of the server.
	443	Inbound	Access to the HTTPS web user interface.
	1935	Inbound/ Outbound	RTMP inputs and outputs.
	5322	Inbound	SSH connection for secured remote access to the server (access to the system settings menu or access for AVIWEST support).
	5959 - 5960	Inbound/ Outbound	NDI Discovery Protocols.
	6960 - 69xx*	Inbound	NDI input streams. *Here, you must open a port range equal to the number of NDI inputs streams (as defined by the license).
	7901* - 79xx**	Inbound/ Outbound	SIP Intercom for MoJoPro. *This default setting can be changed in the Base Port field from the <b>Settings/Network</b> menu. **Here, you must open a port range starting from the Base Port (as defined above) +1, and equal to the number of IP inputs (as defined by the license). For instance, if the server has 16 IP inputs and your Base Port is 7900, you must open the port range 7901 to 7916.

Protocol	Destination Port	Traffic direction	Use
	7690 - 79xx*	Outbound	NDI output streams. *Here, you must open a port range equal to the number of NDI outputs stream (as defined by the license).
	8444	Inbound/ Outbound	SNMP Web User Interface through HTTPS..
	8884*	Inbound	For field unit remote control from the Web UI through HTTPS *This default setting can be changed in the <b>SST Tunnel Port</b> field in the <b>Settings/Network</b> menu.
	8885*	Inbound	For field unit remote control from the Web UI through HTTP. *This default setting can be changed in the <b>SST Tunnel Port</b> field in the <b>Settings/Network</b> menu.
	8888	Inbound	Access to the HTTP web user interface.
	8891*	Inbound/ Outbound	RTSP support. *This default setting can be changed in the <b>Settings/Network/Advanced</b> menu.
	8893	Inbound/ Outbound	RESTful API.
	8896	Inbound/ Outbound	RESTful API through HTTPS.
	12000-12009	Inbound/ Outbound	Access to the FTP server running on StreamHub, with FTP mode in passive mode.

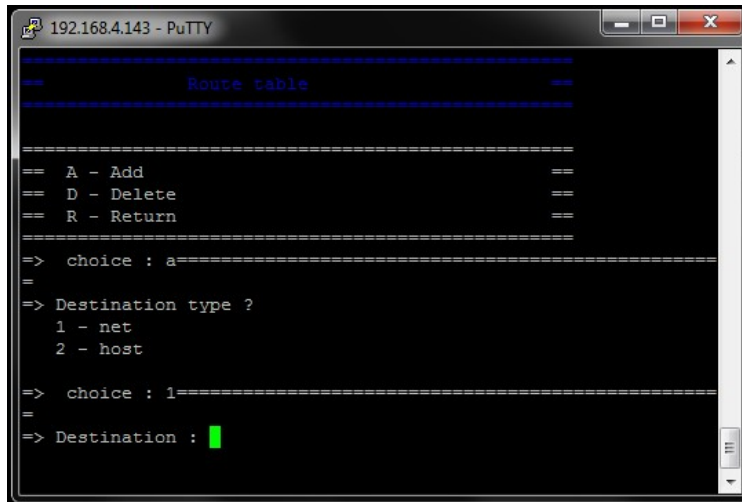
## Configuring IP Routes

According to your network architecture; you may need to configure IP routes on the server. To configure an IP route:

1. Press the number corresponding to **IP Settings** menu.



2. Press **T** on your keyboard to access the **Route table** page.
3. Press **A** on your keyboard to add a new route.
4. According to the type of destination for which you want to add a route:
  - Press **1** on your keyboard to configure a network route (**net**).
  - Press **2** on your keyboard to configure a host route (**host**).
5. Type the destination IP address.



