Airvine Wave Tunnel

Configuration Guides

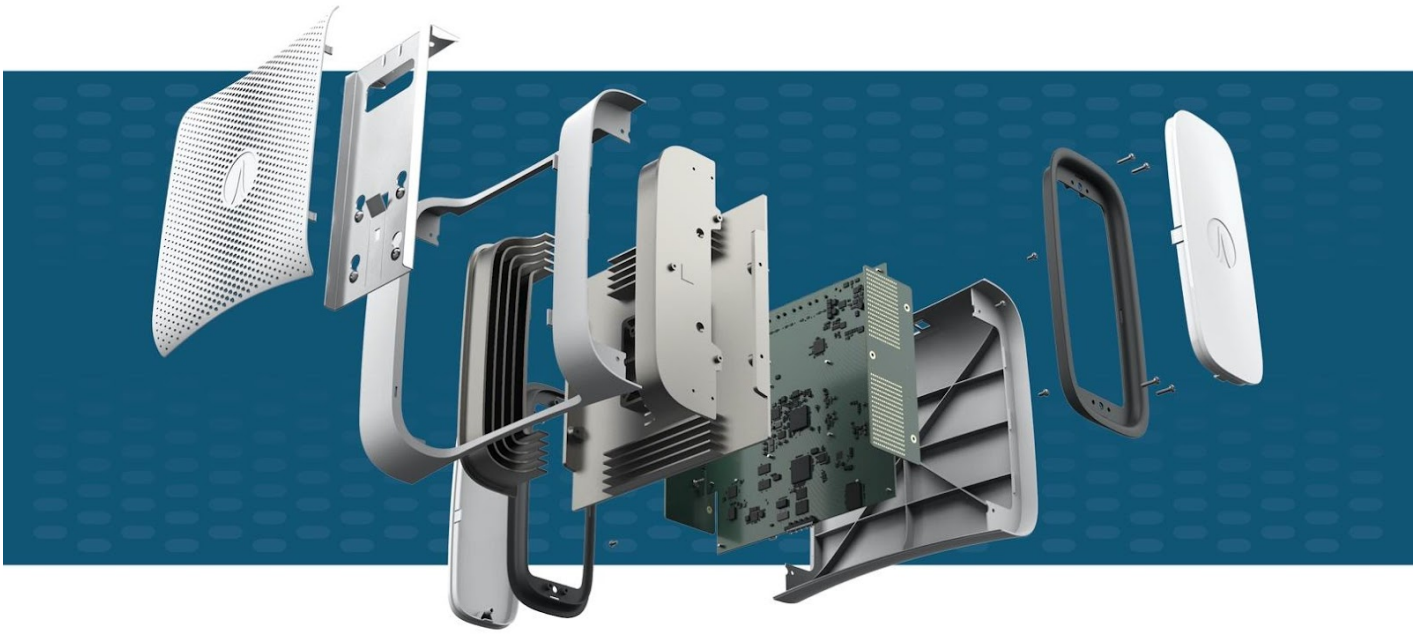


TABLE OF CONTENTS

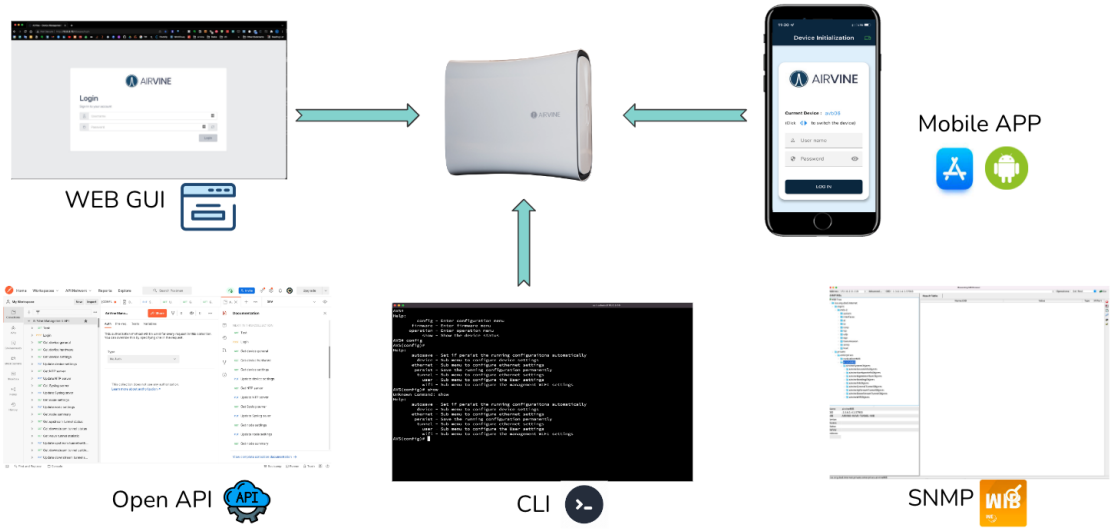
This document provides the instructions on how to configure and monitor your WaveTunnel network. You can follow the instructions described in each section to set up the WaveTunnel connections, change the configurations,monitor and troubleshoot your network.

Management Interfaces of WaveTunnel device

There are several management interfaces supported by the WaveTunnel device which you can use to manage the network. It includes:

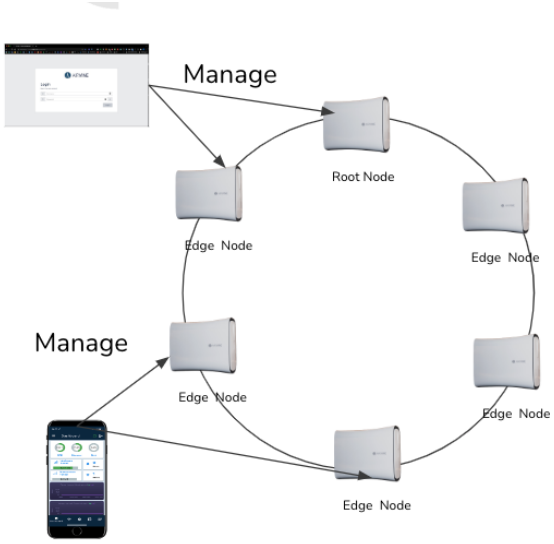
- WEB GUI
- Mobile App
- Command-Line interface
- Open API
- SNMP interface

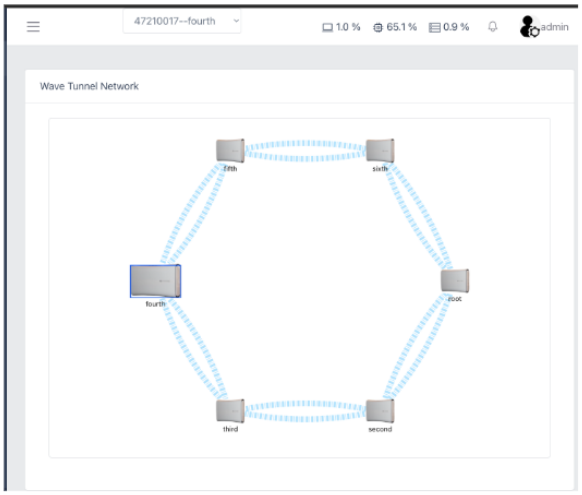
You can select the interfaces in your environment which are most appropriate to configure and monitor your network.



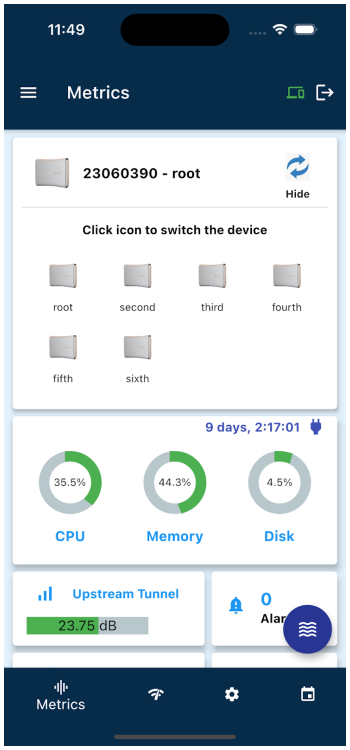
For Open API and SNMP, please refer to the API/SNMP documents for more detailed information.

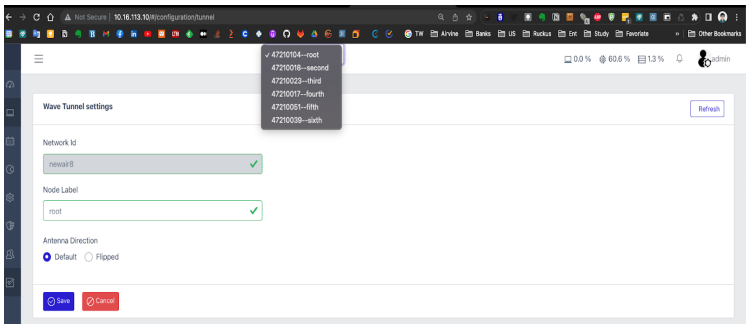
The architecture of the WaveTunnel network is designed as the “controller-less” system. It means there is no central controller in the network to manage the WaveTunnel devices. You can connect to any WaveTunnel device in the network to manage others via the WEB GUI or Mobile App. Please refer to the diagrams below.





To manage the WaveTunnel device, you can select any device on the network from the drop-down list in the WEB GUI or Mobile App.





Prerequisites for using the management interfaces

Hardware Installation Package

A complete installation hardware package includes the items listed below:

- WaveTunnel device
- Mounting bracket
- Power supply

Note: In accordance with FCC Part 15.21, Changes or modifications not expressly approved by Airvine Scientific Inc. could void the user's authority to operate the equipment.

Note: In accordance with FCC Part 15.105, This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

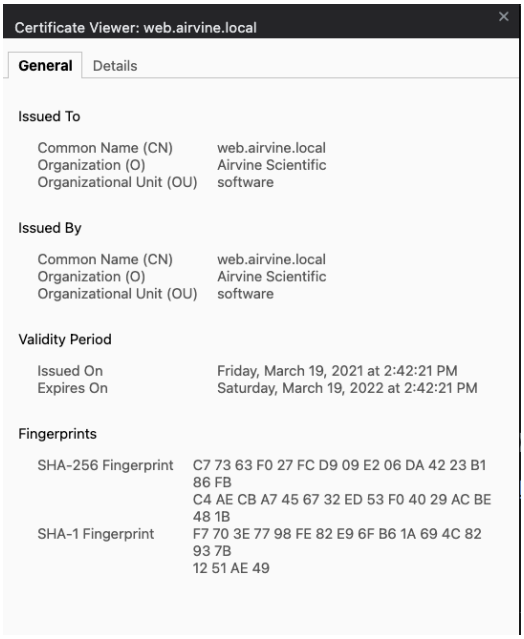
Web GUI Prerequisites

For being able to connect to the WEB GUI of the WaveTunnel device, you need a computer installed with one of the following web browsers:

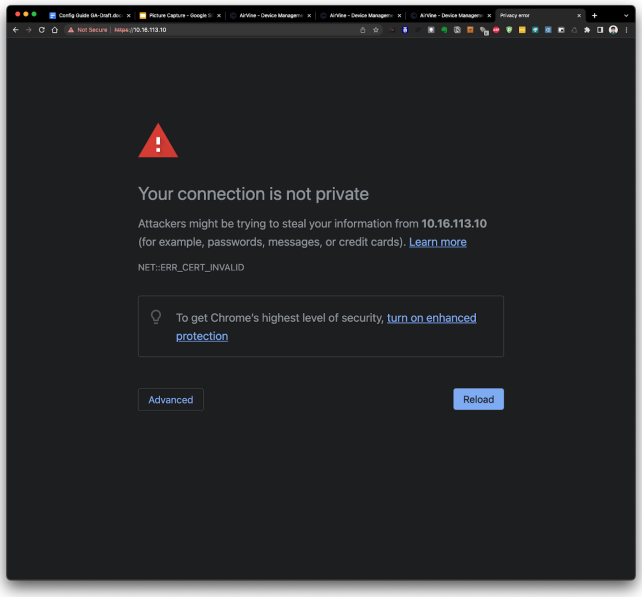
- Google Chrome
- Microsoft Edge
- Safari
- Firefox

The WEB GUI supports both **http** and **https** connections.For https connections,the web server of the WaveTunnel device uses the self-signed certificate. Thus, you need to ignore the security warnings on the browser to bypass the validation.

The information of the Airvine self-signed certificate.



For Google Chrome, there is no link on the warning page to ignore the certificate and move forward. You can type **“thisisunsafe”** to proceed.



The default login credential of the WEB GUI are

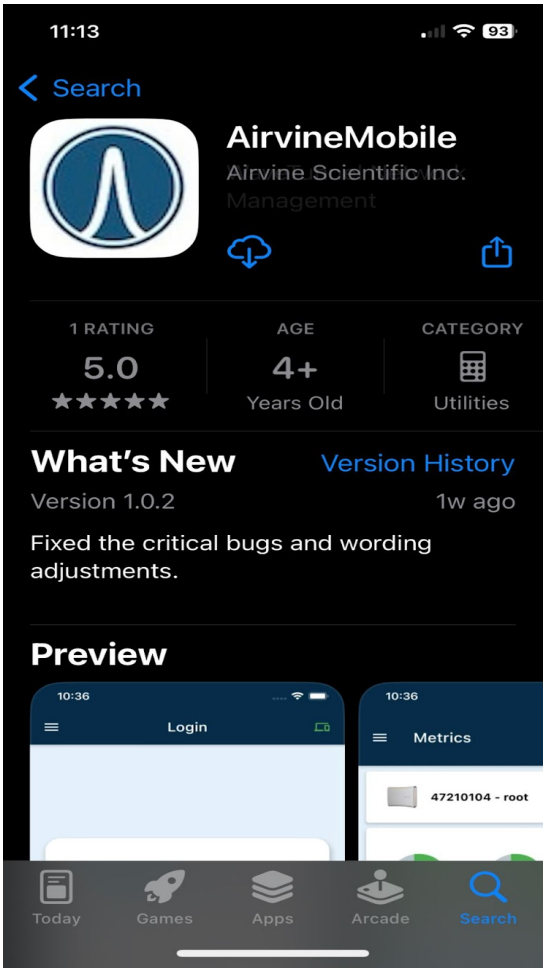
User name: **admin**
Password: **admin**

Mobile App Prerequisites

Download the "AirvineMobile" App from the App Store.

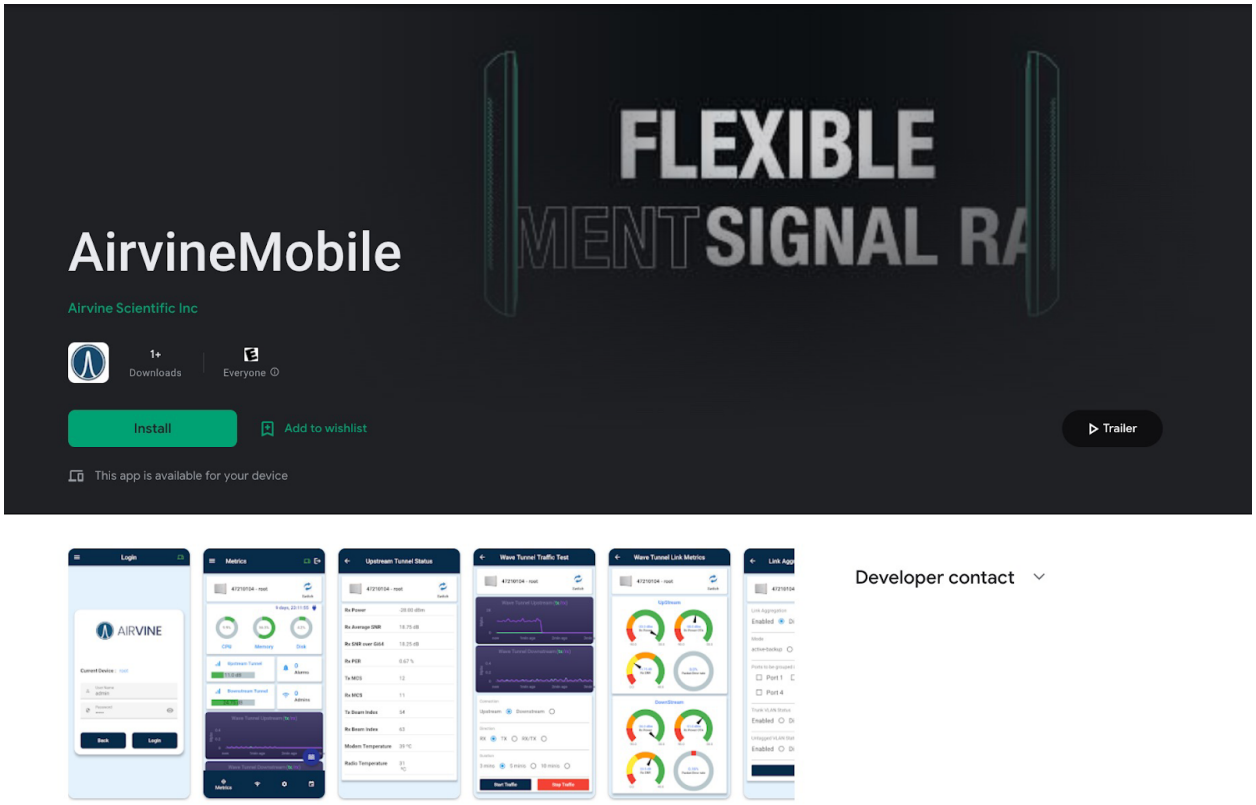
[Apple iOS]

Search "AirvineMobile" from the App Store in your mobile device.



[Android]

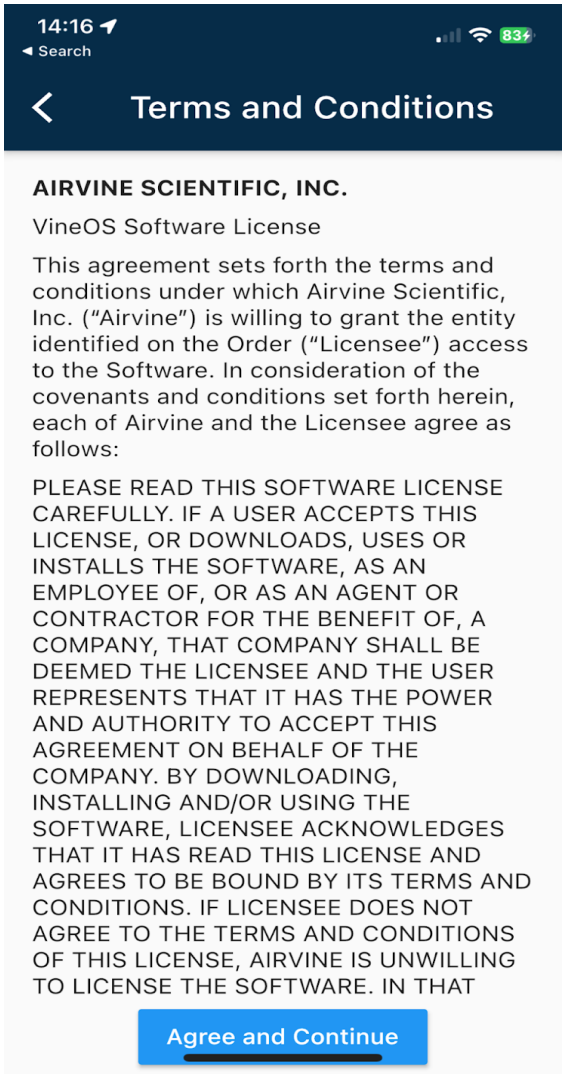
Search AirvineMobile and download the App from Google Play.



The default login credential of the mobile App are

User name: **admin**
Password: **admin**

If you wish to use the WaveTunnel mobile app for managing your WaveTunnel devices, please read the "Terms and Conditions" before connecting.



Command-Line Interface Prerequisites

There are two methods you can use to get into the command-line interface of the WaveTunnel device. You can either use the serial cable or connect through the SSH connection.

The default login credential of the command-line interface is as follows.

User name: admin
Password: admin

Enable Password: blank, just hit enter key

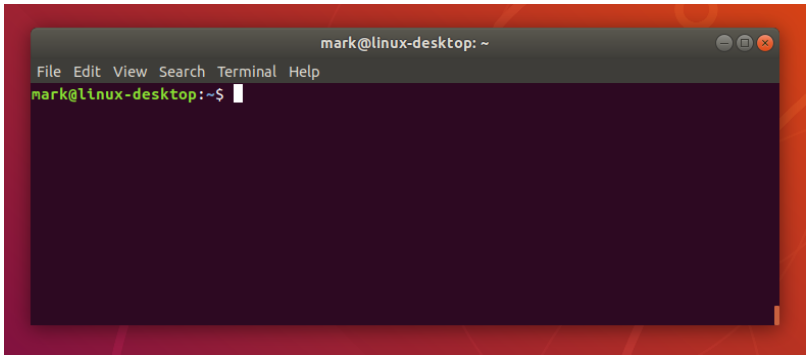
[CLI command keys]

Key	Action
Enter	Show the sub categories or command list
Tab	Auto complete
↑ ↓	View the command history
..	Go up to the parent category
Exit or Ctrl+D	Exit the CLI

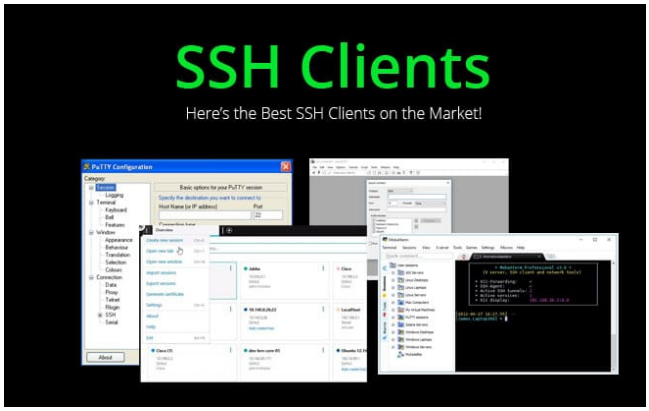
[SSH Client]

To connect the WaveTunnel device, you need to have the SSH(Secure Shell protocol) client. It can be the Linux terminal console or SSH client on other operating systems. For example, Putty, Kitty, MobaXterm…..etc.

Linux Terminal



SSH Clients



With these ssh clients, you can type “ssh admin@[IP of WaveTunel]” to connect to the device.

For example, ssh admin@192.168.3.1 if you are connecting through the management WLAN.

```
allen@allen-unc: ~
allen@allen-unc:~$
allen@allen-unc:~$ ssh admin@192.168.1.100
admin@192.168.1.100's password:
Last login: Mon Sep 19 02:38:16 2022 from 192.168.1.200
AVS>

Help:
     deviceinfo - Show the device general information
         enable - Enter 'enable' for enable mode;'enable password' to change the password
           ping - Ping destination ip. Ex: ping 8.8.8.8
     traceroute - Trace route to destination ip. Ex: traceroute 8.8.8.8
             .. - Navigate up one category
           exit - Exit Command line interface


AVS>
```

[Serial USB cable]

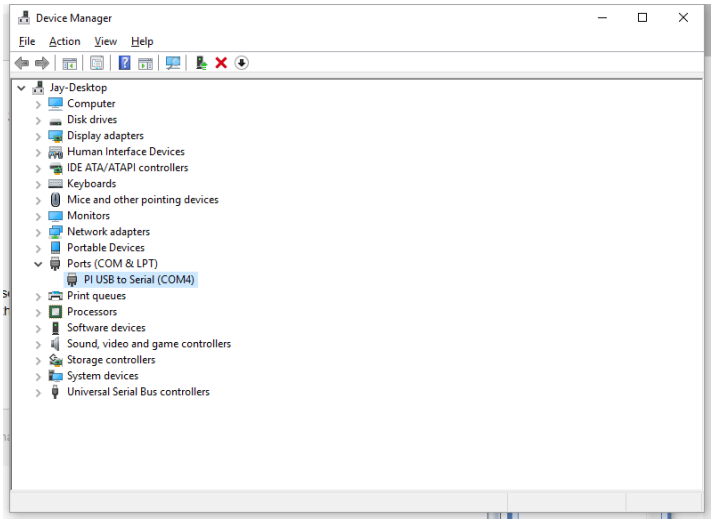
Micro-USB cable is required to connect to the WaveTunnel device if you want to use the console.

To use the serial cable connecting to the WaveTunnel device, you need to know the name of the serial port.

Below is an example of Linux or MacOS.

```
allen@allen-unc: ~
allen@allen-unc:~$ ls -al /dev/ttyUSB*
crw-rw---- 1 root dialout 188, 0 Sep 22 21:09 /dev/ttyUSB0
crw-rw---- 1 root dialout 188, 1 Sep 22 21:09 /dev/ttyUSB1
allen@allen-unc:~$
```

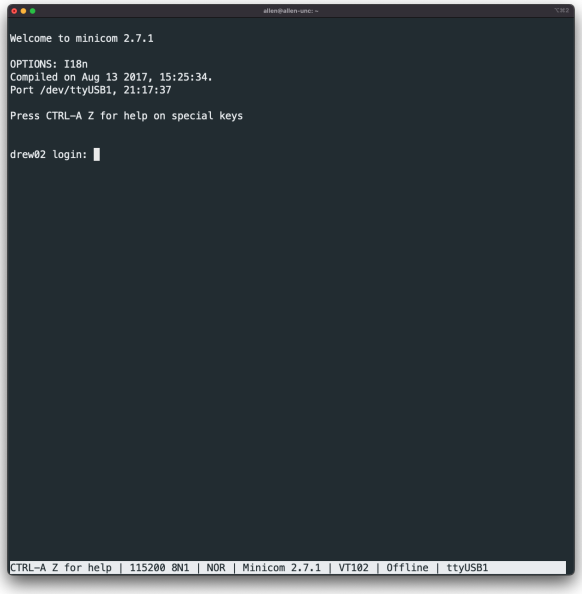
For Windows OS, please check the COM



Once you know the name of the serial port, you need to configure the settings in minicom or Putty as follows.

```
allen@allen-unc: ~

+-----------------------------------------------------------------------+
| A -    Serial Device      : /dev/ttyUSB0                              |
| B - Lockfile Location     : /var/lock                                 |
| C -   Callin Program      :                                           |
| D -  Callout Program      :                                           |
| E -    Bps/Par/Bits       : 115200 8N1                                |
| F - Hardware Flow Control : No                                        |
| G - Software Flow Control : No                                        |
|                                                                       |
|    Change which setting?                                              |
+-----------------------------------------------------------------------+
        | Screen and keyboard      |
        | Save setup as dfl        |
        | Save setup as..          |
        | Exit                     |
        | Exit from Minicom        |
        +--------------------------+
```

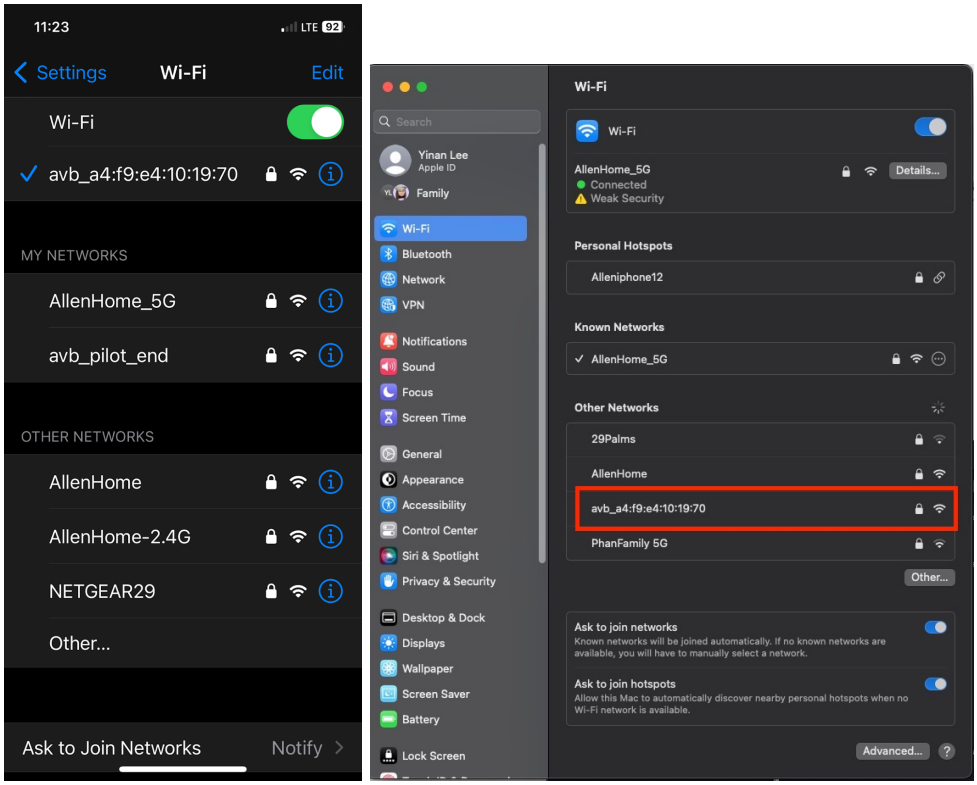
You can see the screen if you can connect to the device.



The console prompt after successfully login.

How to connect to the new WaveTunnel device

1. Management WLAN
   The default management SSID is **“avb_[MAC_ADDRESS]”**. You can check the MAC address from the label of your WaveTunnel device.



You can connect to this SSID with your mobile device or laptop. The default passphrase is **“airvine!”**.

For the laptop, type “http://192.168.3.1” on your browser to access the WEB GUI.

2. Ethernet cable

You can plug in the ethernet cable to any of the ports of the WaveTunnel device.The default IP address of the WaveTunnel device is “**192.168.0.253**”. Set the IP address of your laptop to the same subnet(e.g. 192.168.0.100) for being able to connect to the WaveTunnel device.

3. Serial console cable

Please refer to the “Command-Line Interface Prerequisites” above.

Initialize the WaveTunnel device

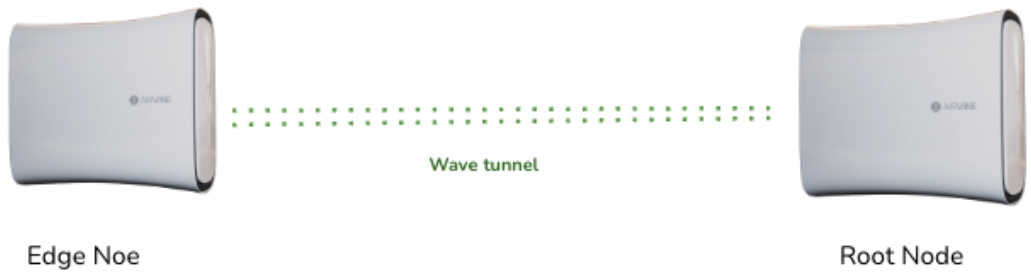
Before You Begin you will need the following:

- MAC address, which is printed on each WaveTunnel device.
- Mounting location for each node
- Root node Ethernet cabling
- Each of the nodes to be installed must be in the factory default state
- The network topology of your deployment. Please refer to the following example for the pilot phase.

Mounting Instructions

Select mounting locations for each node in the network. Nodes should be mounted using the appropriate bracket and hardware, and then powered-up before beginning the configuration process. When multiple Ethernet cables are used ensure they are bundled together.

Important: These pre-production Nodes need to be mounted facing the same direction so the radios can communicate properly (see below WaveTunnel example, the Airvine logo is on the same side.



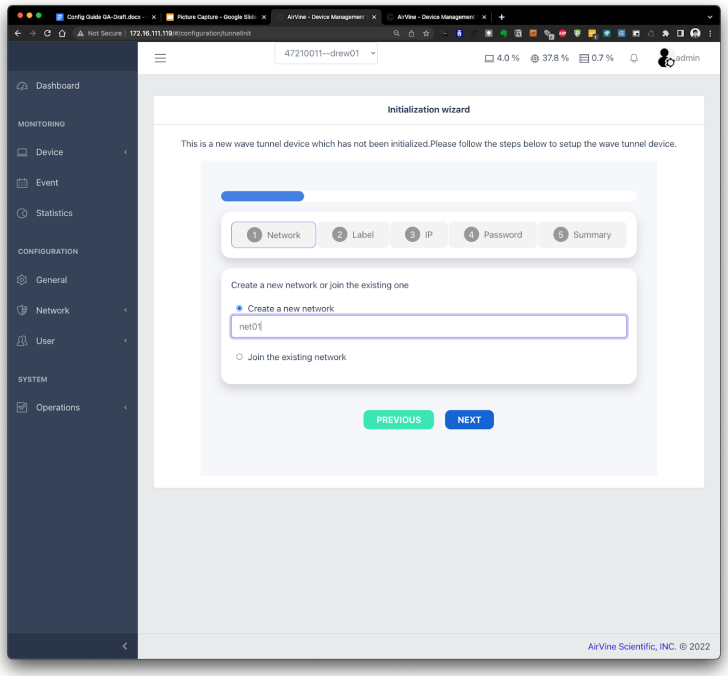
For more detailed mounting instructions, please see the "WaveTunnel Installation Guide".

Take the example below to set up the wave tunnel connection between the first(root) and the second(edge) nodes.

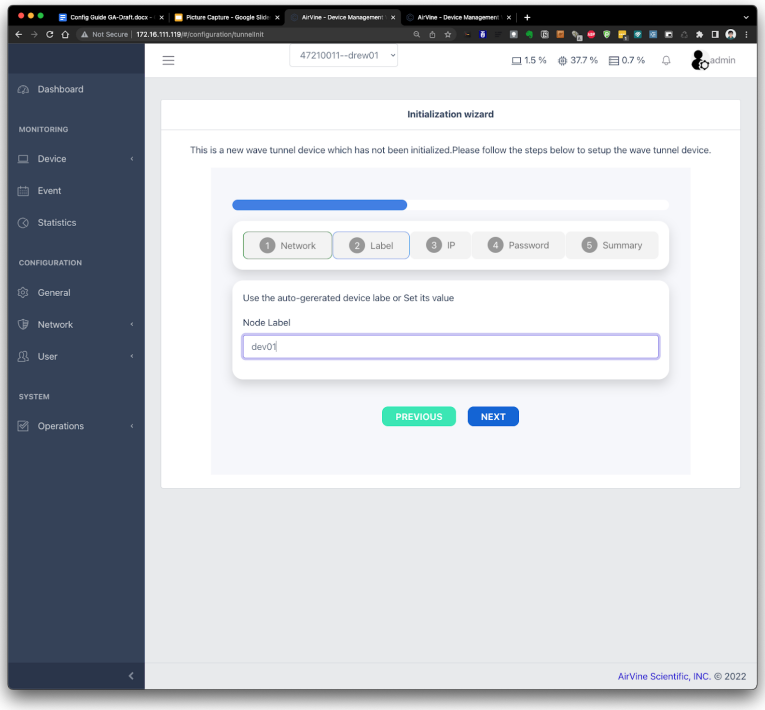
[WEB GUI]
Connect the WEB GUI through the default management SSID or ethernet cable.

- Set up the Root Node

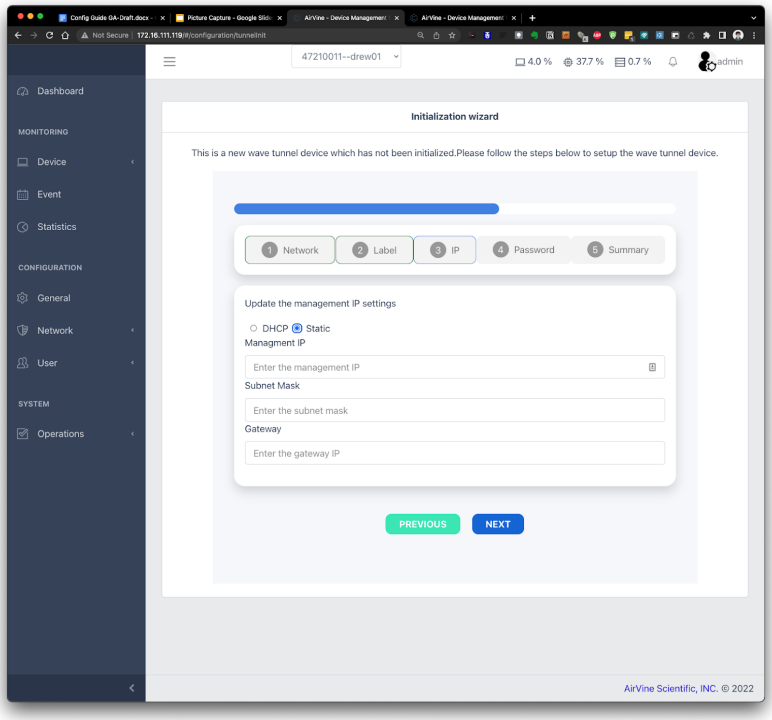
After logon to the WEB GUI, the initialization wizard is shown on the landing page. Following the Initialization wizard to set up the wave tunnel connection. The first step is selecting “Create a new network” and giving the name of this network.



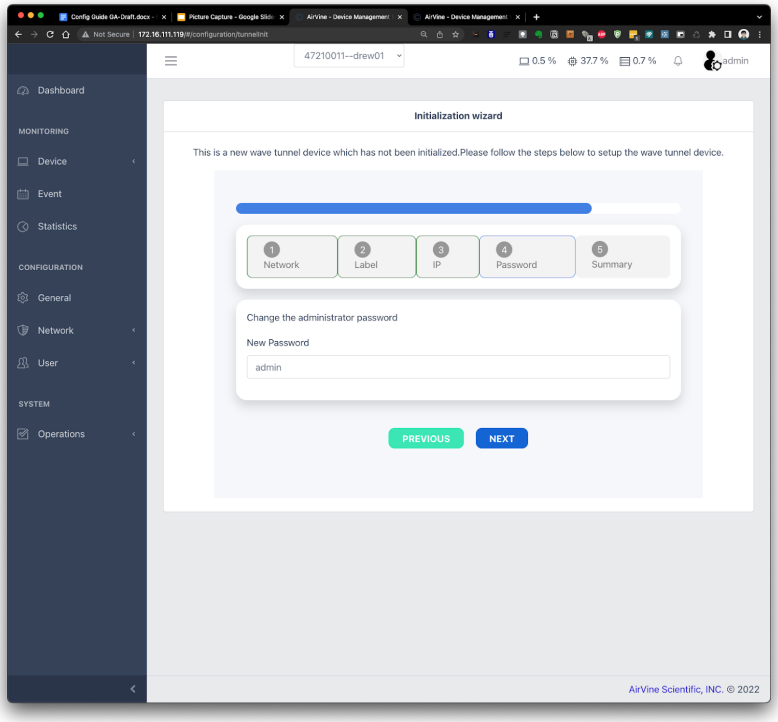
Input the label of this root node to recognize it later.



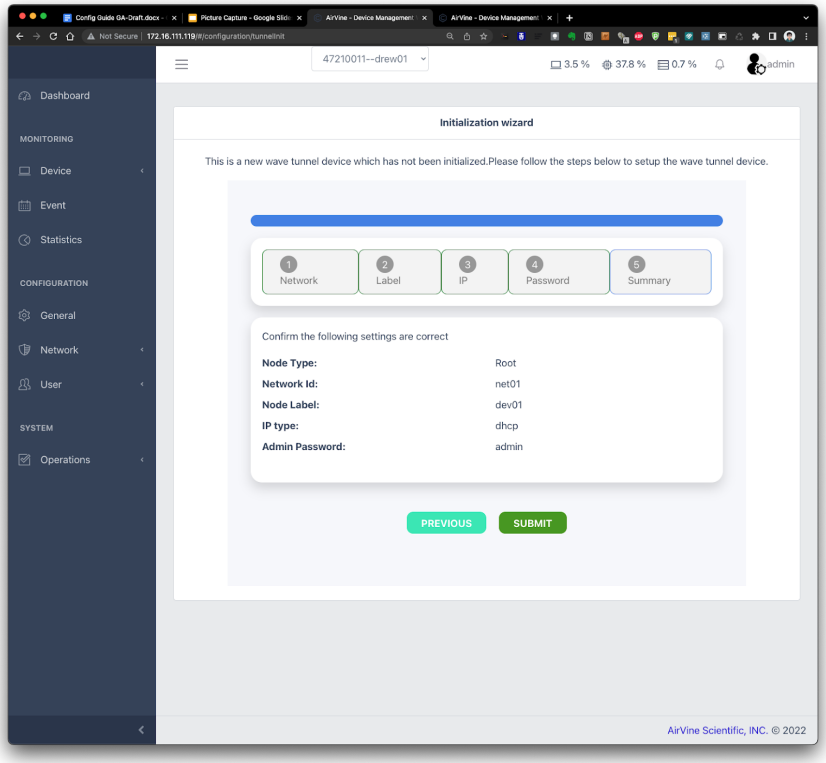
Configure the management IP of this WaveTunnel device. It can be DHCP or Static IP.



For security considerations, you can also change the default admin password in this step.

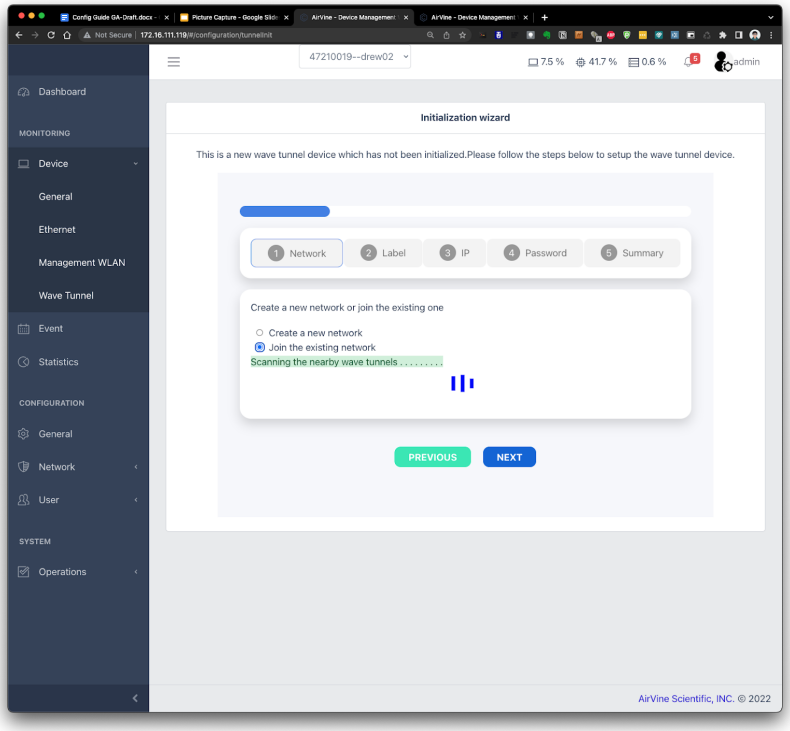


Review the settings and then click the “submit’ button to finish the configurations. You can go back to the previous steps to change the setting before clicking the “submit” button.After setup successfully, you can see the Dashboard page in your browser.

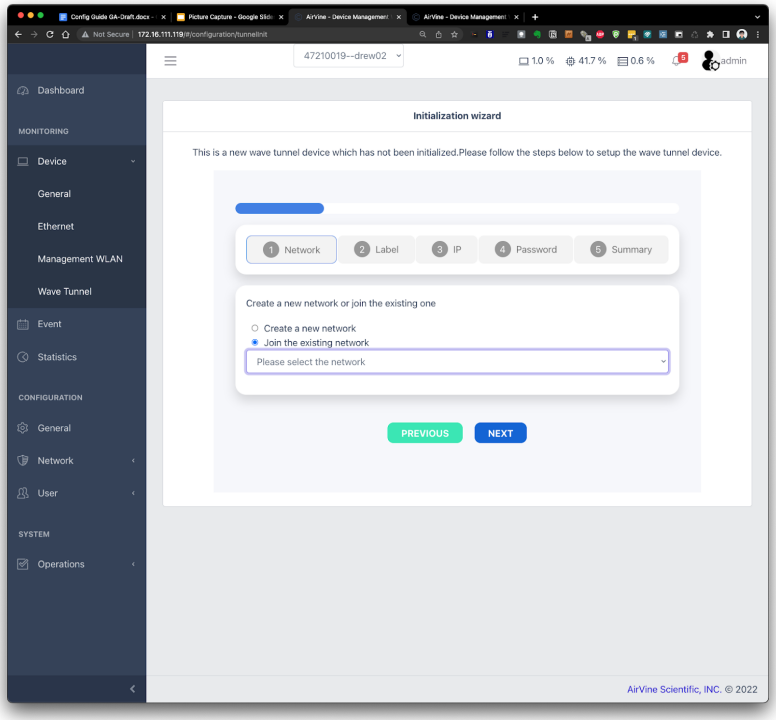


- Set up the Edge Node

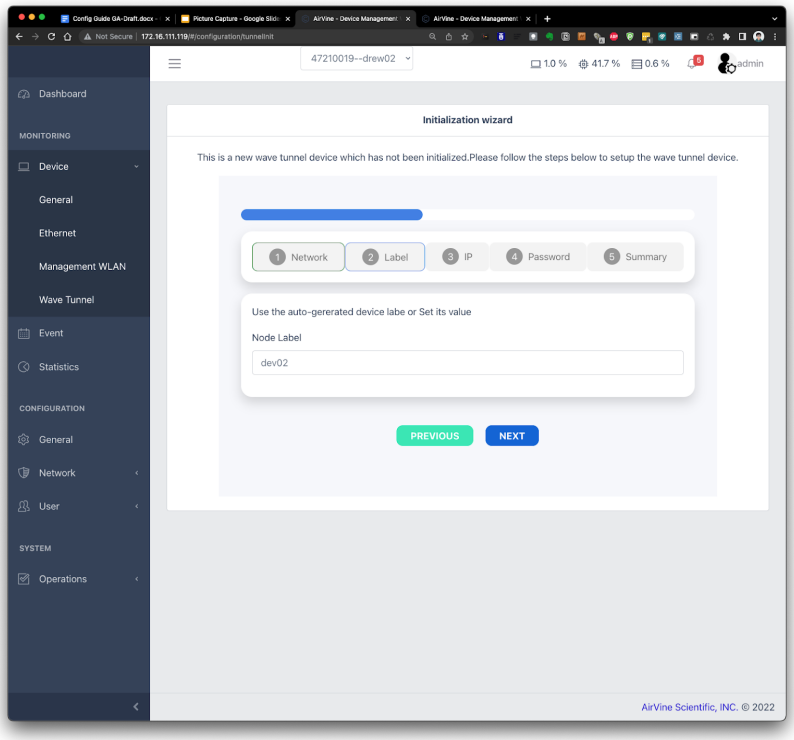
After logon to the WEB GUI, the initialization wizard is shown on the landing page. Following the Initialization wizard to set up the wave tunnel connection. The first step is selecting “join the existing network”. The page automatically scans the nearby WaveTunnel network and shows the list in the dropdown list.



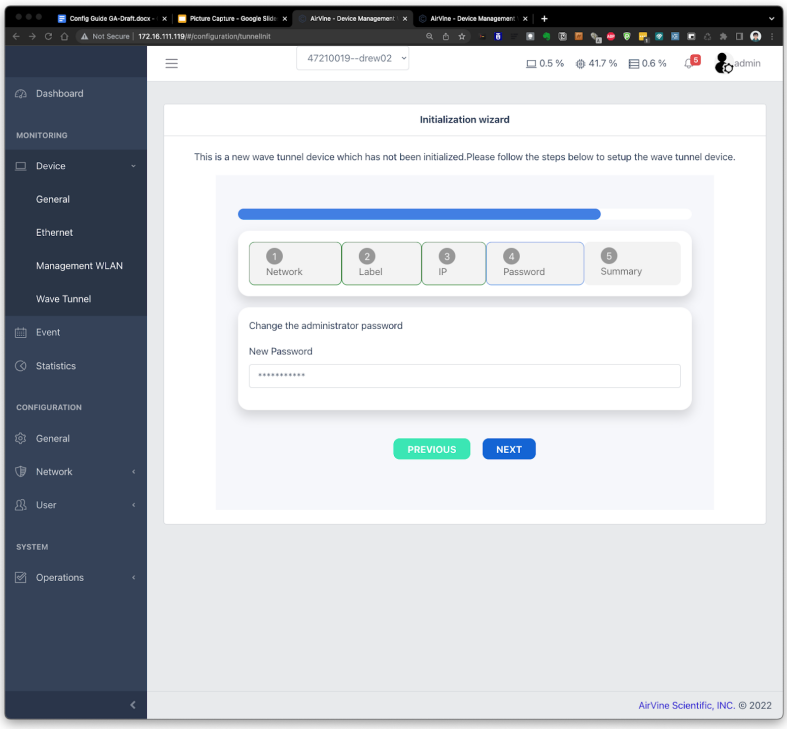
Select the network you want to connect from the drawdown list and then go to the “next” step.