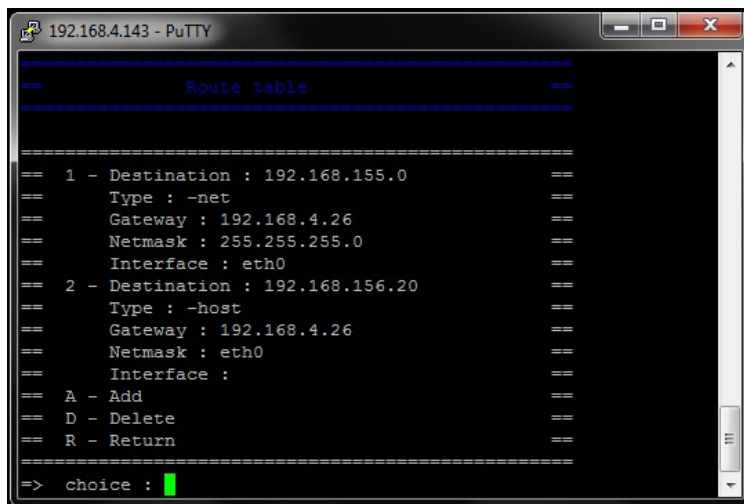
```
192.168.4.143 - PuTTY
=====
Route table
=====
== A - Add ==
== D - Delete ==
== R - Return ==
=====
=> choice : a=====
=
=> Destination type ?
1 - net
2 - host
=> choice : 1=====
=
=> Destination : █
```

6. If the destination is a network, type the **netmask**.
7. Type the **gateway** (that must be on the same LAN as the server).
8. Press **1** or **2** on your keyboard to select the Ethernet interface for which you want to set this route.

## Deleting IP Routes

To delete an IP route:

1. Press the number corresponding to **IP Settings** menu.
2. Press **T** on your keyboard to access the **Route table** page.
3. Press **D** on your keyboard to delete a route.
4. Press on your keyboard the digit corresponding to the route to delete. A message prompts you to confirm.



5. Press **Y** to confirm or **N** to cancel and then press **Enter**.

## Configuring Security Settings

Accessing the Security Settings menu allows you to enable or disable the server's services.



### Note

It is recommended to disable all services that are not used.

To configure security settings:

1. Access the server's settings menu. (See [Accessing Settings Menu.](#))
2. Press the number corresponding to the **Security Settings** menu.

```
=====
== 1 - IPMI Settings ==
== 2 - IP Settings ==
== 3 - Password Settings ==
== 4 - Security Settings ==
== 5 - System Settings ==
== S - Restart services ==
== B - Reboot Device ==
== H - Halt Device ==
== E - Exit ==
=====
=> choice : _
```

3. Enter the menu item for the settings that you want to configure and make your selections.

```
===== Server Security Settings =====
=====
== 1 - Web UI Access : X http / https ==
== 2 - Samba Server : Enable / X Disable ==
== 3 - SNMP : Enable / X Disable ==
== 4 - SSH : X Enable / Disable ==
== 6 - FTP Server Settings ==
== R - Return ==
=====
=> choice : █
```

4. When finished, press **R** to close the **Security Settings** menu and return to the previous menu.



## Configuring System Settings

If the system settings configured on your server do not match your needs, you can change them from the server's settings menu. The following system settings can be altered.

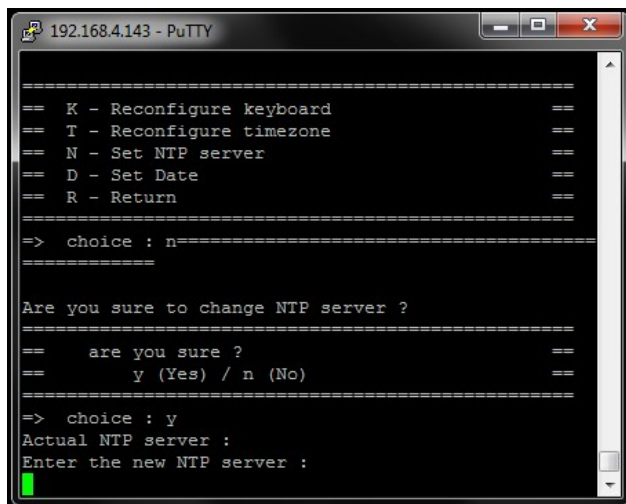
### Contents

- [Setting an NTP Server](#)
- [Setting the Time Zone](#)
- [Reconfiguring the Keyboard](#)

## Setting an NTP Server

To set an NTP server:

1. Access the server's settings menu. (See [Accessing the Settings Menu.](#))
2. Press the number corresponding to System **Settings** menu.
3. Press **N** on your keyboard to set an NTP server.
4. When prompted to confirm, press **Y** to confirm or **N** to cancel. If an NTP server is already configured, it is displayed.