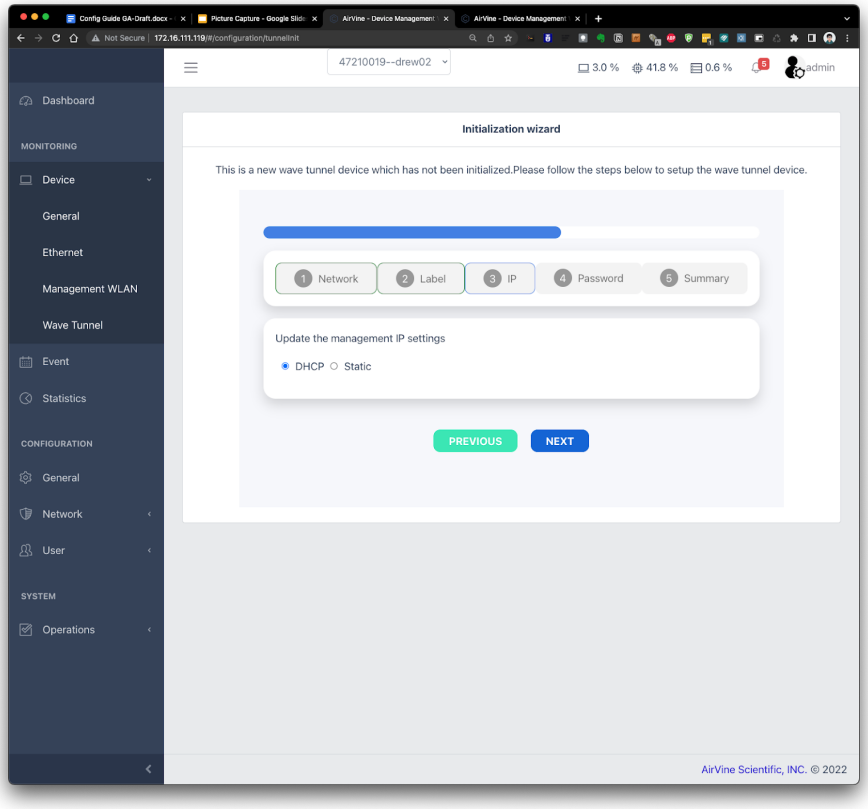
Input the label of this leaf node to recognize it later.



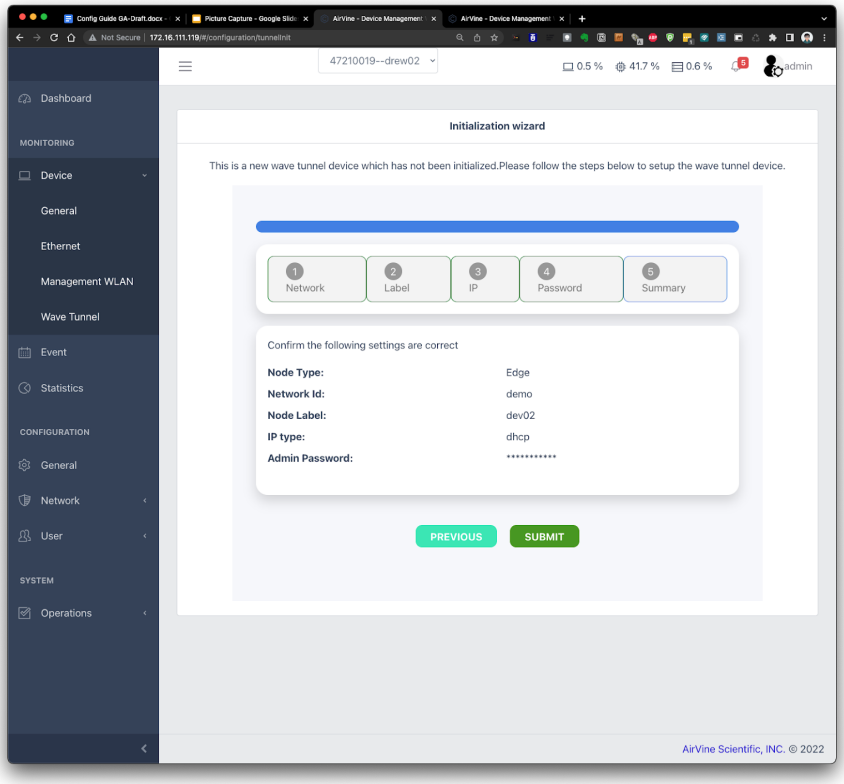
For security considerations, you can change the default admin password in this step.



Configure the management IP of this WaveTunnel device, it can be DHCP or Static IP.



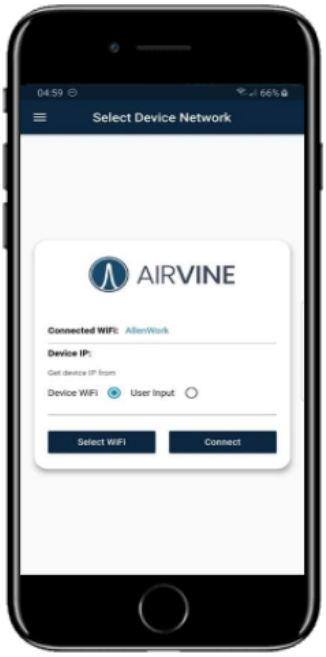
Review the settings and then click the “submit’ button to finish the configurations. You can go back to the previous steps to change the setting before clicking the “submit” button.After setup successfully, you can see the Dashboard page in your browser.



If you need to set up more than two WaveTunnel devices in your network, you can repeat the Leaf node setup steps to initialize the configurations for the remaining nodes. The max. Number of the WaveTunnel nodes supported in this release is up to 8.

[Mobile App]

Open “AirvineMobile” App on your mobile device to configure a WaveTunnel node. The “Select Device Network” page appears for you to select the device network. Click “Select Wi-Fi” to select the management Wi-Fi SSID.

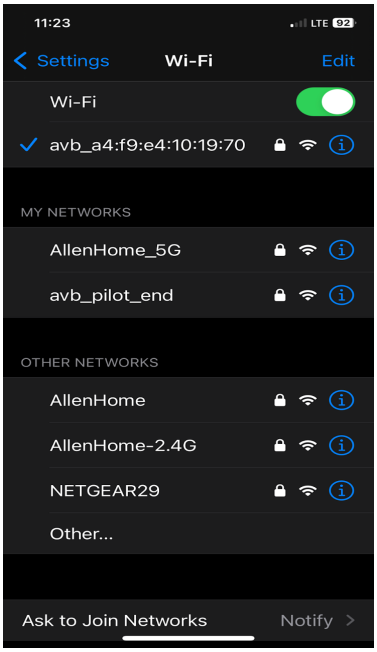


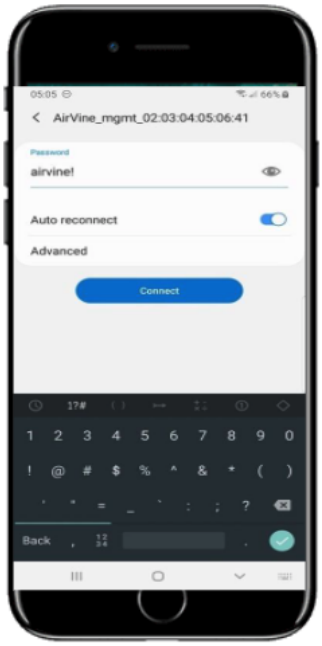
Connect the WaveTunnel node to be configured via the default management SSID which is “avb_[Device MAC]”.

A WaveTunnel node's MAC address is included in the default SSID for aiding in the setup of a network when there are other WaveTunnels broadcasting SSIDs in the area. The MAC address is labeled on each WaveTunnel unit.

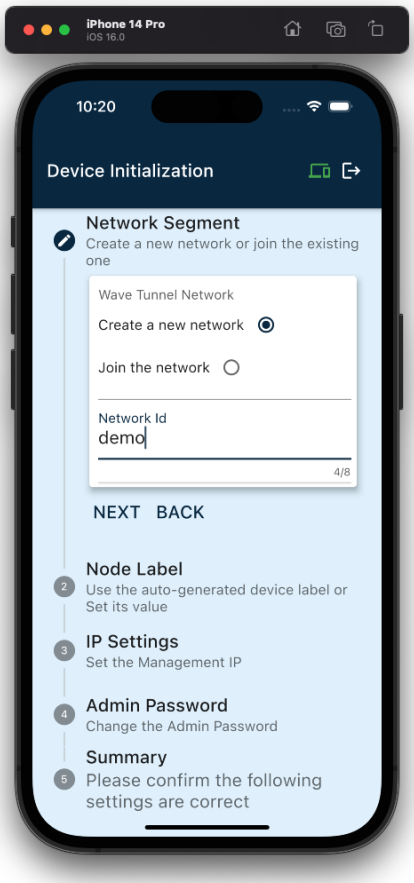
The default password for the management SSID is “airvine!”. The exclamation mark is required.

Once connected to the management Wi-Fi SSID, please press “<” on the bottom right to go to the “AirvineMobile” App.





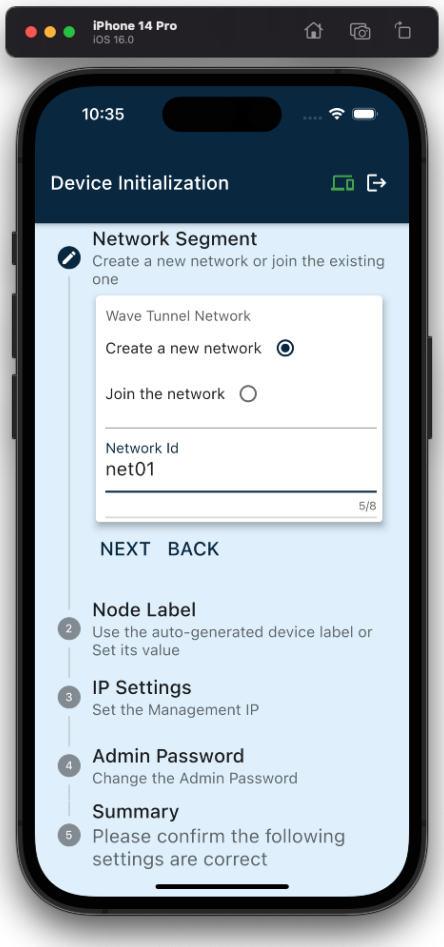
The “AirvineMobile” App is checking to see if it can reach the device via the selected Wi-Fi SSID. If the mobile App can reach the device, it will show the Initialization page.



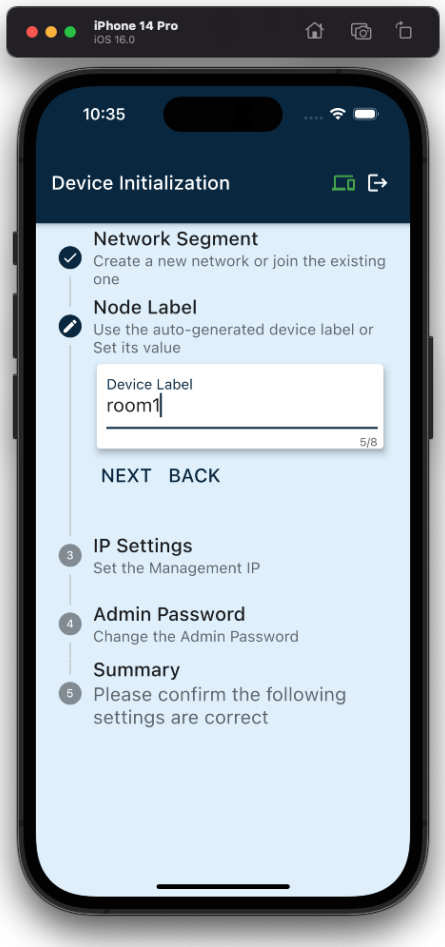
There are slight differences between the configurations of the root node and all other nodes. Please check the steps below.

Initializing the root device:

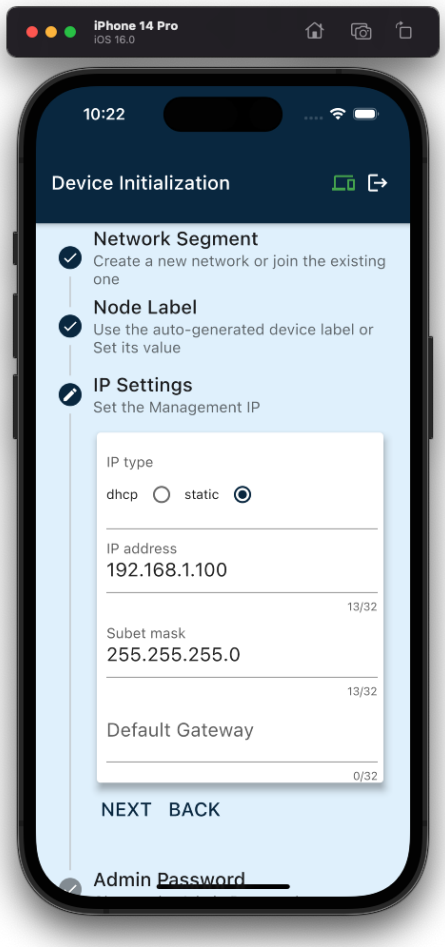
- To configure the root device, select the “Create a new network” option in the network segment step.
- Then input the Network ID for this new deployment. The Network ID can be automatically generated, or you can input any meaningful string for future identification of your network, for example.
  “net01”.
- Click “NEXT” for the next setting.



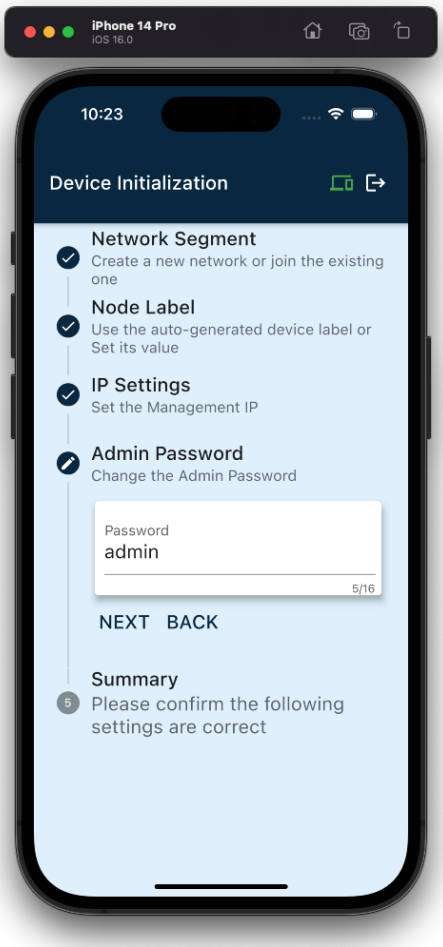
Input the “Device Label” for this device. It will be used to recognize your device later.



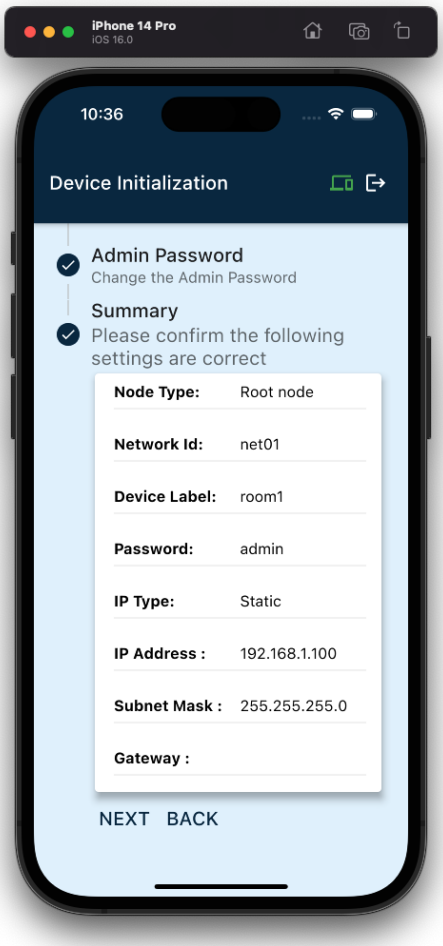
Click “Next” to set the management IP of your device.



Click “Next” to change the admin password of your device.



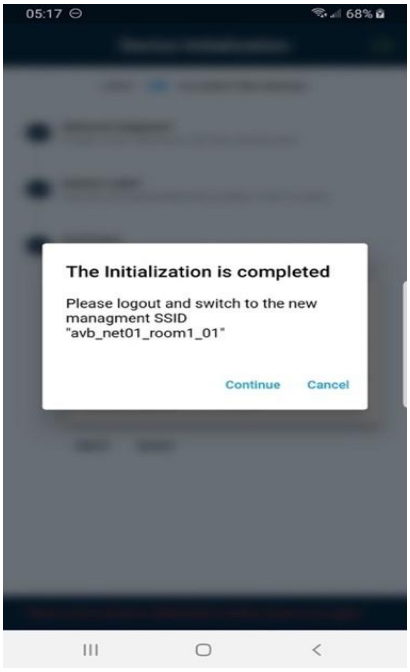
Click “Next” to check the summary of your configurations.



Once you confirm the configurations are correct, click “Next” to initialize the settings for this device.

When the initialization is completed, the popup window appears. Click “Continue” to finish the settings.

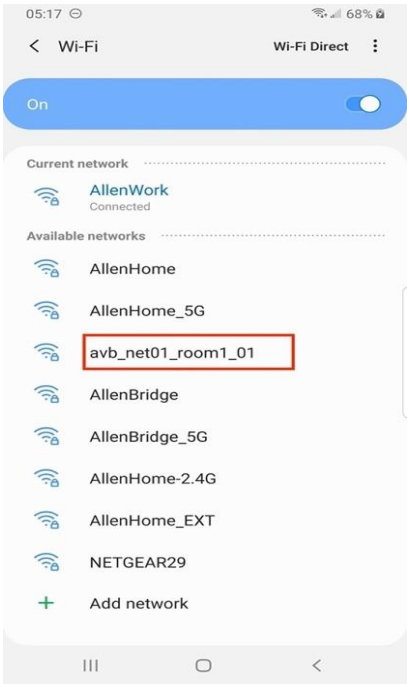
Note: the format of the management SSID for the WaveTunnel node has changed to a combination of **avb_[network Id]_[device label].**



The “Select Device Network” page will be shown to you after completing the initialization step.

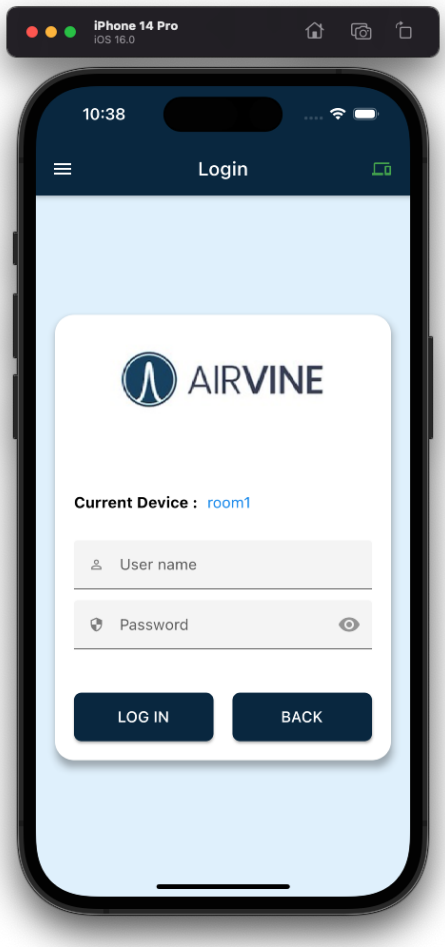
Click on “Select Wi-FI” to switch to the newly configured management SSID “avb_net01_room1”.

The management SSID changes after completing the initialization process from a default SSID to an SSID based on network Id and node label.



Click “Connect” to go to the Login page.

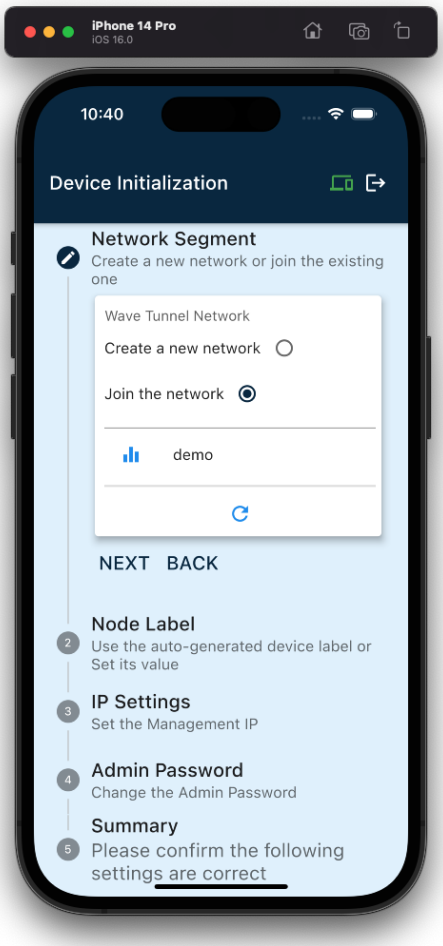
The root device has now been configured successfully. You can use the default username and password to login into the mobile App management pages.



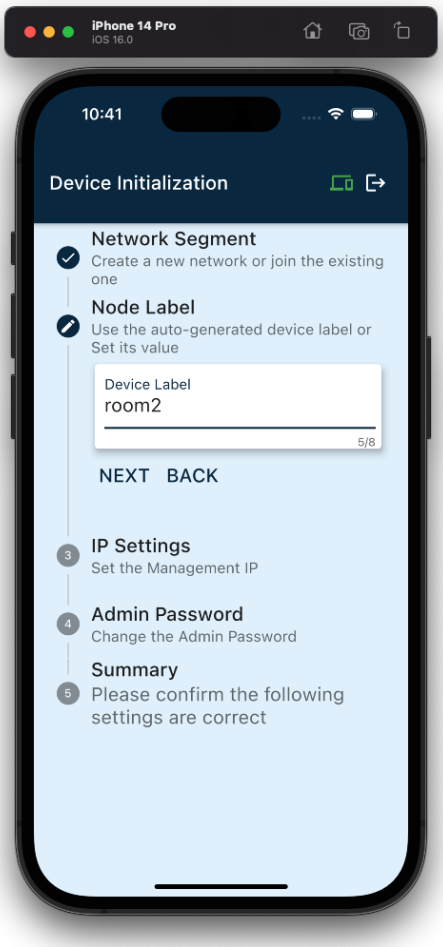
To configure the remaining devices in the network, select the “Join the network” option in the network segment step.

Nearby WaveTunnel devices will be broadcasting their SSIDs, which will appear in the list. Click on the SSID of the next node to be configured. This is the node that will talk to the root node that was just configured. Then click “next” for next settings.

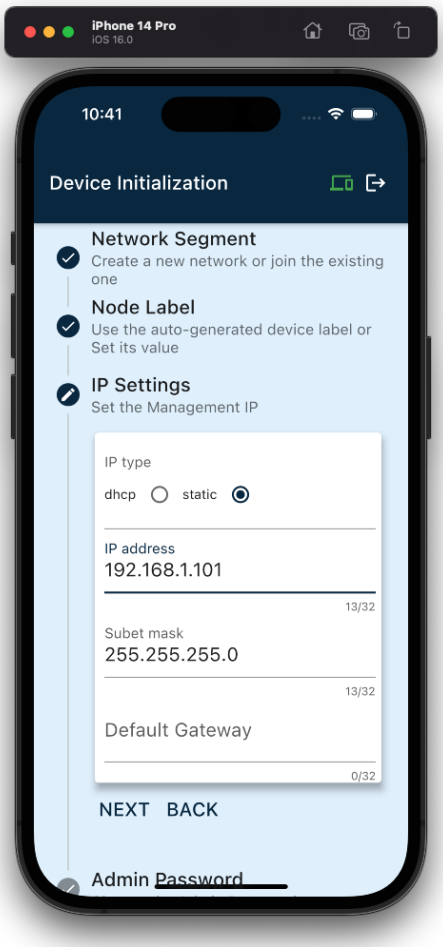
As each node is added to the network, traffic flows are automatically configured between that node and the root node. These flows can pass through relay nodes, but all traffic must flow to and from the root node.



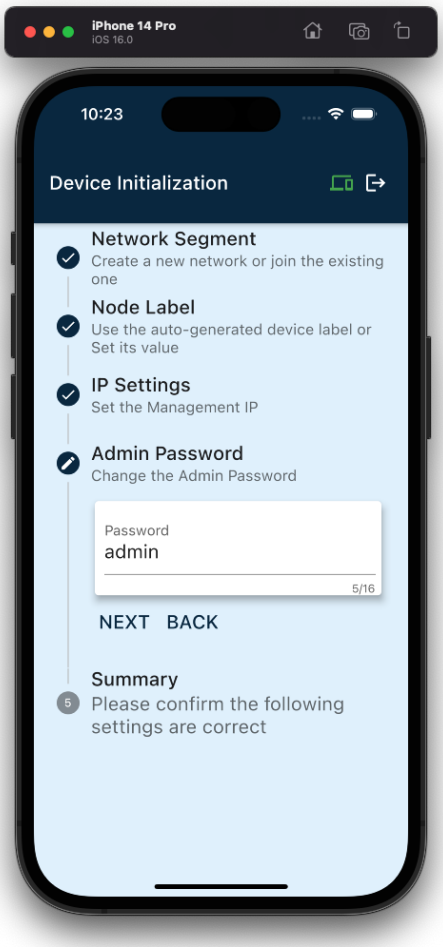
Enter the "Device Label" for this device. Your device can be recognized later using this information.



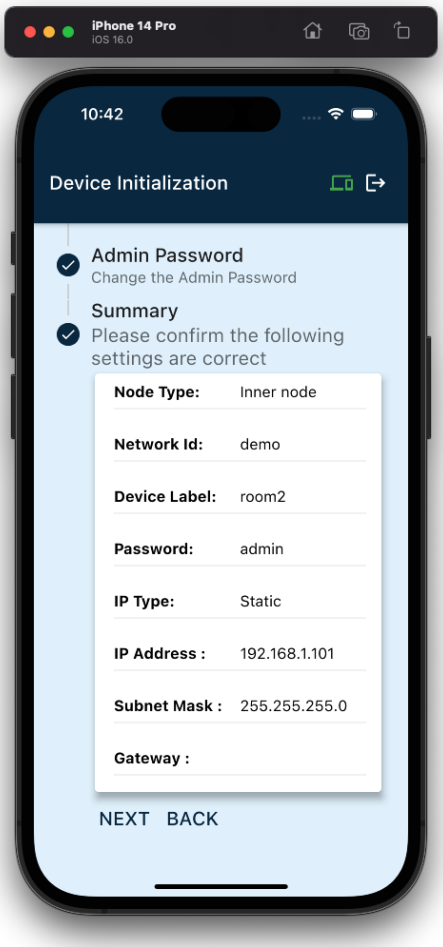
Click “Next” to set the management IP of your device.



Click “Next” to change the admin password of your device.

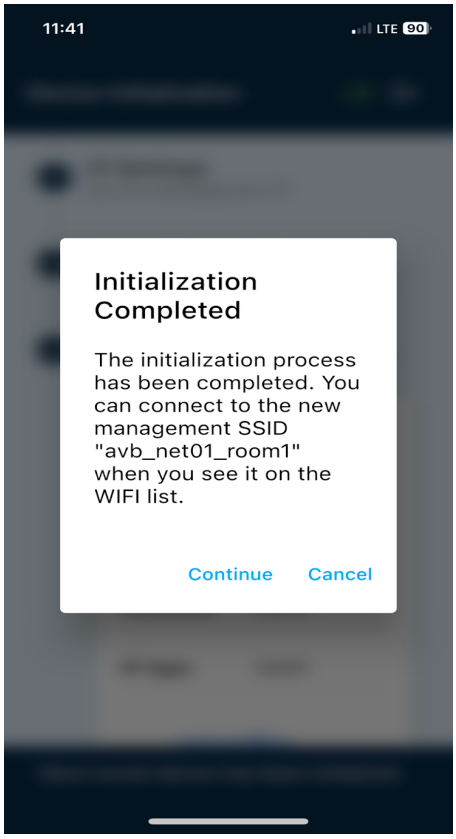


Click “Next” to check the summary of your configurations.

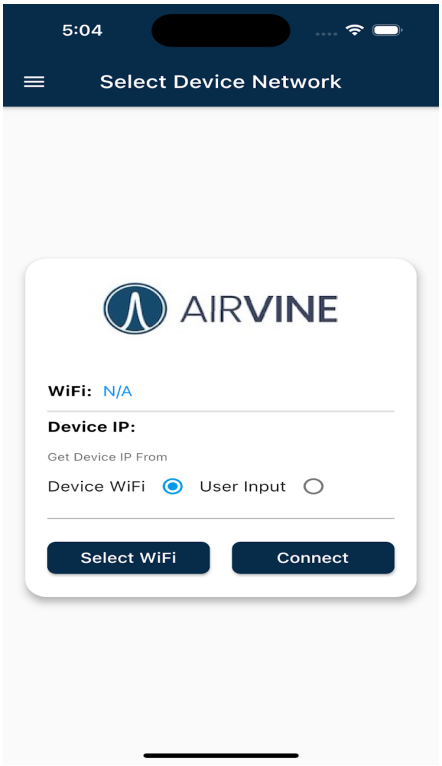


Once you confirm the configurations are correct, click “Next” to initialize the WaveTunnel settings for this device. When the initialization is completed, the popup window appears. Click “Continue” to finish the settings.

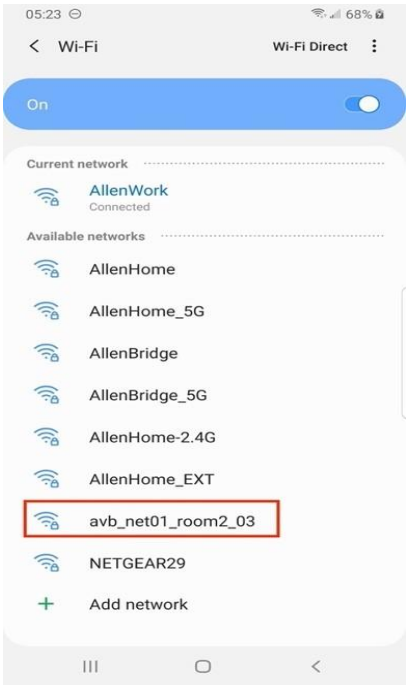
The format of the management SSID is now a combination of **avb_[network Id]_[device label].**

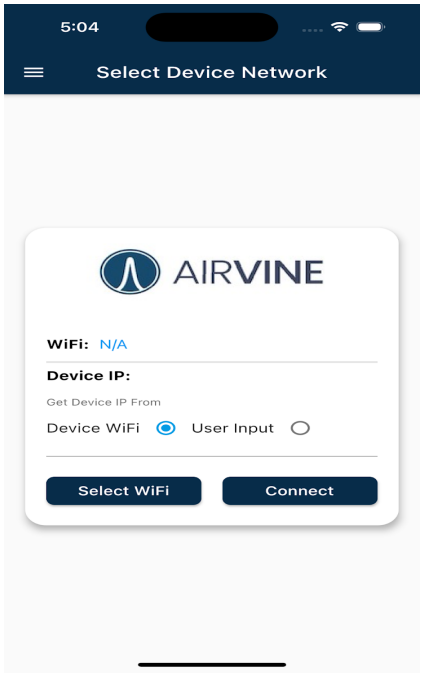


The “Select Device Network” page will be shown for you to switch the New Management SSID.

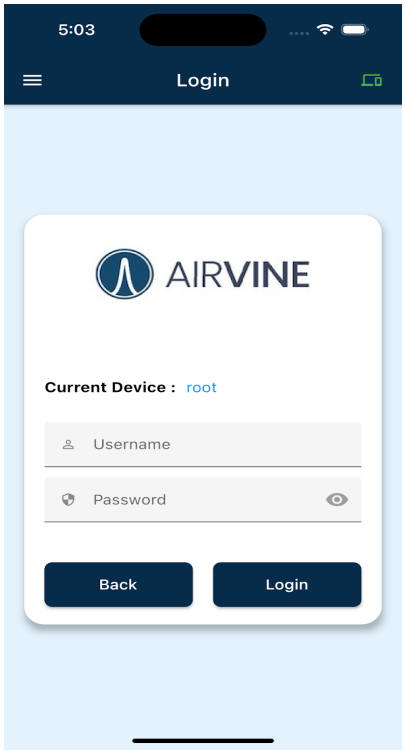


Click “Select Wi-FI” to switch to the newly configured management SSID “avb_net01_room2”.

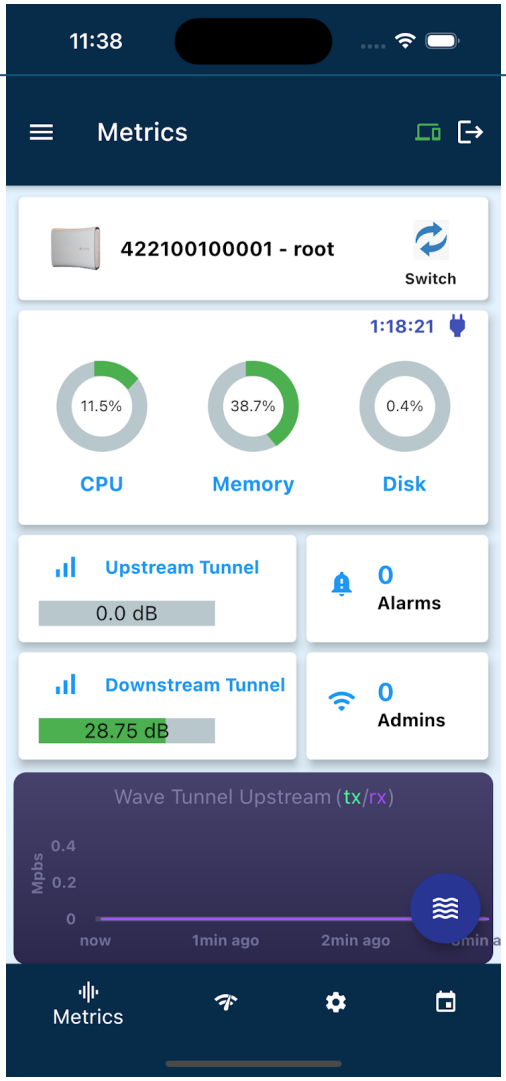




Click “Connect” to go to the Login page



This device is configured successfully. You can use the default username and password to login the mobile App management page. You will see the tunnel connection is established on the dashboard page.



Manage the WaveTunnel device firmwares

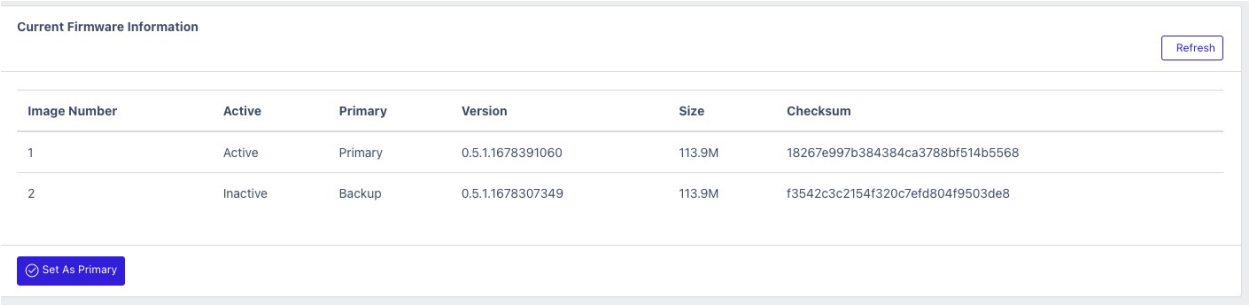
Check the current firmware information

There are two image banks in the WaveTunnel device which allow us to load two firmware image files. But only one image is active and the other is the backup. This gives us the capability to update the image to the back bank first without impacting the service. Also, we can revert back to the previous if the new firmware is not running well.

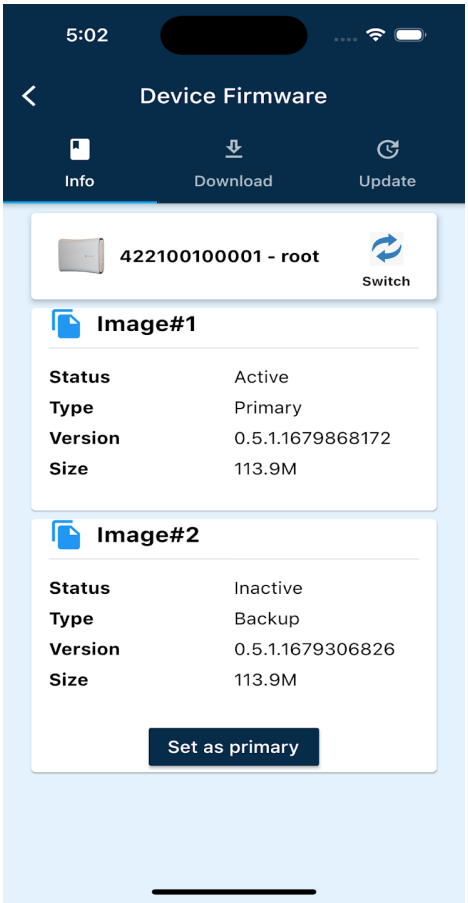
The Firmware information page shows the following information.

Active status, Is Primary or backup image, Firmware version , Size, checksum.

[WEB GUI]
Operation -> Firmware Update



[Mobile App]
Settings -> Firmware -> Info



[CLI]
Firmware -> info

```
AVS# firmware
AVS(firmware)#

Help:
          info - Show the current firmware status
      download - Download the firmware file from the configured server
         write - Write the firmware file into image bank
       primary - Set the firmware image as primary
          file - Sub menu to manage the firmware file
        server - Sub menu to configure the firmware file servers
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(firmware)# info


Current firmware info:
```

Image number	Active	Primary	Version	Size	Checksum
1	Active	Primary	0.5.1.1678391060	113.9M	18267e997b384384ca3788bf514b5568
2	Inactive	Backup	0.5.1.1678307349	113.9M	f3542c3c2154f320c7efd804f9503de8

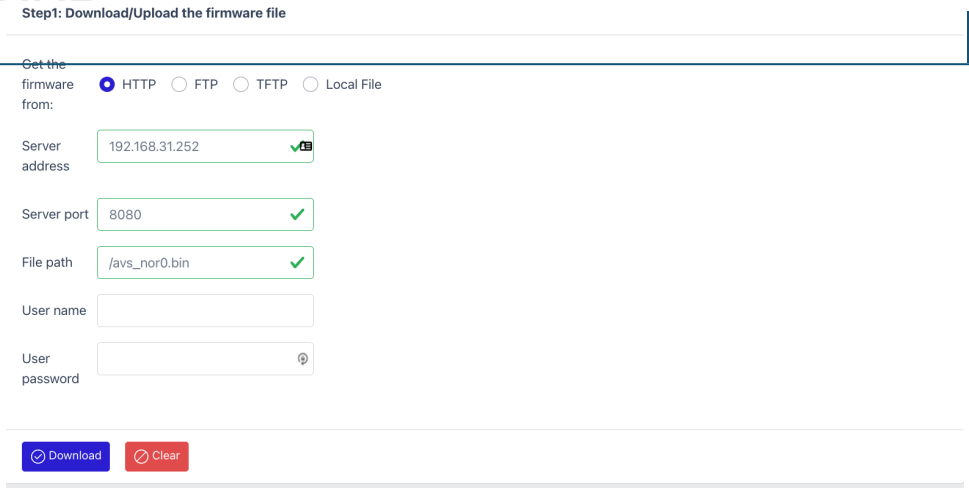
```
AVS(firmware)#
```

Upload/Download the firmware file to the device

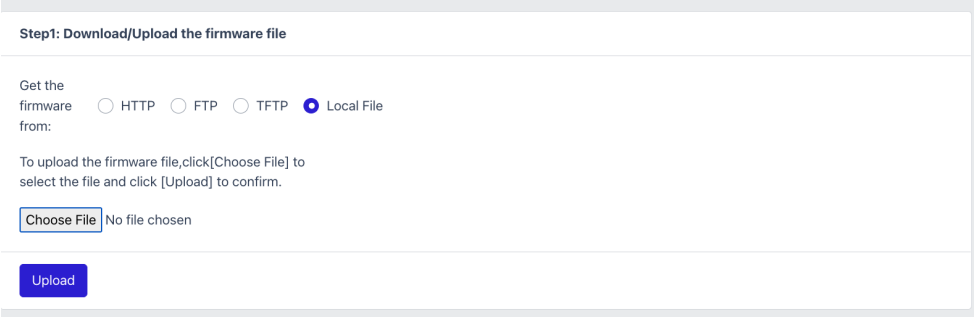
There are two mechanisms you can get the firmware image file to be loaded into your WaveTunnel device. You can set up the Http,FTP or TFPF server and put the image file on it. Then, you can download the image file from the server through WEB GUI, Mobile App or CLI to your device. Or you can directly upload the firmware image file from your local laptop through the WEB GUI to the device.

For the download mechanism, you need to put the server address, server port , the file path of the image file, user name(optional),password(optional) before starting the download operation.

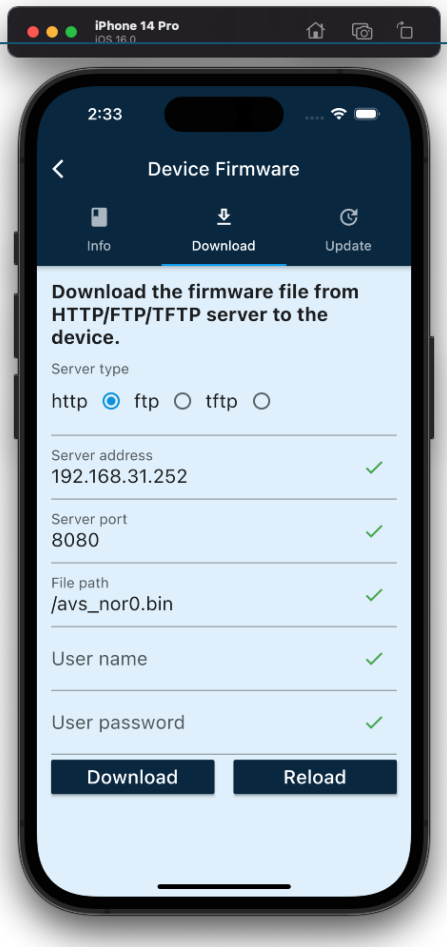
[WEB GUI]
Operation -> Firmware Update -> Step 1
Input the server setting and click “download” button



Select the firmware image file from your local laptop and then click “upload” button.



[Mobile App]
Settings -> Firmware -> Download
Input the server setting and click download button



[CLI]
Firmware - > Server

Input the server configurations in this category.

```
ssh admin@10.16.113.10
AVS(firmware-server)#

Help:
            ll - List the firmware server setting
           set - Set the attribute of the firmware file servers
          save - Save the changed attributes of the file servers
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(firmware-server)# ll

Firmware file server settings
```

Description	Attribute Name	Current Value
Server type	serverType	HTTP
HTTP server address	httpServer	192.168.31.252
HTTP server port	httpPort	8080
HTTP remote image path	httpPath	/avs_nor0.bin
HTTP server user name	httpUser	
HTTP server user password	httpPassword	
FTP server address	ftpServer	192.168.31.252
FTP server port	ftpPort	21
FTP remote image path	ftpPath	/avs_nor0.bin
FTP server user name	ftpUser	
FTP server user password	ftpPassword	
TFTP server address	tftpServer	192.168.31.252
TFTP server port	tftpPort	69
TFTP remote image path	tftpPath	/avs_nor0.bin

Firmware -> download

Input the “download” command to download the file

```
ssh admin@10.16.113.10
AVS(firmware-server)# ..
AVS(firmware)# ll
Unknown Command: ll

Help:
          info - Show the current firmware status
      download - Download the firmware file from the configured server
         write - Write the firmware file into image bank
       primary - Set the firmware image as primary
          file - Sub menu to manage the firmware file
        server - Sub menu to configure the firmware file servers


AVS(firmware)# download
```

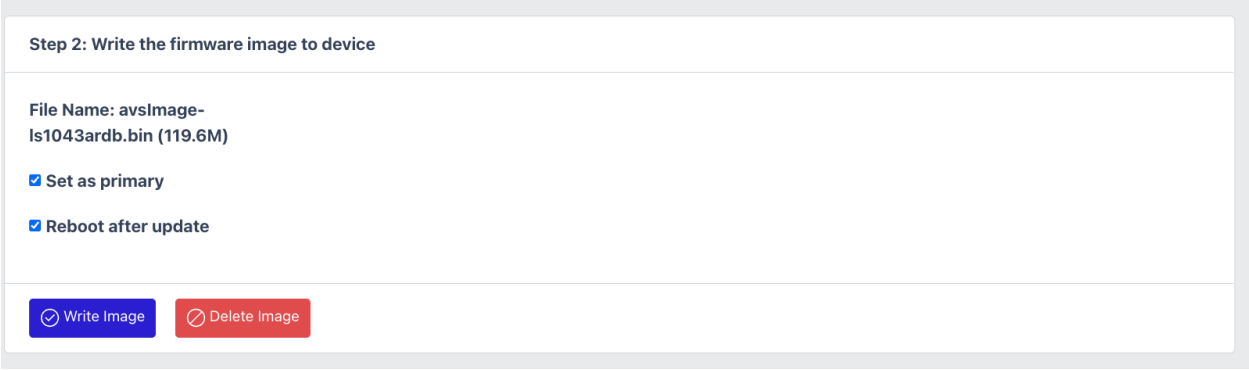
Update the firmware

Once the firmware image file is downloaded or uploaded to the WaveTunnel device. You can see the image file name on the page. Clicking the “Write image” button to update the firmware to the WaveTunnel device. Clicking the “Delete image” button to discard the uploaded image.

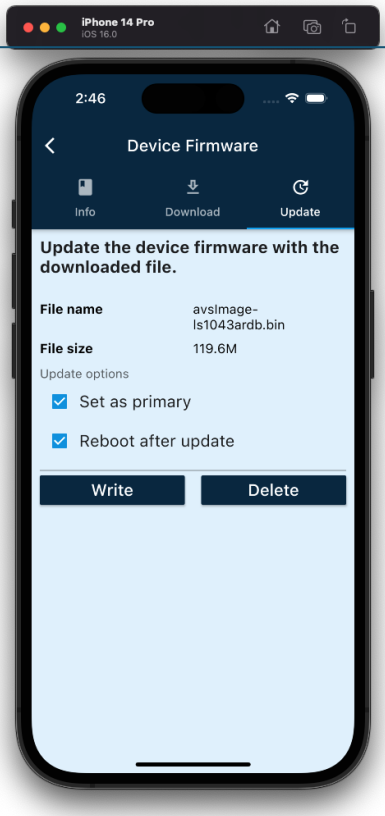
There are two options on the update page.

[Set as primary] => The updated image will set to primary after system reboot
[Reboot after update] => The WaveTunnel will be rebooted automatically after the firmware update operation. Un-selected it to delay the reboot if you want to do it later. But the image will only take effect after the system reboot with the primary flag set.

[WEB GUI]
Operation -> Firmware Update -> Step 2



[Mobile App]
Settings -> Firmware -> Update



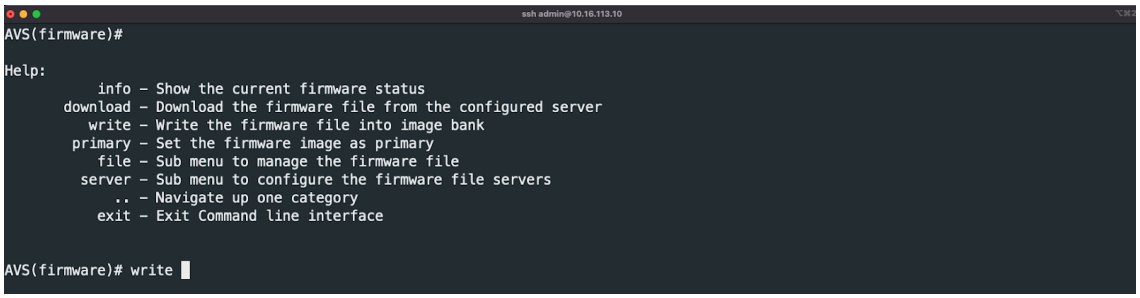
[CLI]
Firmware -> File -> Info

To check if the firmware image file exists or not.

```
AVS(firmware)#

Help:
          info - Show the current firmware status
      download - Download the firmware file from the configured server
         write - Write the firmware file into image bank
       primary - Set the firmware image as primary
          file - Sub menu to manage the firmware file
        server - Sub menu to configure the firmware file servers
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(firmware)# file
AVS(firmware-file)#

Help:
          info - Show information of the downloaded firmware file
        verify - Verify the the downloaded firmware file
        delete - Delete the downloaded firmware file
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(firmware-file)# info

Available firmware image file:
| Name                  | Size   |
|-----------------------|--------|
| avsImage-ls1043ardb.bin | 119.6M |

AVS(firmware-file)#
```

Firmware - > Write

Type “write” command to trigger the firmware update operation.



Configure the WaveTunnel device

Once the Wave tunnel connections are established,you should not change the setting in most scenarios. But if you do need to modify the configuration,here are the pages for you to do it.