A screenshot of a PuTTY terminal window titled "192.168.4.143 - PuTTY". The terminal displays a menu with options: "K - Reconfigure keyboard", "T - Reconfigure timezone", "N - Set NTP server", "D - Set Date", and "R - Return". The user has selected 'N', and the terminal prompts "choice : n". Below this, it asks "Are you sure to change NTP server ?" and "are you sure ?" with options "y (Yes) / n (No)". The user has selected 'y', and the terminal shows "Actual NTP server :" followed by "Enter the new NTP server :". A green cursor is visible at the end of the prompt.

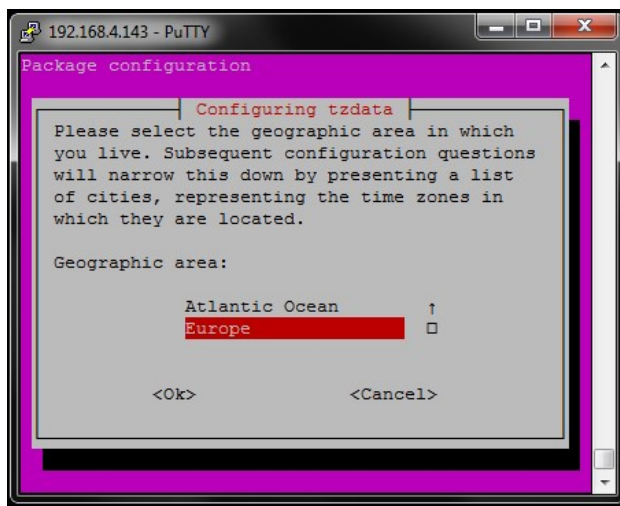
```
=====  
== K - Reconfigure keyboard ==  
== T - Reconfigure timezone ==  
== N - Set NTP server ==  
== D - Set Date ==  
== R - Return ==  
=====  
=> choice : n=====  
=====  
Are you sure to change NTP server ?  
=====  
== are you sure ? ==  
== y (Yes) / n (No) ==  
=====  
=> choice : y  
Actual NTP server :  
Enter the new NTP server :  
█
```

5. Type the new NTP server address (e.g., ntp.ubuntu.com) or set it blank to erase the NTP server currently set.
6. Press **Enter** on your keyboard.

## Setting the Time Zone

To change the time zone configured on your server:

1. Access the server's settings menu. (See [Accessing Settings Menu.](#))
2. Press the number corresponding to **System Settings** menu.
3. Press **T** on your keyboard to reconfigure the time zone.
4. When prompted to confirm, press **Y** to confirm, and then press the **Enter** key.



*The current time zone is highlighted in red.*

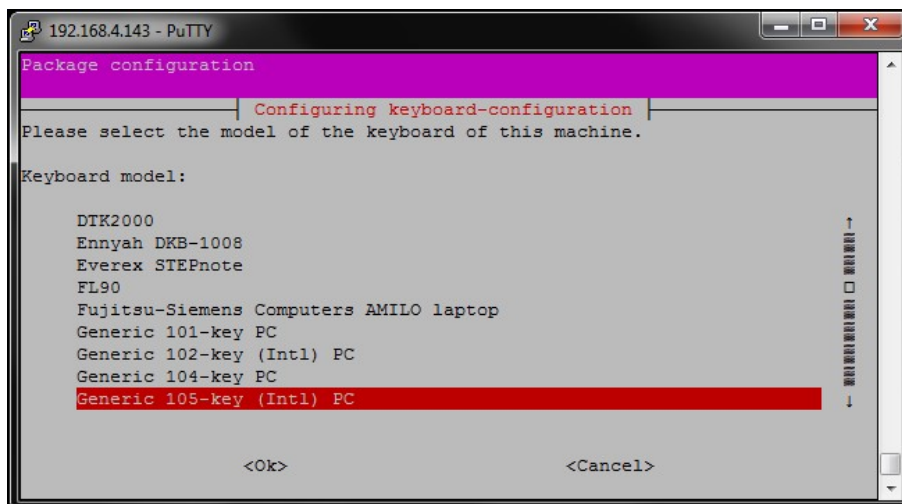
5. Press the up or down arrows on your keyboard to select a geographic area from the list.
6. Press the right arrow and then the **Enter** key on your keyboard to confirm **<Ok>** or to cancel **<cancel>** the selection.
7. Repeat steps 5 and 6 mentioned above on the following page to select the city or region.