Update the WaveTunnel Configurations

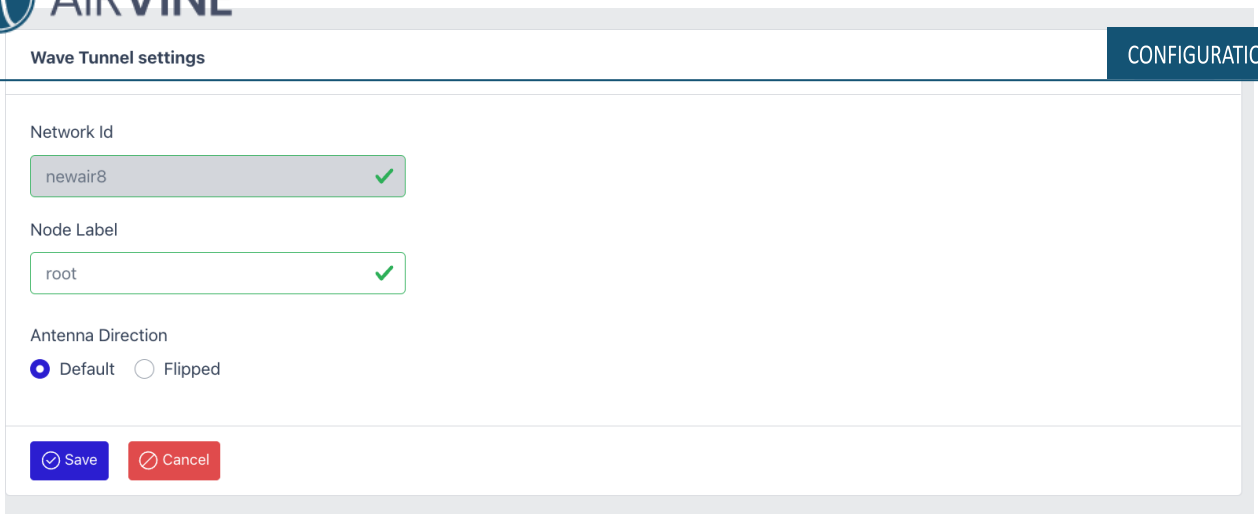
General WaveTunnel settings

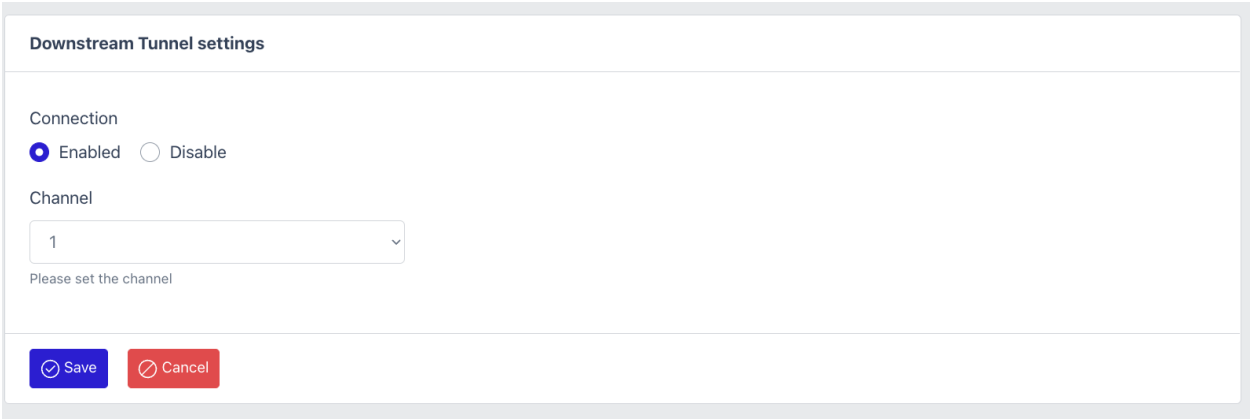
The General Node settings,you can change the label and the antenna direction. For the antenna direction, you will need to adjust the position of the nodes after you make the changes. We suggest you not change it if there is no strong requirement.

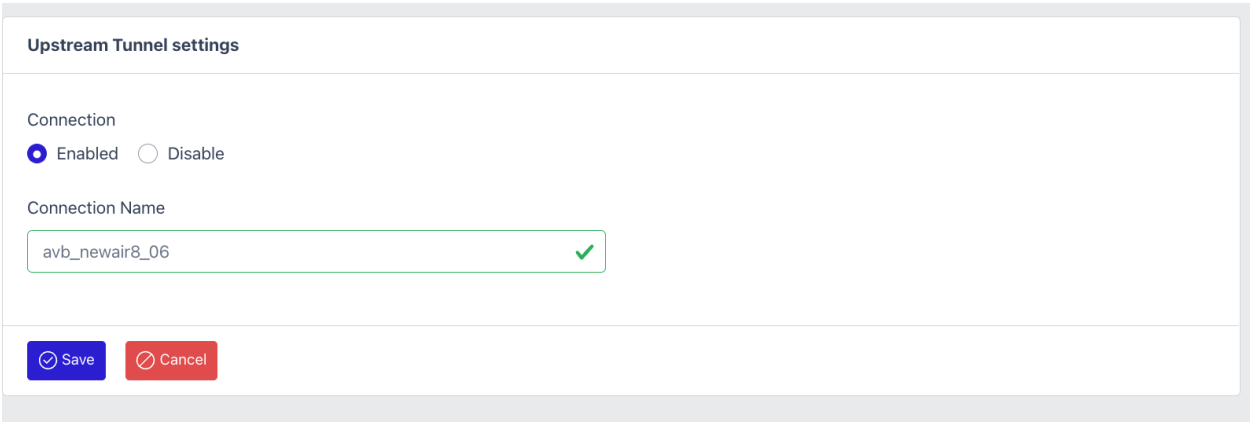
The Downstream tunnel settings.
You can enable/disable the downstream connection or change the channel value. If you disable the connection,it will cause the connection to be lost in the network. We suggest disable only when there is no downstream node connected. For the channel setting,please ensure the channel setting is not identical to the neighboring device to avoid the interference.

The Upstream tunnel settings.
You can enable/disable the upstream connection or change the connection name. If you disable the connection,it will cause the connection to be lost in the network. We suggest disable only when there is no upstream node connected or you want to switch the upstream connection to another device.

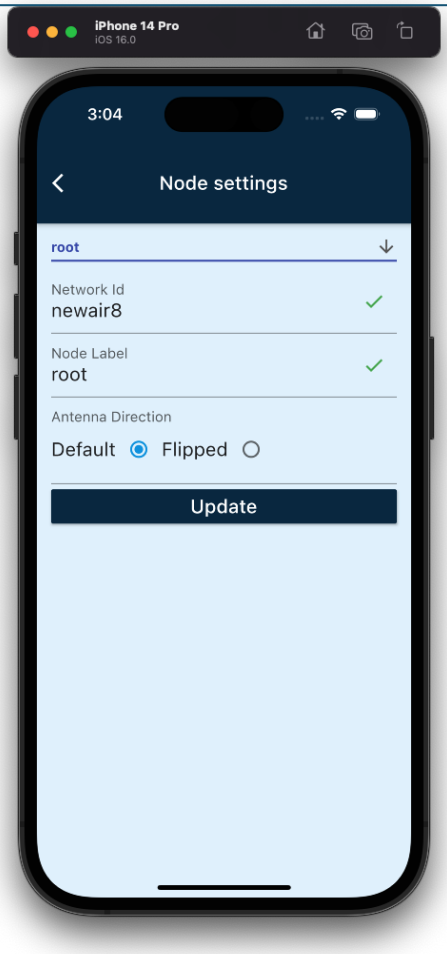
[WEB GUI]
Configuration -> Network -> Wave Tunnel



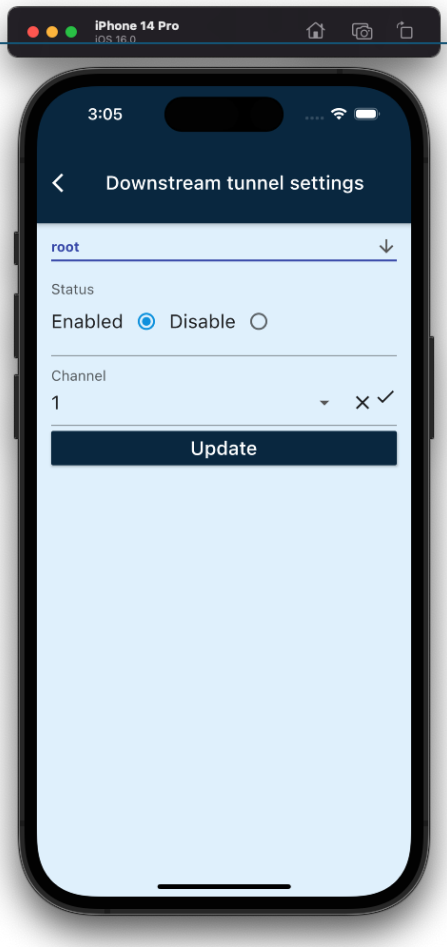




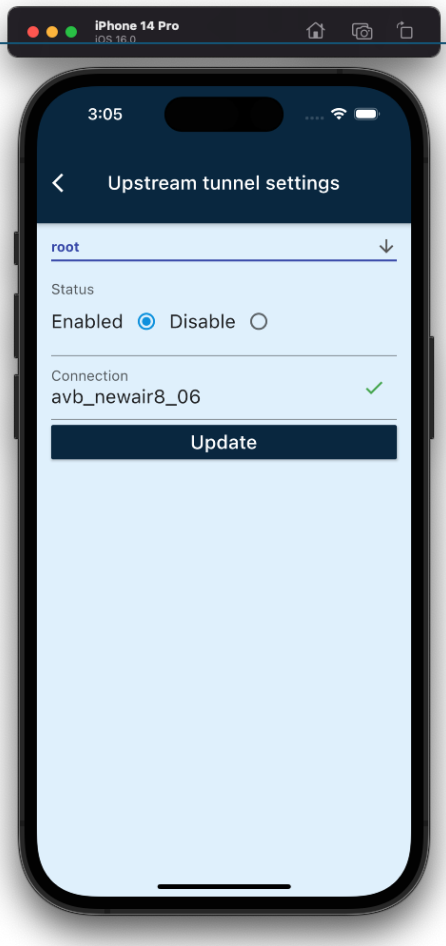
[Mobile App]
Settings -> Wave Tunnel settings



Settings -> Downstream Tunnel settings



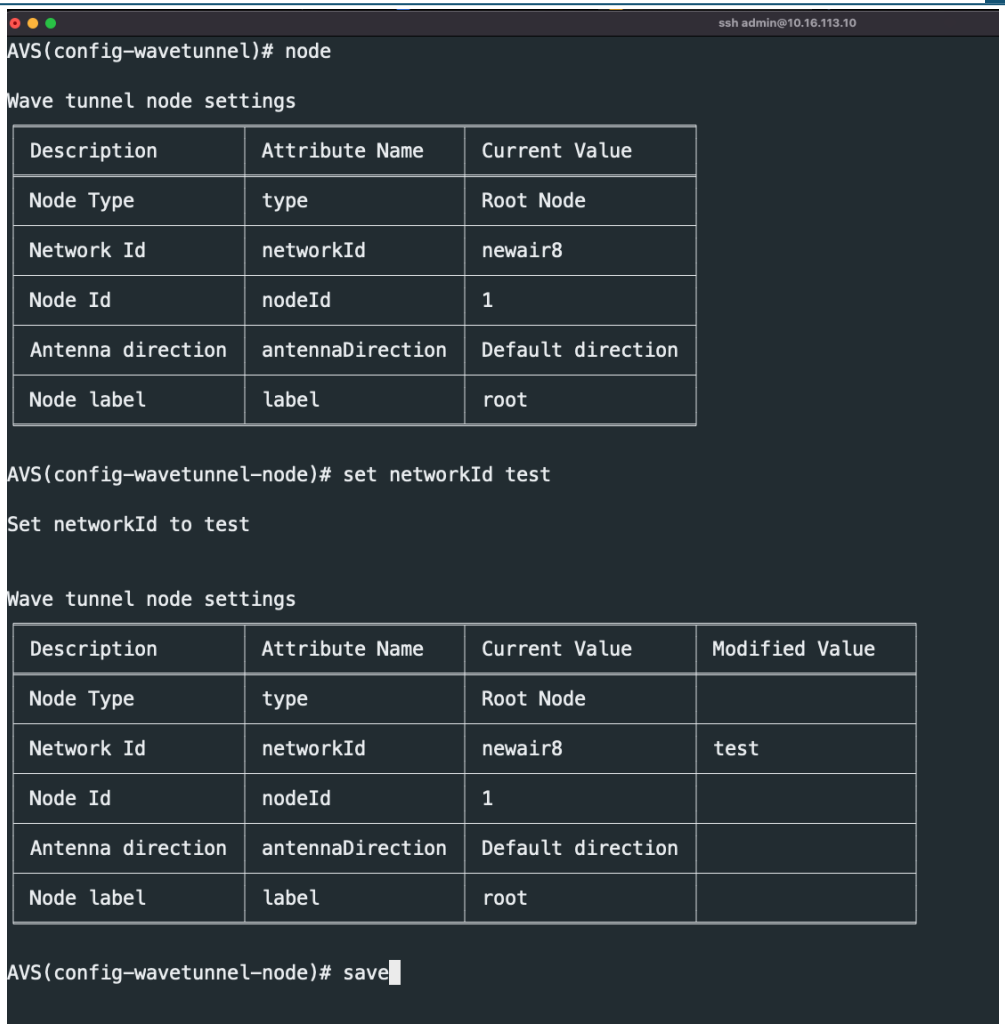
Settings -> Upstream Tunnel settings



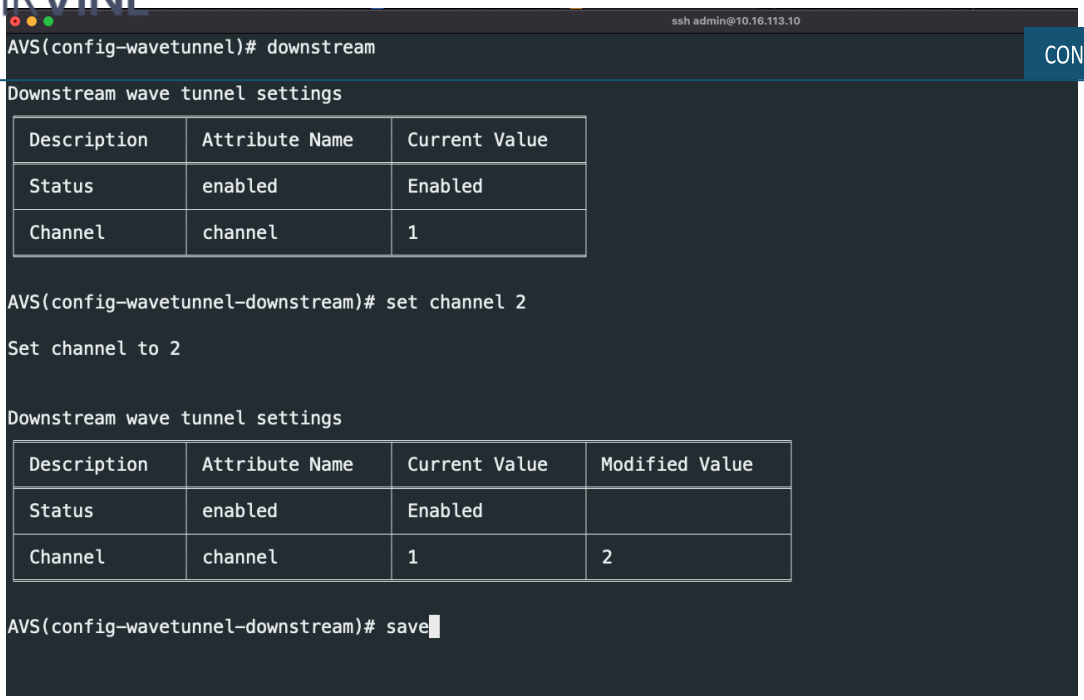
[CLI]
config -> wavetunnel

```
AVS(config)#

Help:
        device - Sub menu to configure the device settings
      ethernet - Sub menu to configure the ethernet settings
    wavetunnel - Sub menu to configure the wave tunnel settings
          wifi - Sub menu to configure the management WIFI settings
       persist - Save the running configuration permanently
      autoSave - Set if persist the running configuraitons automatically
          user - Sub menu to configure the User settings
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(config)# wavetunnel
AVS(config-wavetunnel)#

Help:
    downstream - Configure the downstream wave tunnel settings
          node - Configure the wave tunnel node settings
      upstream - Configure the upstream wave tunnel settings
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(config-wavetunnel)#
```

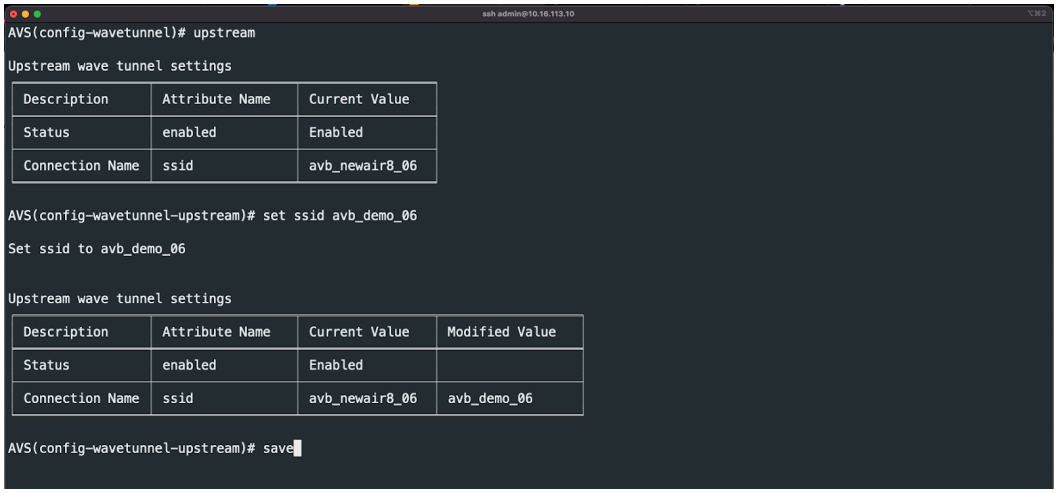
config -> wavetunnel -> node



config -> wavetunnel -> downstream



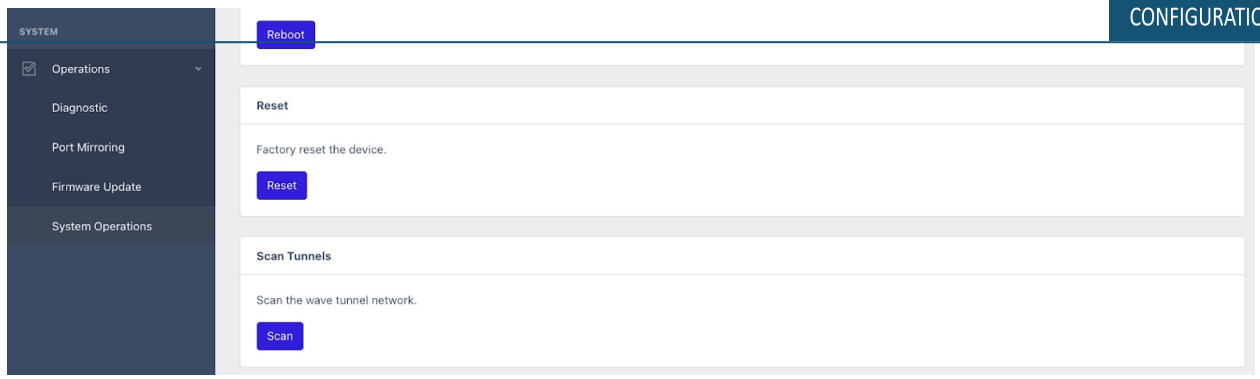
config -> wavetunnel -> upstream



Scan the WaveTunnel network

If there is a WaveTunnel device removed from the network or you are seeing the abnormal network diagram on the WEB GUI, you can use the “Scan Tunnel” to clean up the cache data of network devices. It will retrieve the information from each node in the network and reflect the changes of your network.

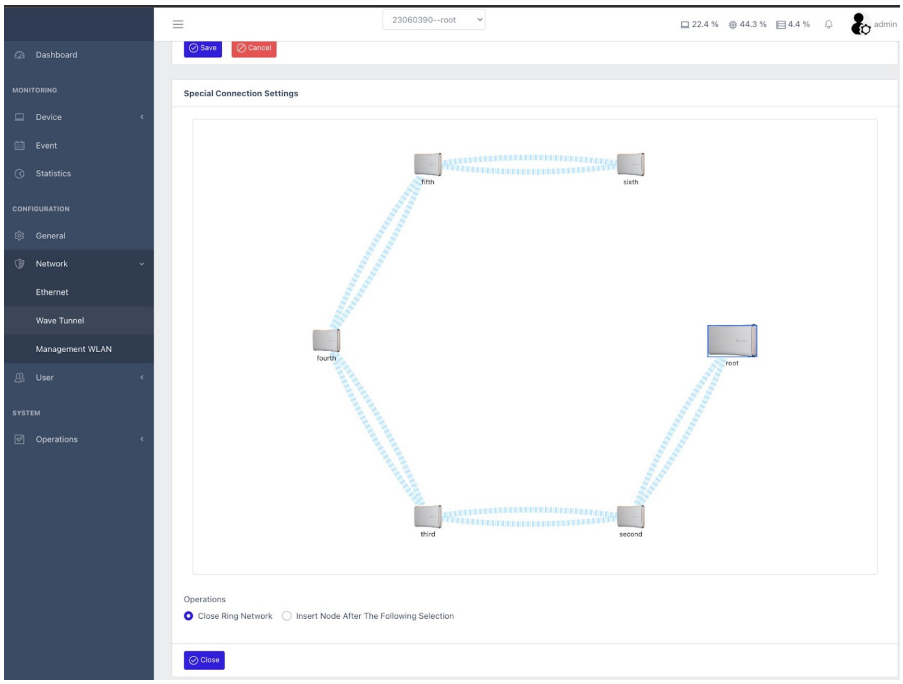
System -> System Operations-> Scan Tunnel

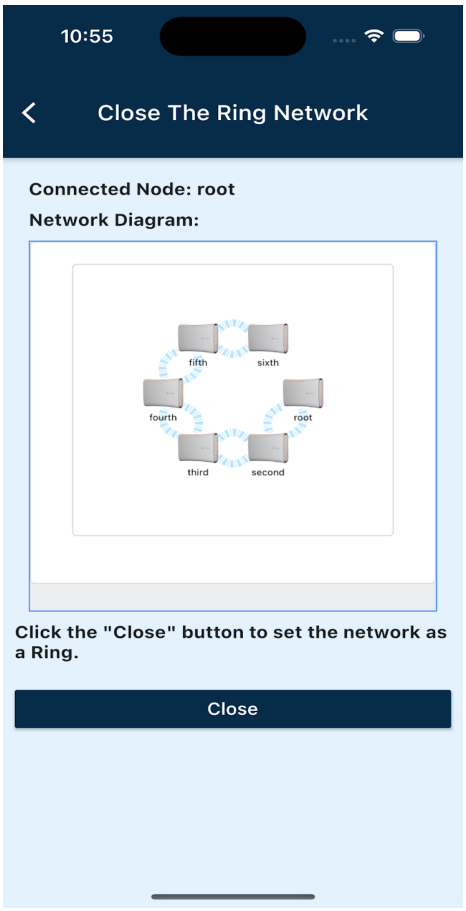


Close the Ring Network

WaveTunnel devices are configured in order (from root to leaf).. If you want to form a ring network to support the redundancy. You can use this function to close the ring network. The configuration is to set the root node point to the end leaf node. You can either do it from WEB GUI or Mobile App.

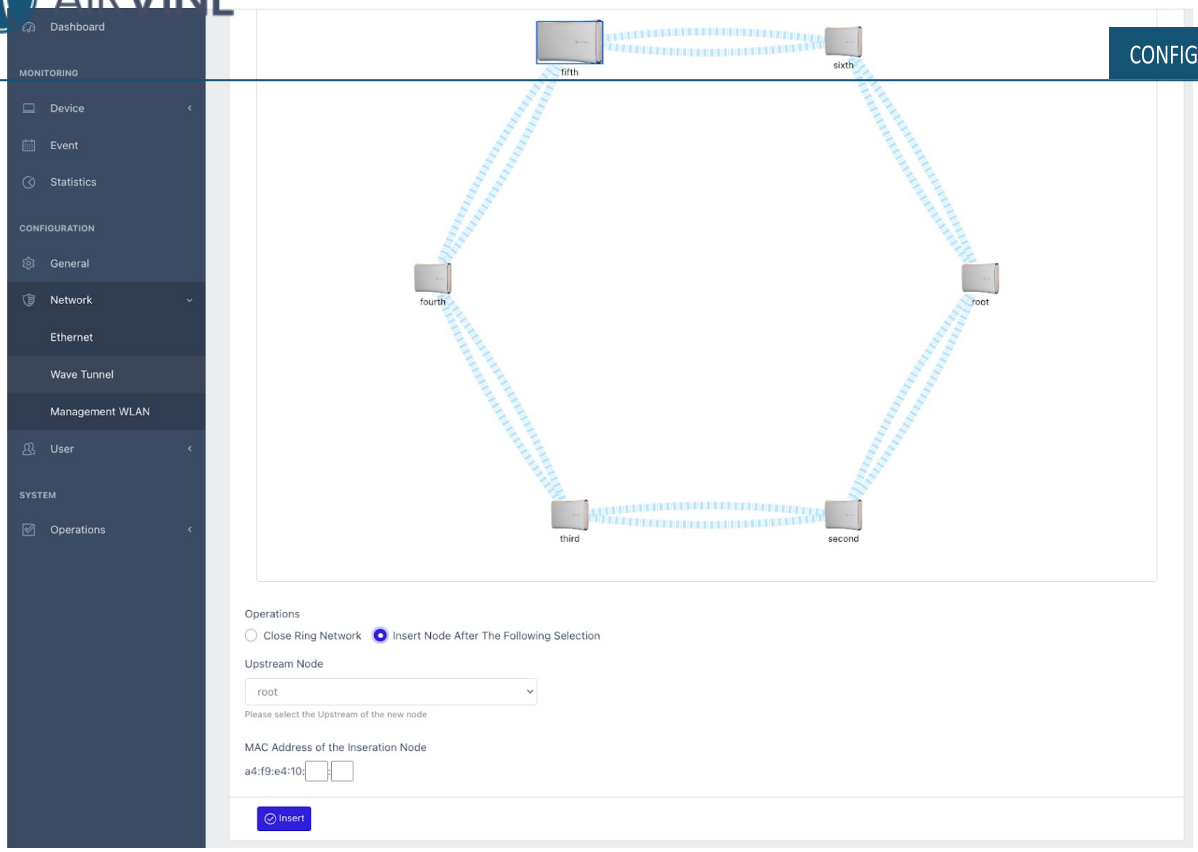
[WEB GUI]
Configuration -> Network -> Wave Tunnel

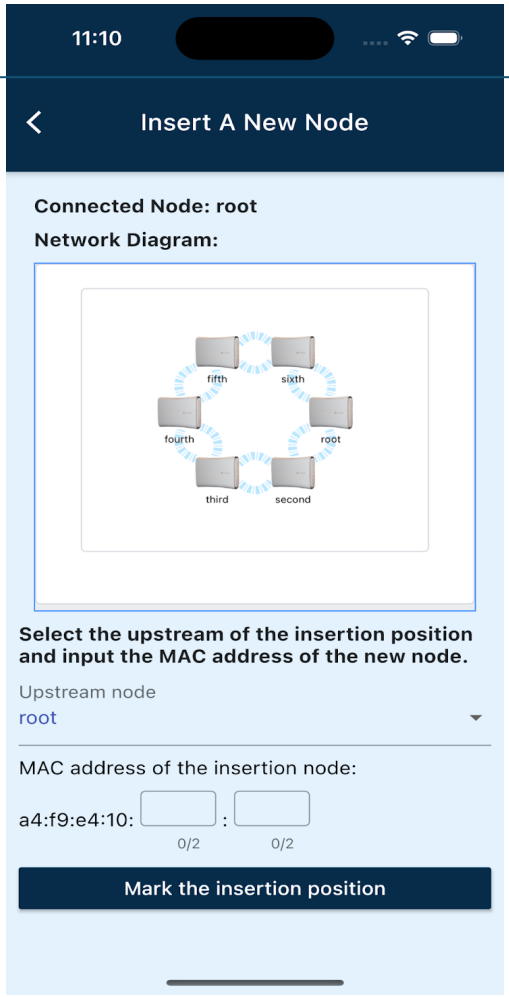




Insert a WaveTunnel Device to the Network

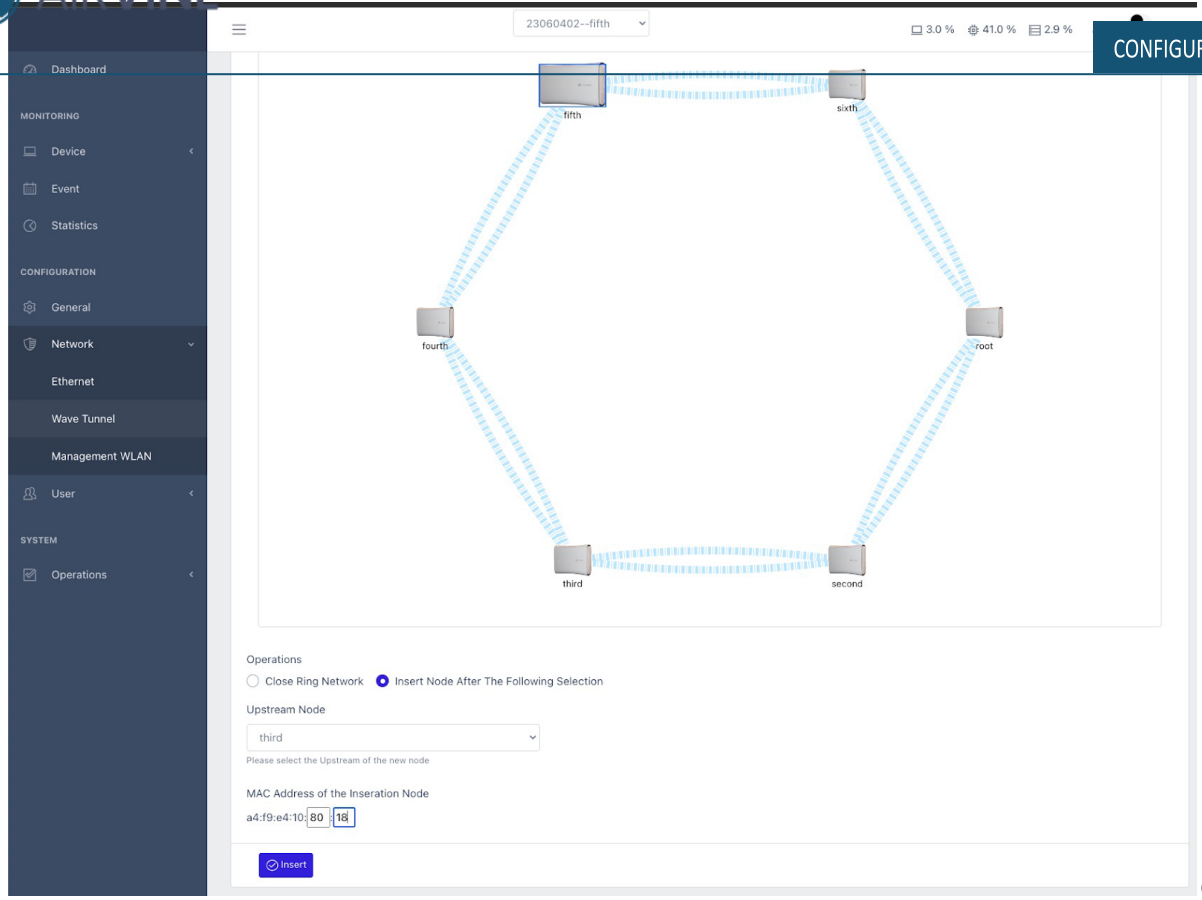
WaveTunnel devices are configured in order (from root to leaf). The function can be used to finish the setup if you need to install a new WaveTunnel device in the position of an existing network.


Dashboard
MONITORING
Device
Event
Statistics
CONFIGURATION
General
Network
Ethernet
Wave Tunnel
Management WLAN
User
SYSTEM
Operations
fifth
sixth
fourth
root
third
second
Operations
Close Ring Network
Insert Node After The Following Selection
Upstream Node
root
Please select the Upstream of the new node
MAC Address of the Inseration Node
a4:f9:e4:10:
Insert



There are two steps to finish the insertion. Let's take the above network as an example for inserting a device between node third and node fourth.

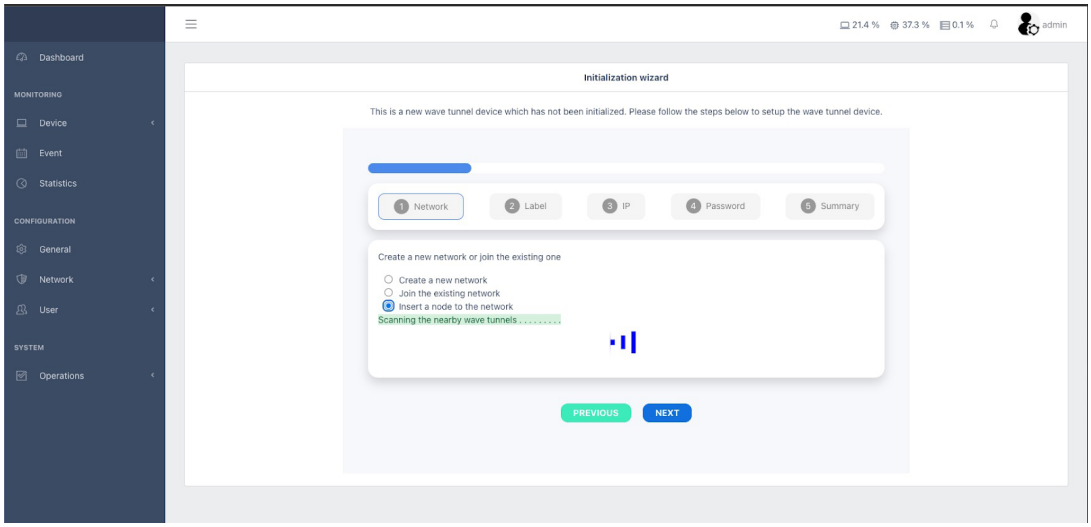
Step 1: Mark the insertion position
Connect to any device in the existing network. Select node "third" as the upstream node and input the MAC address of the new node which is planned to be inserted.

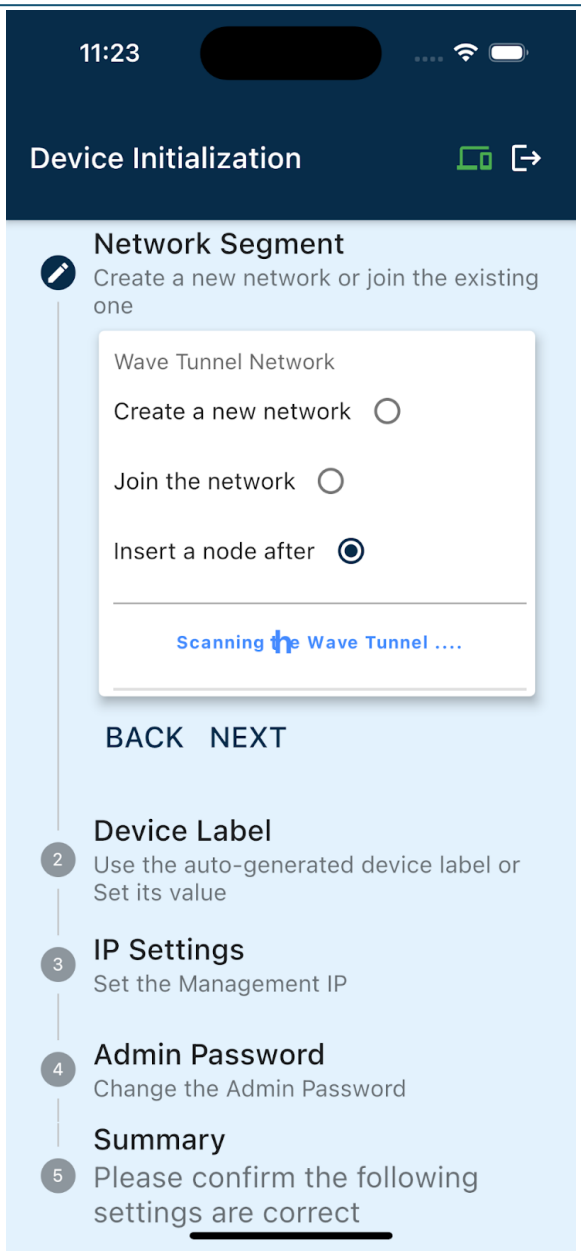


d

Step 2: join the new WaveTunnel device to the network

Use WEB GUI or Mobile to connect to the new WaveTunnel device. In the setup wizard, select the option “Insert a node into the network”. Following the steps of the setup wizard to finish the initialization of the new device. Once finished, you can see the new node is inserted into the position specified in step 1.





Note: You need to finish step (2) within 30 minutes after step(1). Otherwise, the settings in step (1) will be rollback. This design is to avoid the service impact of the WaveTunnel disconnection.

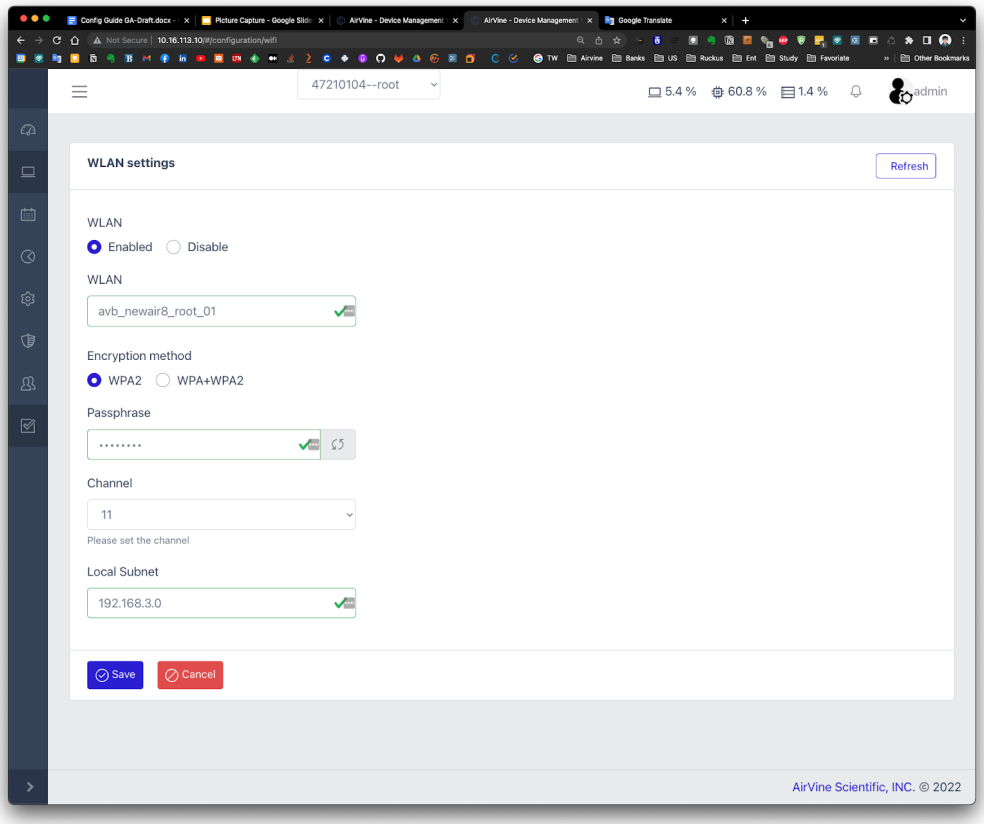
Update the Management WLAN

The management WLAN is mainly for the management purposes. You can change the settings according to your need. For example, you can disable the WLAN or change the default passphrase after the wave tunnel initialization for security considerations.

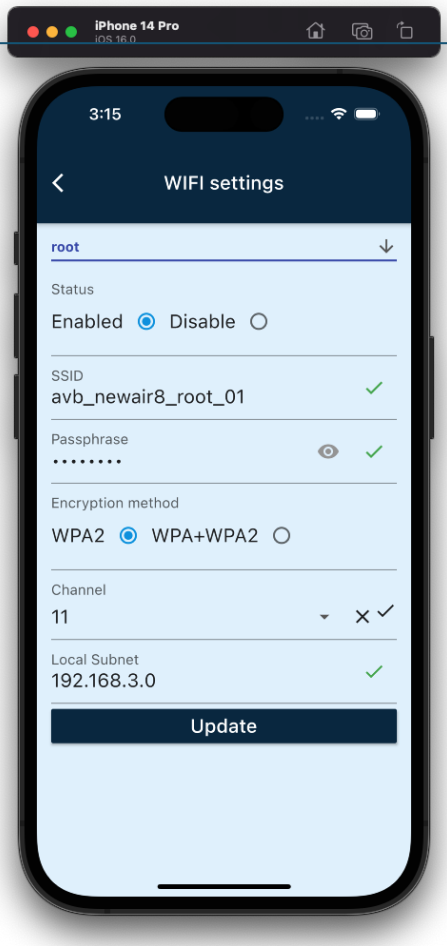
There are several attribute values you can change on this page. It includes enabled/d
SSID name,encryption method, passphrase, channel and local subnet.

[WEB GUI]

Configuration -> Network -> Management WLAN



[Mobile App]
Settings -> WIFI settings



[CLI]
config -> wifi

ssh admin@10.16.113.10

```
AVS(config)#

Help:
        device - Sub menu to configure the device settings
      ethernet - Sub menu to configure the ethernet settings
    wavetunnel - Sub menu to configure the wave tunnel settings
          wifi - Sub menu to configure the management WIFI settings
       persist - Save the running configuration permanently
      autoSave - Set if persist the running configuraitons automatically
          user - Sub menu to configure the User settings
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(config)# wifi

Management WIFI settings
```

Description	Attribute Name	Current Value
Connection	enabled	Enabled
SSID	name	avb_newair8_root_01
Encryption method	encryption	WPA2
Passphrase	passphrase	airvine!
Channel	channel	11
Local subnet	subnet	192.168.3.0

```
AVS(config-wifi)#
```

```
AVS(config-wifi)# ll

Management WIFI settings
```

Description	Attribute Name	Current Value
Connection	enabled	Enabled
SSID	name	avb_newair8_root_01
Encryption method	encryption	WPA2
Passphrase	passphrase	airvine!
Channel	channel	11
Local subnet	subnet	192.168.3.0

```
AVS(config-wifi)# set channel 1

Set channel to 1

Management WIFI settings
```

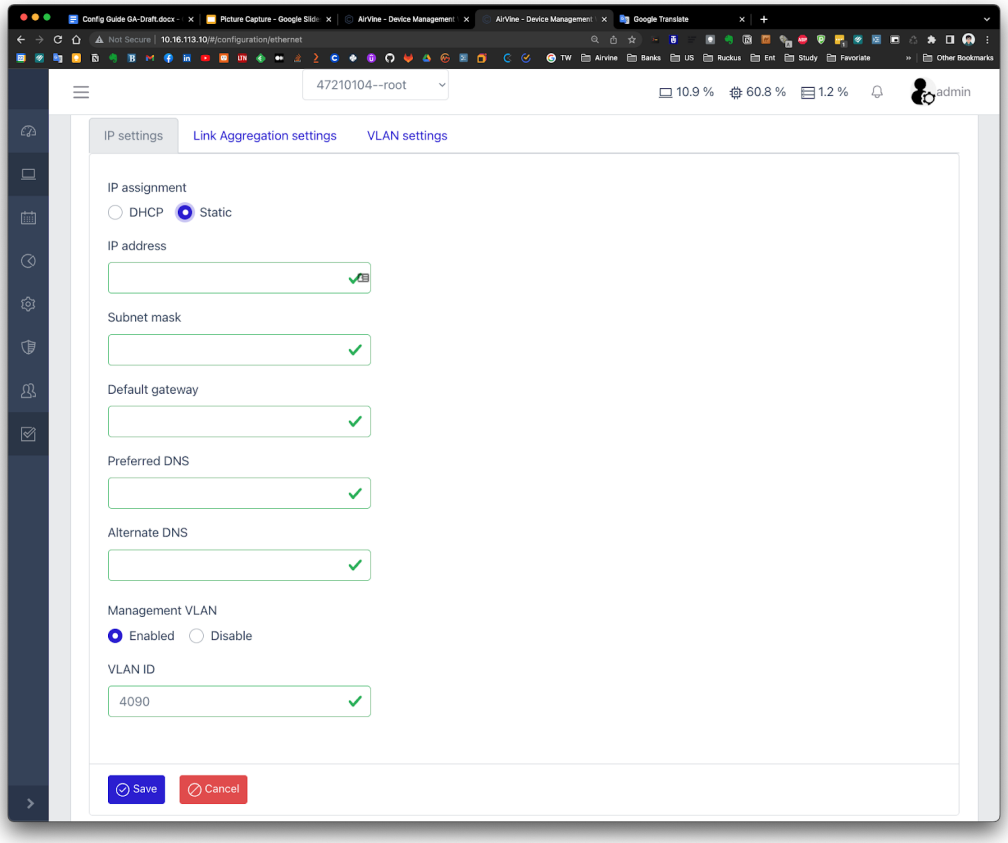
Description	Attribute Name	Current Value	Modified Value
Connection	enabled	Enabled	
SSID	name	avb_newair8_root_01	
Encryption method	encryption	WPA2	
Passphrase	passphrase	airvine!	
Channel	channel	11	1
Local subnet	subnet	192.168.3.0	

```
AVS(config-wifi)# save
```

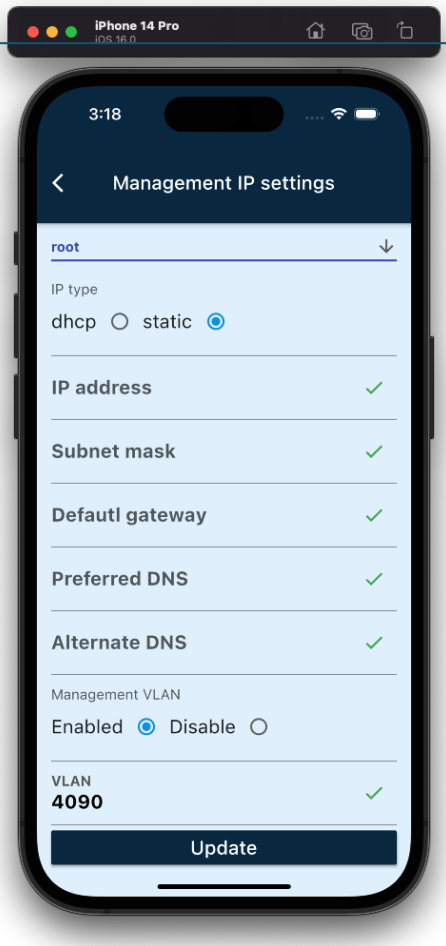
Management IP settings

You can configure the management IP of the WaveTunnel device on this page. It includes the type of IP assignment, IP address, subnet mask, default gateway and management VLAN.