## Reconfiguring the Keyboard

If you want to connect a keyboard directly to the server to access the server's **Settings** menu without using a computer, you may need to change the default keyboard settings.

To reconfigure the keyboard:

1. Access the server's settings menu. (See [Accessing Settings Menu.](#))
2. Press the number corresponding to **System Settings** menu.
3. Press **K** on your keyboard to select a keyboard type from the list.



4. A message prompts you to confirm.
5. Press **Y** to confirm or **N** to cancel. The keyboard currently configured on the server is highlighted in red.
6. Press the up or down arrows on your keyboard to select a keyboard from the list.
7. Press the right arrow and then the **Enter** key on your keyboard to confirm **<Ok>** or to cancel **<cancel>** the selection.
8. On the following 3 pages, follow the same procedure to select the country, the keyboard layout, and the use of the "AltGr" key.

The keyboard is now reconfigured.

## Maintaining the Server Application

### Contents

- [Restarting the Server Services](#)
- [Rebooting the Server](#)
- [Monitoring the System Health](#)

## Restarting the Server Services

You may have to restart the server services for maintenance purposes.



### Important

This operation leads to disconnecting all the online field units from the server and stopping actions in progress on the field units and on the server (Live or Forward).

To restart the server services from the server's settings menu:

1. Access the server's settings menu. (See [Accessing Settings Menu.](#))
2. Press **S** on your keyboard to restart the server services.
3. Press **Y** to confirm or **N** to cancel.
4. Press the **Enter** key on your keyboard. The Services stop and then restart.



## Monitoring the System Health

You can have access to a SNMP monitoring system to get information and health indicators.



### Note

This function is available only on Haivision servers and needs to be activated before use. Please contact the Haivision technical support team to obtain the configuration procedure as well as login and password.

Use port **8444** to access the https Web User Interface of this monitoring system. Please refer to the [SuperDoctor 5 User Guide](#) available on the Supermicro website for more details concerning SuperDoctor functionalities.



## LiveGuest Configuration

When using a StreamHub to receive LiveGuest connections, some considerations should be taken with the NAT (Network Address Translator) used between your StreamHub and the public internet. This is done to ensure connectivity from any guest using the LiveGuest solution.

Your NAT should be configured as a Full Cone NAT or Address Restricted Cone NAT, to allow proper connectivity from any remote guest. Port Restricted Cone NAT and Symmetric Cone NAT may prevent proper connectivity of remote guests, depending on the Guest own network and NAT configuration. More details on the NAT types may be found in the publicly available [RFC 3489](https://datatracker.ietf.org/doc/html/rfc3489) (<https://datatracker.ietf.org/doc/html/rfc3489>).

For more details concerning LiveGuest usage and configuration, please refer to [\(4.3.1\) Managing a Guest Interview using LiveGuest](#).

## Obtaining Documentation

This document was generated from the Haivision InfoCenter. To ensure you are reading the most up-to-date version of this content, access the documentation online at <https://doc.haivision.com>.

## Getting Help

Haivision Systems	
General Support	North America (Toll-Free) <b>1 (877) 224-5445</b>  International <b>1 (514) 334-5445</b>  <i>and choose from the following:</i> Sales - 1, Cloud Services - 3, Support - 4
Managed Services	U.S. and International 1 (512) 220-3463
Fax	1 (514) 334-0088
Support Portal	<a href="https://support.haivision.com">https://support.haivision.com</a>
Product Information	<a href="mailto:info@haivision.com">info@haivision.com</a>

Haivision MCS, LLC.	
Haivision MCS Support	<b>1 (800) 792-5975</b>
GuardianCare Portal	<a href="https://portal.cinemassive.com/">https://portal.cinemassive.com/</a>