[WEB GUI]
Configuration-> Network ->Ethernet ->IP settings



[Mobile App]
Settings-> Management

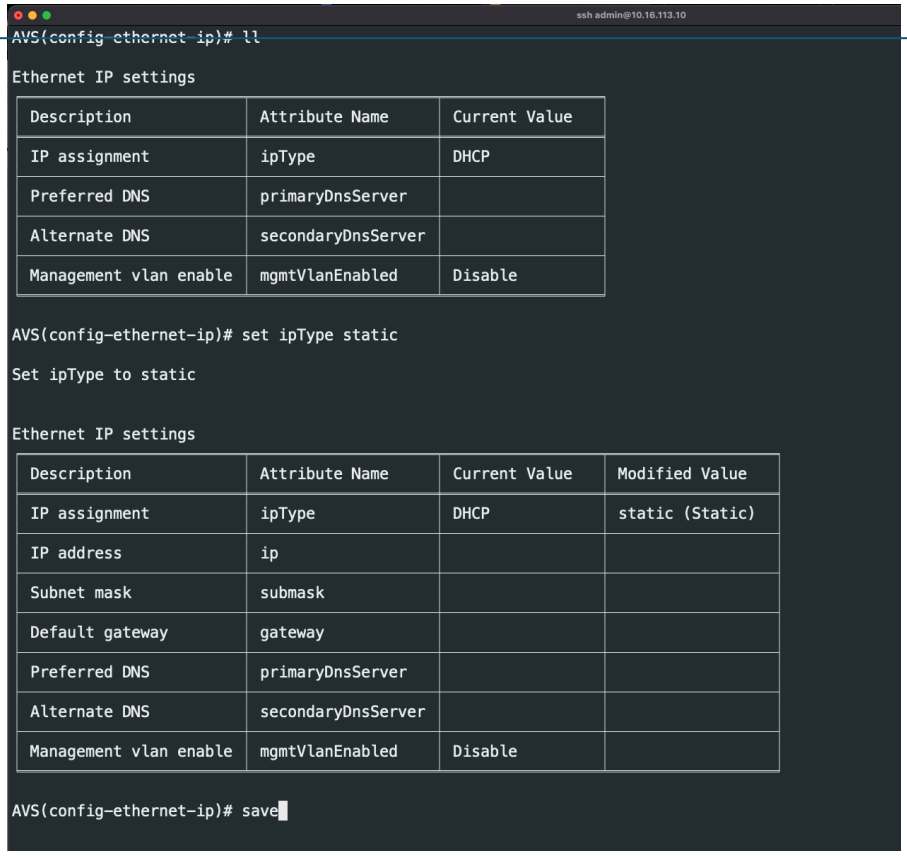


[CLI]
config ->ethernet-> management

```
AVS(config)#

Help:
        device - Sub menu to configure the device settings
      ethernet - Sub menu to configure the ethernet settings
    wavetunnel - Sub menu to configure the wave tunnel settings
          wifi - Sub menu to configure the management WIFI settings
       persist - Save the running configuration permanently
      autoSave - Set if persist the running configuraitons automatically
          user - Sub menu to configure the User settings
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(config)# ethernet
AVS(config-ethernet)# management

Ethernet IP settings
```

Description	Attribute Name	Current Value
IP assignment	ipType	DHCP
Preferred DNS	primaryDnsServer	
Alternate DNS	secondaryDnsServer	
Management vlan enable	mgmtVlanEnabled	Disable

```
AVS(config-ethernet-ip)#
```



ssh admin@10.16.113.10

```
AVS(config-ethernet-ip)# ll

Ethernet IP settings
```

Description	Attribute Name	Current Value
IP assignment	ipType	DHCP
Preferred DNS	primaryDnsServer	
Alternate DNS	secondaryDnsServer	
Management vlan enable	mgmtVlanEnabled	Disable

```
AVS(config-ethernet-ip)# set ipType static

Set ipType to static

Ethernet IP settings
```

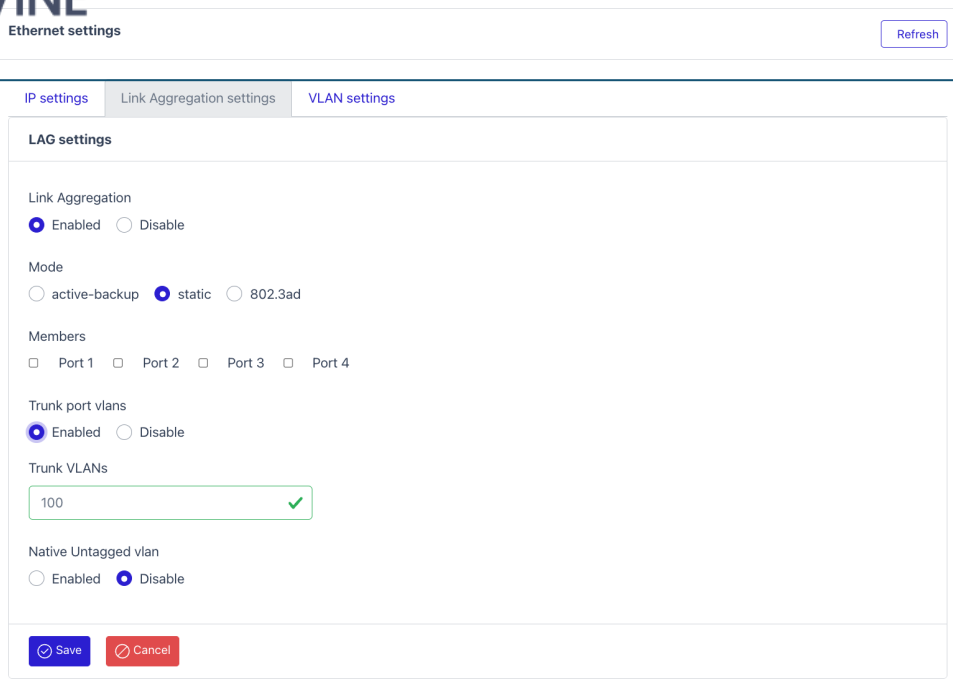
Description	Attribute Name	Current Value	Modified Value
IP assignment	ipType	DHCP	static (Static)
IP address	ip		
Subnet mask	submask		
Default gateway	gateway		
Preferred DNS	primaryDnsServer		
Alternate DNS	secondaryDnsServer		
Management vlan enable	mgmtVlanEnabled	Disable	

```
AVS(config-ethernet-ip)# save
```

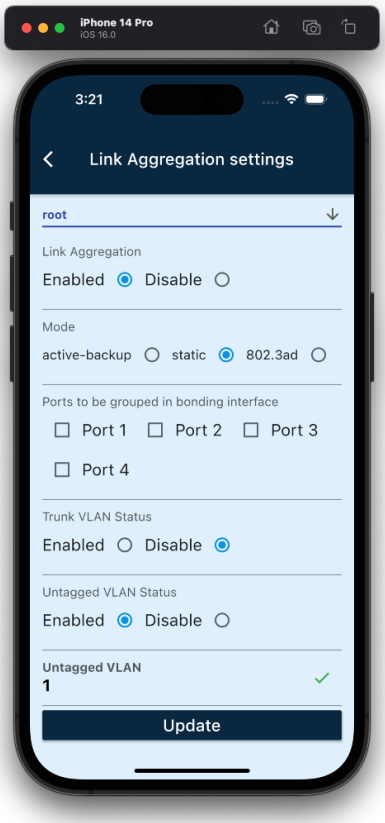
Link aggregation settings

If your backend switch supports link aggregation, you can configure ethernet ports on this page. Select the LAG type and the ports want to be aggregated. The LAG interface also supports trunk VLAN and native VLAN. For trunk VLAN,it can be a range of VLAN id. For example, 2,3,4-8.

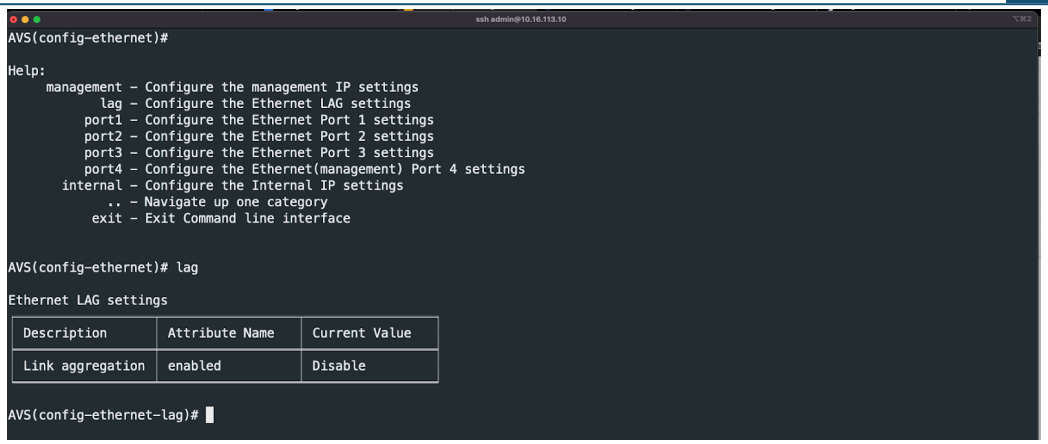
[WEB GUI]
Configuration-> Network ->Ethernet ->Link aggregation settings

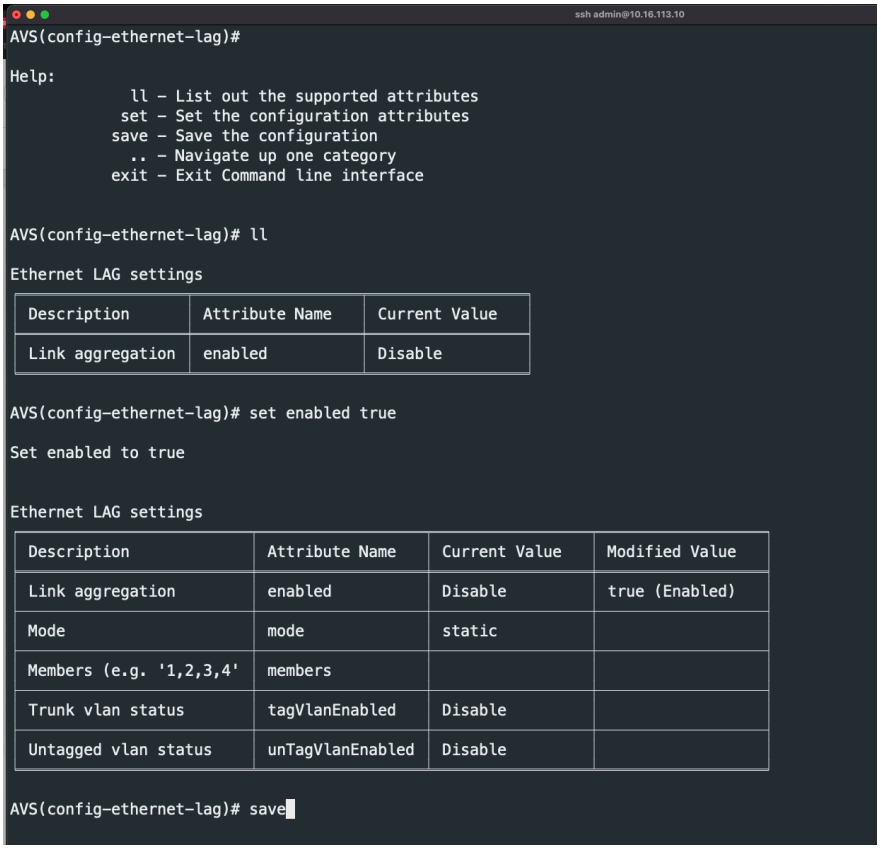


[Mobile App]
Settings -> LAG



[CLI]



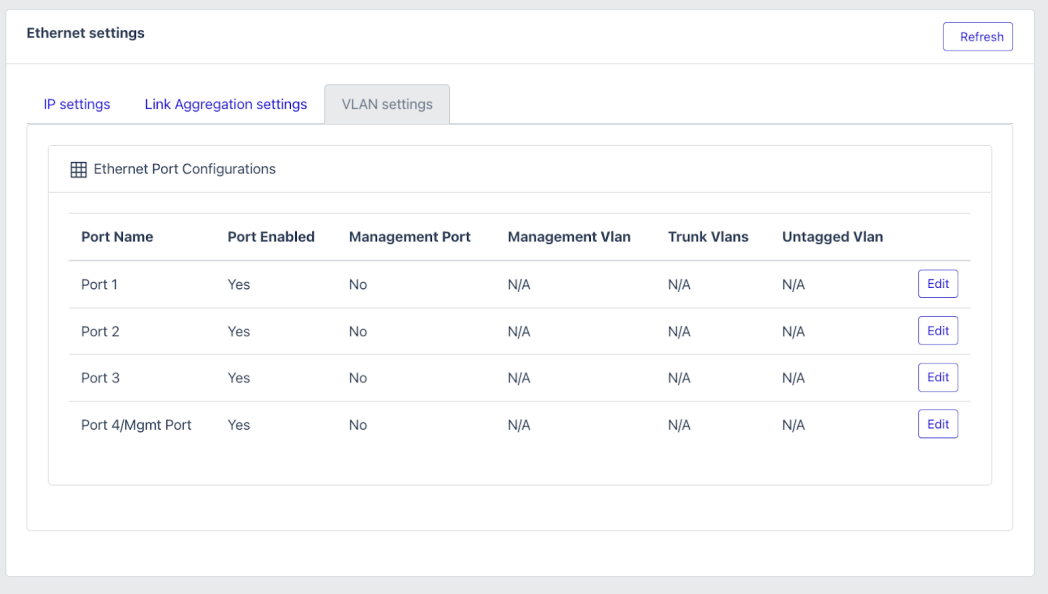


Ethernet Port and VLAN settings

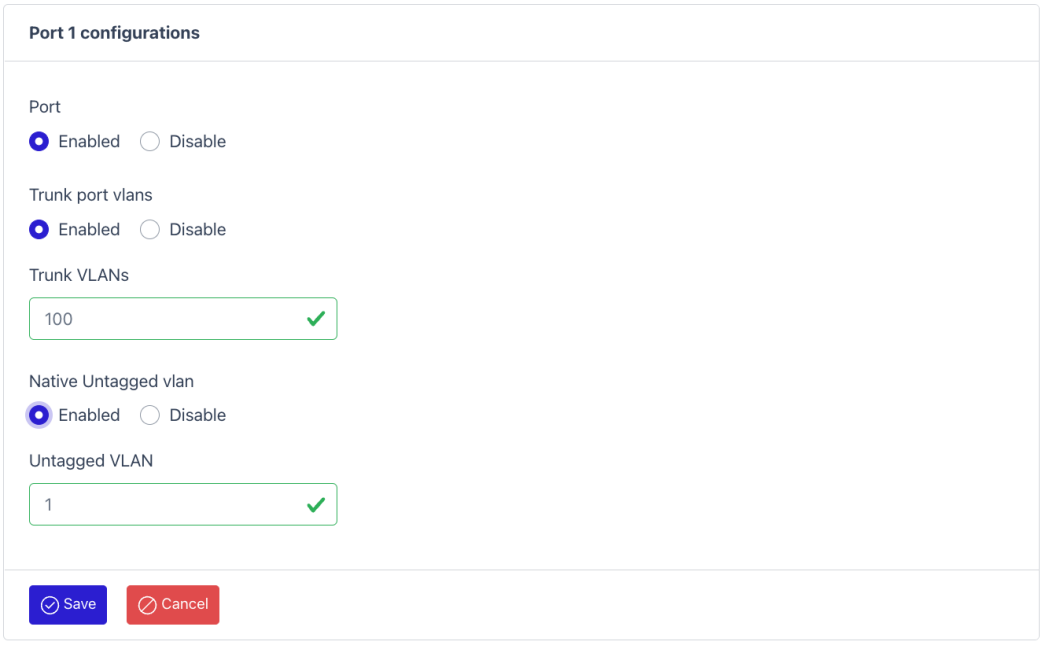
You can configure the ethernet port settings on this page. Enable/Disable the ethernet port or change the VLAN settings. The ethernet port supports trunk VLAN and native VLAN. For trunk VLAN,it can be a range of VLAN id. For example, 2,3,4-8. The port 4 can be enabled to be the dedicated management interface.

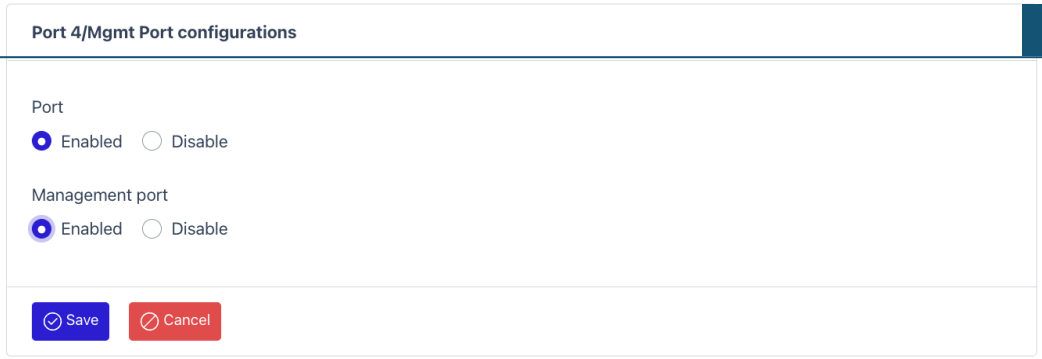
[WEB GUI]

Configuration-> Network ->Ethernet -> VLAN settings



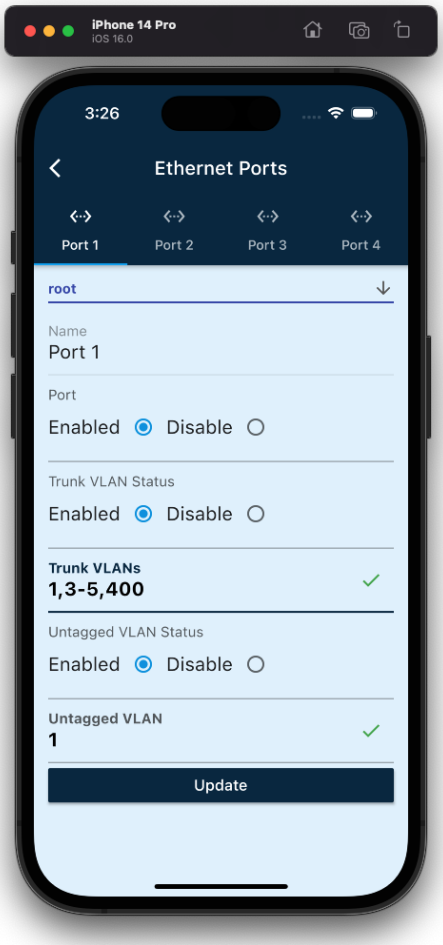
Click “edit” to configure the specific port

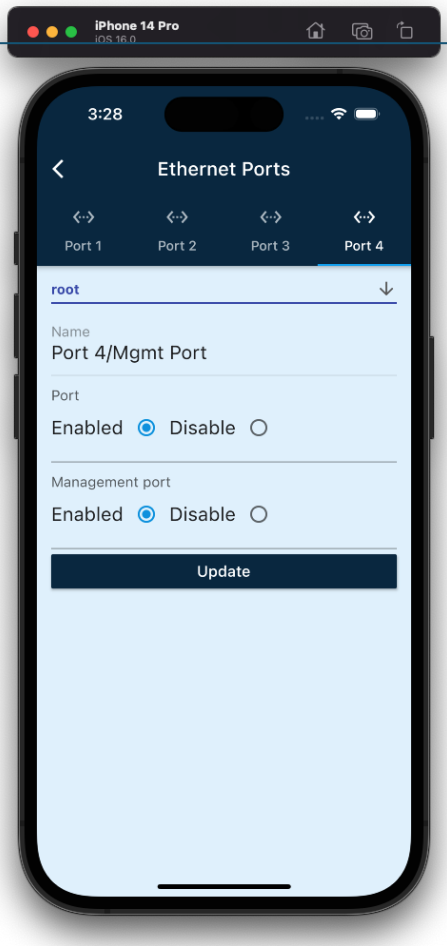




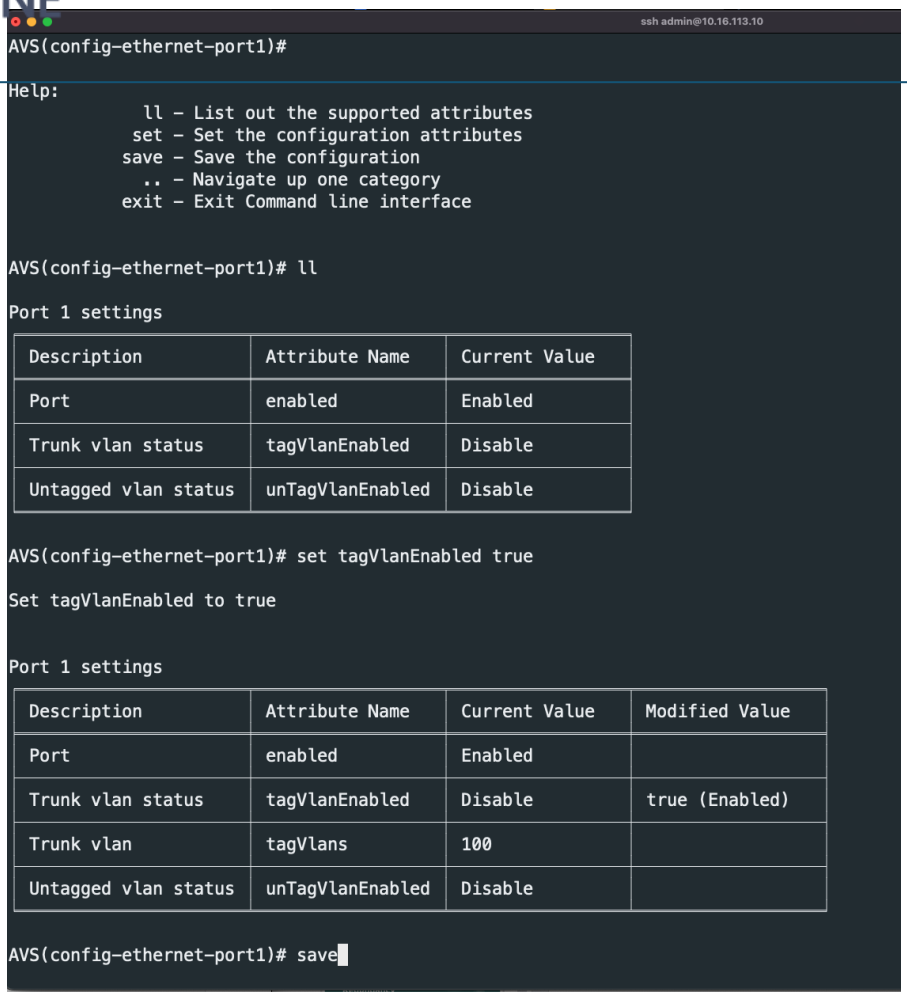
Port 4 can be configured as the dedicated management port.

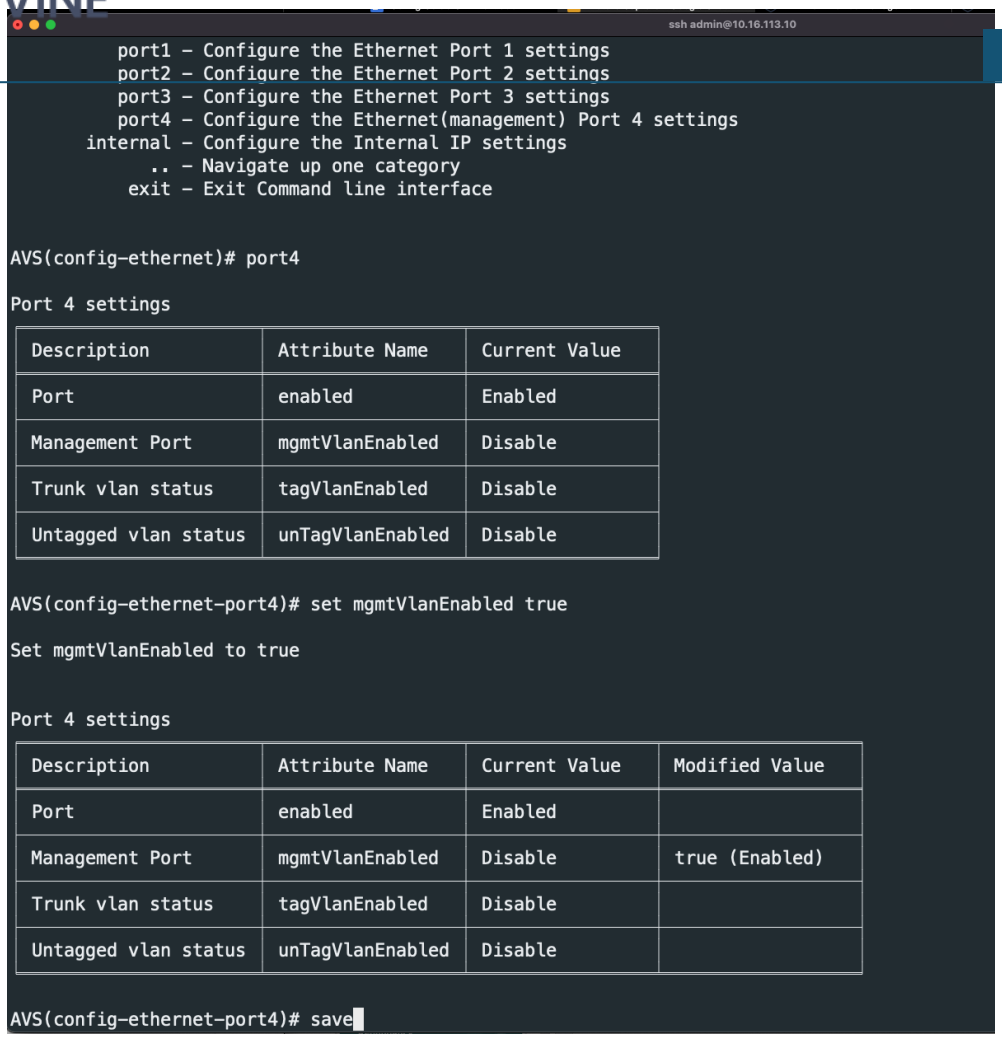
[Mobile App]
Settings -> Ports





[CLI]
config -> ethernet -> portN

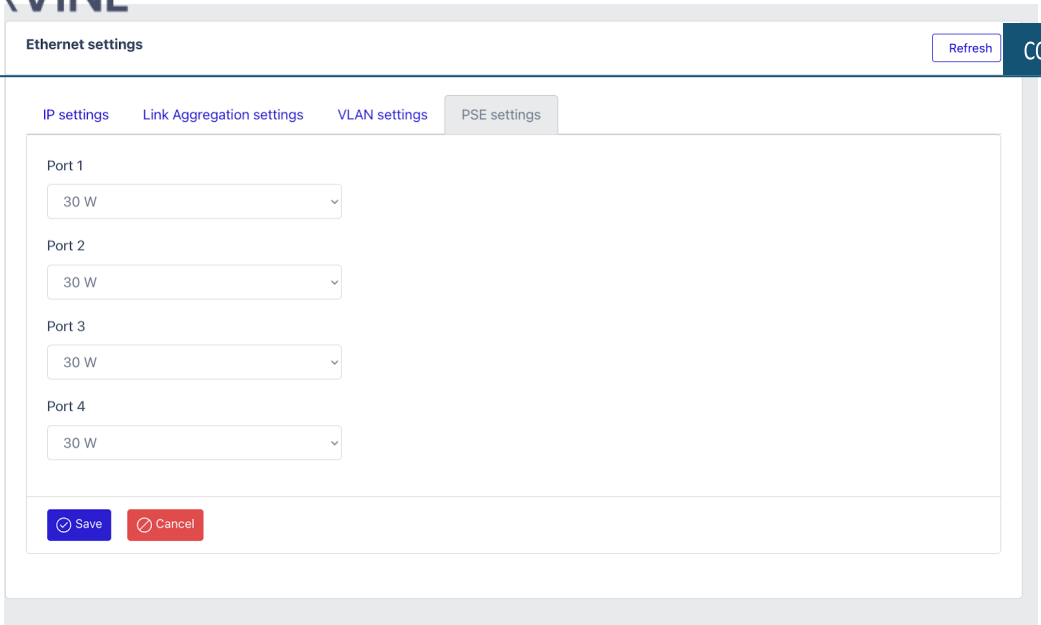

ssh admin@10.16.113.10
AVS(config-ethernet-port1)#
Help:
ll - List out the supported attributes
set - Set the configuration attributes
save - Save the configuration
.. - Navigate up one category
exit - Exit Command line interface
AVS(config-ethernet-port1)# ll
Port 1 settings
Description | Attribute Name | Current Value
Port | enabled | Enabled
Trunk vlan status | tagVlanEnabled | Disable
Untagged vlan status | unTagVlanEnabled | Disable
AVS(config-ethernet-port1)# set tagVlanEnabled true
Set tagVlanEnabled to true
Port 1 settings
Description | Attribute Name | Current Value | Modified Value
Port | enabled | Enabled |
Trunk vlan status | tagVlanEnabled | Disable | true (Enabled)
Trunk vlan | tagVlans | 100 |
Untagged vlan status | unTagVlanEnabled | Disable |
AVS(config-ethernet-port1)# save



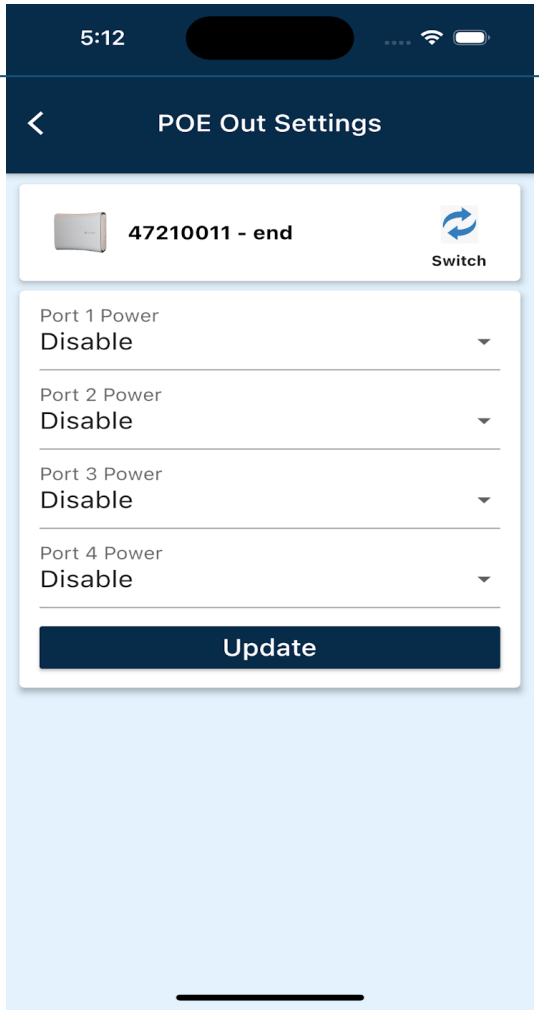
PSE settings

If the WaveTunnel device is powered by AC power. The four ethernet ports can be configured to support the POE out. The max. Watt of the total power is limited to 120W. The default PSE is disabled. If you need to power the external device via the WaveTunnel, please configure the proper PSE settings.

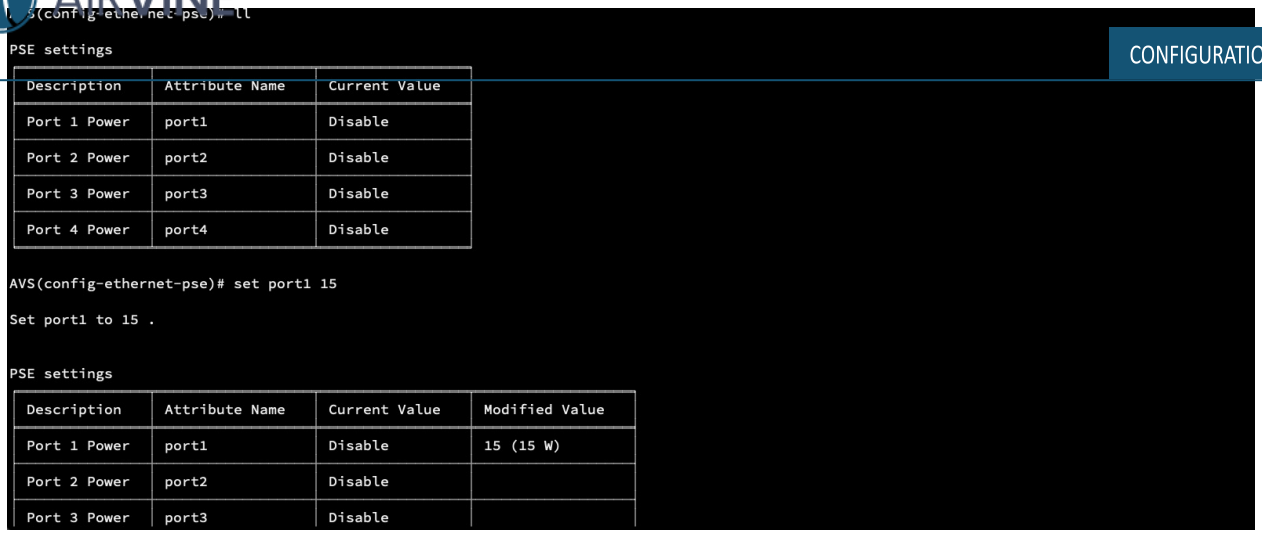
[WEB GUI]
Configuration-> Network ->Ethernet -> PSE



[Mobile App]
Settings -> PSE



[CLI]
config -> ethernet -> pse



```
AVS(config-ethernet-pse)# ll

PSE settings
```

Description	Attribute Name	Current Value
Port 1 Power	port1	Disable
Port 2 Power	port2	Disable
Port 3 Power	port3	Disable
Port 4 Power	port4	Disable

```
AVS(config-ethernet-pse)# set port1 15

Set port1 to 15 .

PSE settings
```

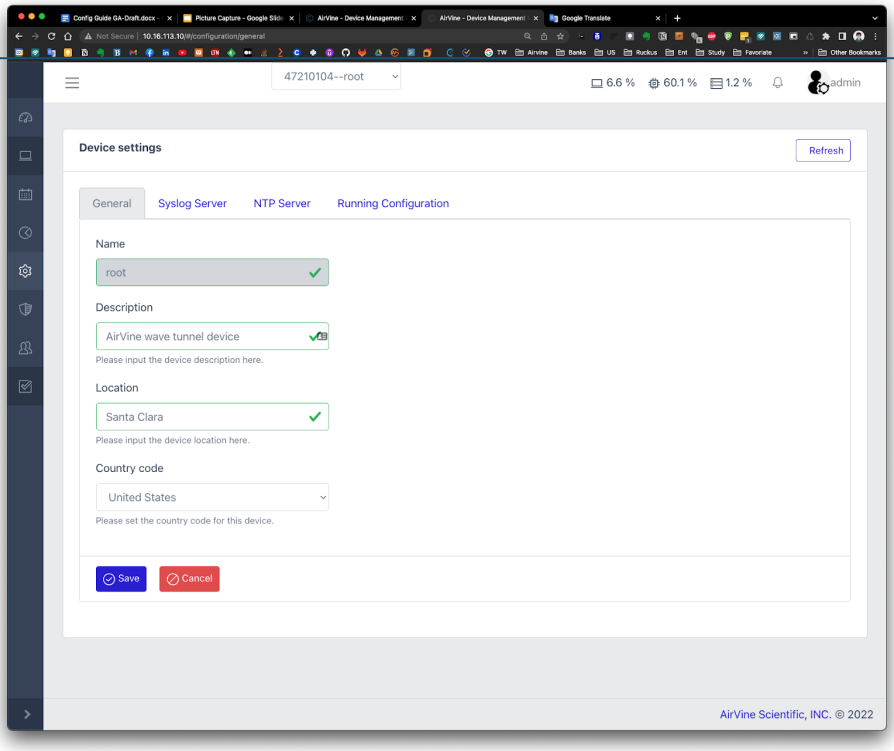
Description	Attribute Name	Current Value	Modified Value
Port 1 Power	port1	Disable	15 (15 W)
Port 2 Power	port2	Disable	
Port 3 Power	port3	Disable	

Update the device settings

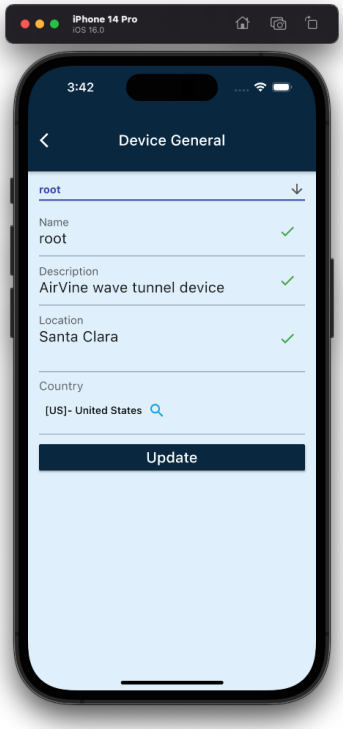
General settings

To update the description,location,Country code of the WaveTunnel device on this page.

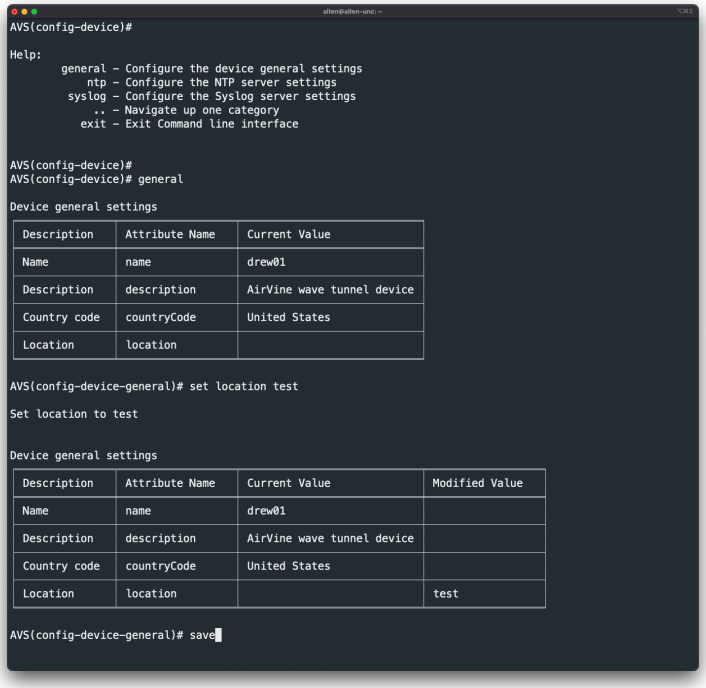
[WEB GUI]
Config -> General



[Mobile App]
Settings -> General



[CLI]
Config -> device -> general



```
AVS(config-device)#

Help:
        general - Configure the device general settings
            ntp - Configure the NTP server settings
         syslog - Configure the Syslog server settings
             .. - Navigate up one category
           exit - Exit Command line interface


AVS(config-device)#
AVS(config-device)# general

Device general settings
```

Description	Attribute Name	Current Value
Name	name	drew01
Description	description	AirVine wave tunnel device
Country code	countryCode	United States
Location	location	

```
AVS(config-device-general)# set location test

Set location to test

Device general settings
```

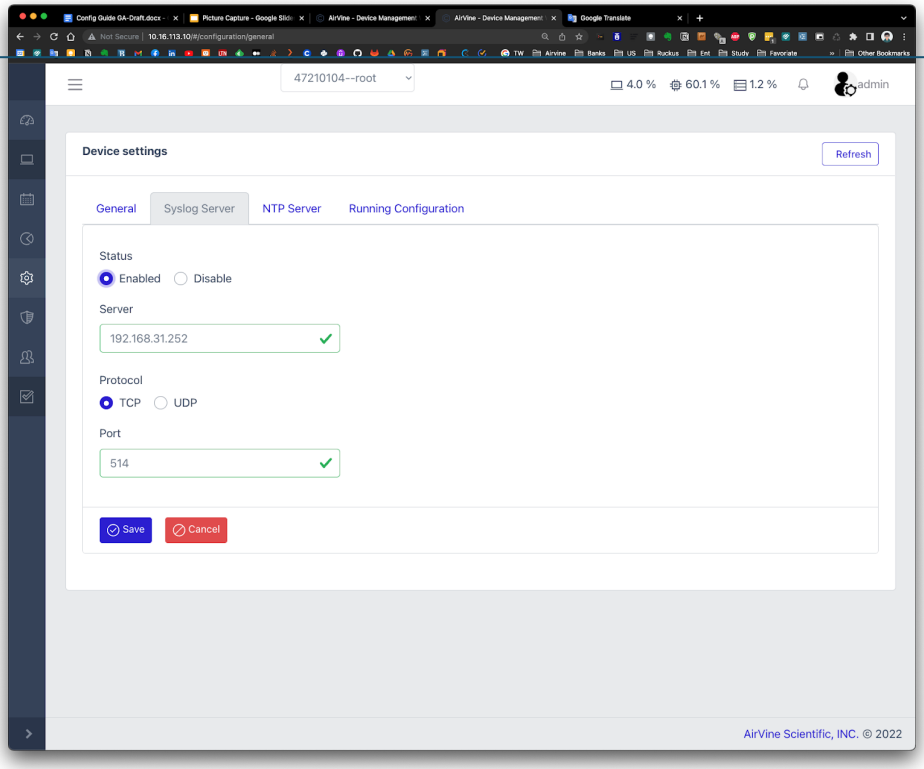
Description	Attribute Name	Current Value	Modified Value
Name	name	drew01	
Description	description	AirVine wave tunnel device	
Country code	countryCode	United States	
Location	location		test

```
AVS(config-device-general)# save
```

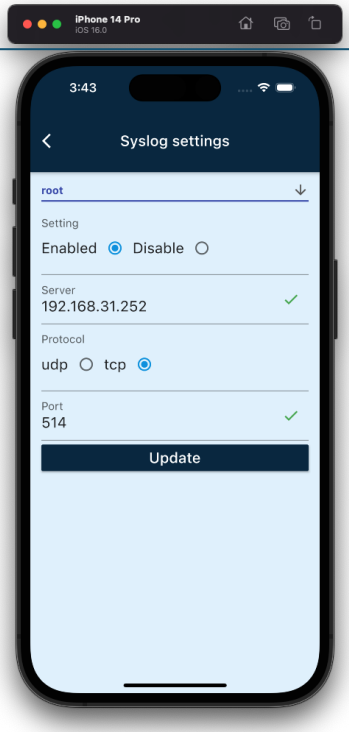
Syslog settings

To export the log messages to the external syslog server, you can enable the syslog server on this page. The settings include enabled/disable, server address, port.

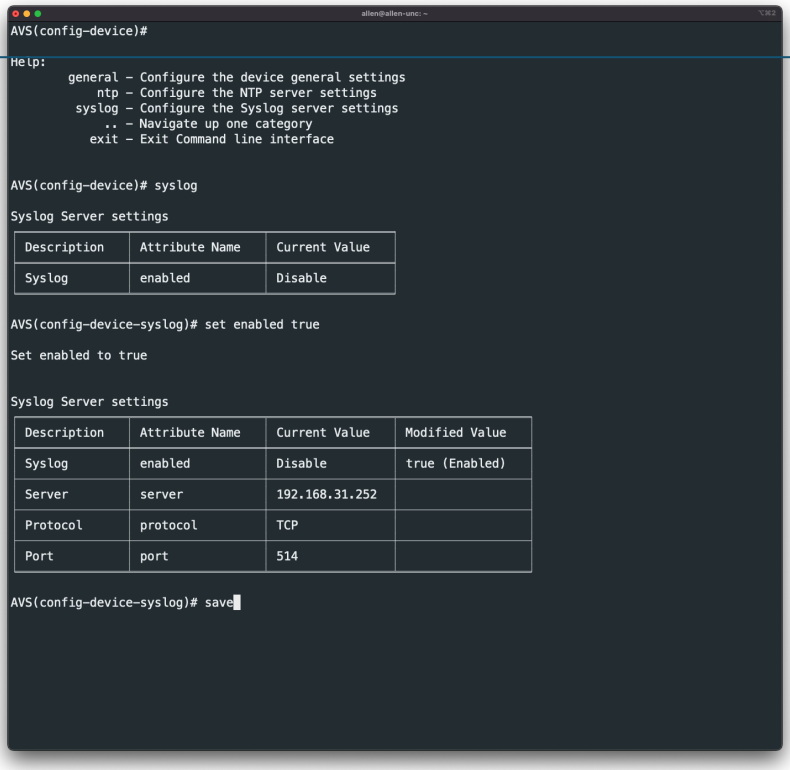
[WEB GUI]
Configuration-> General -> Syslog Server



[Mobile App]
Settings -> Syslog



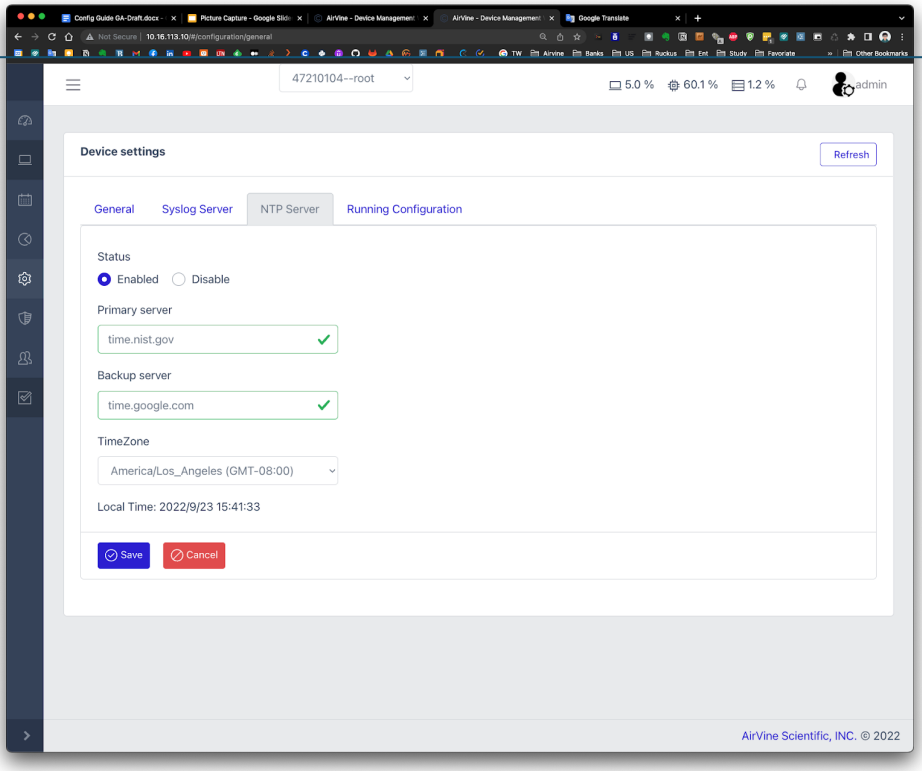
[CLI]
Config -> device -> syslog



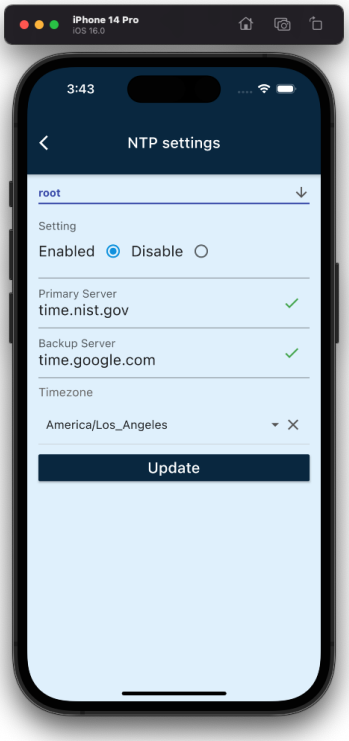
NTP settings

You can configure the NTP settings of the WaveTunnel to synchronize the date time with the external server. It requires that your WaveTunnel can reach the NTP server in your local network or Internet. If there is no NTP server available, the WaveTunnel sync up the date time with the user's client device when they login.

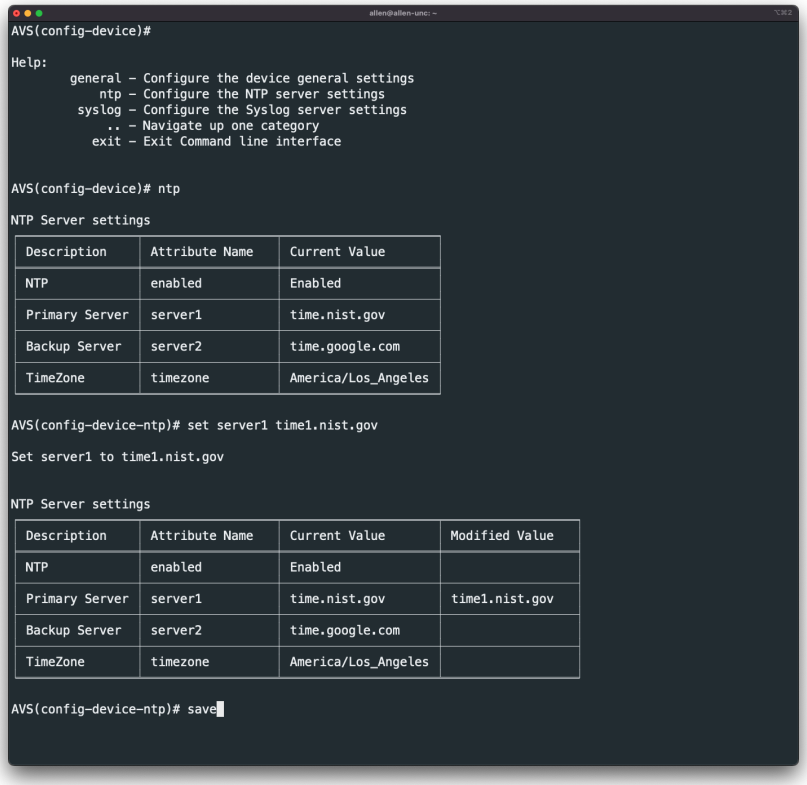
[WEB GUI]
Configuration-> General ->NTP ->



[Mobile App]
Settings -> NTP



[CLI]
config -> device -> ntp



```
AVS(config-device)#

Help:
        general - Configure the device general settings
            ntp - Configure the NTP server settings
         syslog - Configure the Syslog server settings
             .. - Navigate up one category
           exit - Exit Command line interface


AVS(config-device)# ntp

NTP Server settings
```

Description	Attribute Name	Current Value
NTP	enabled	Enabled
Primary Server	server1	time.nist.gov
Backup Server	server2	time.google.com
TimeZone	timezone	America/Los_Angeles

```
AVS(config-device-ntp)# set server1 time1.nist.gov

Set server1 to time1.nist.gov

NTP Server settings
```

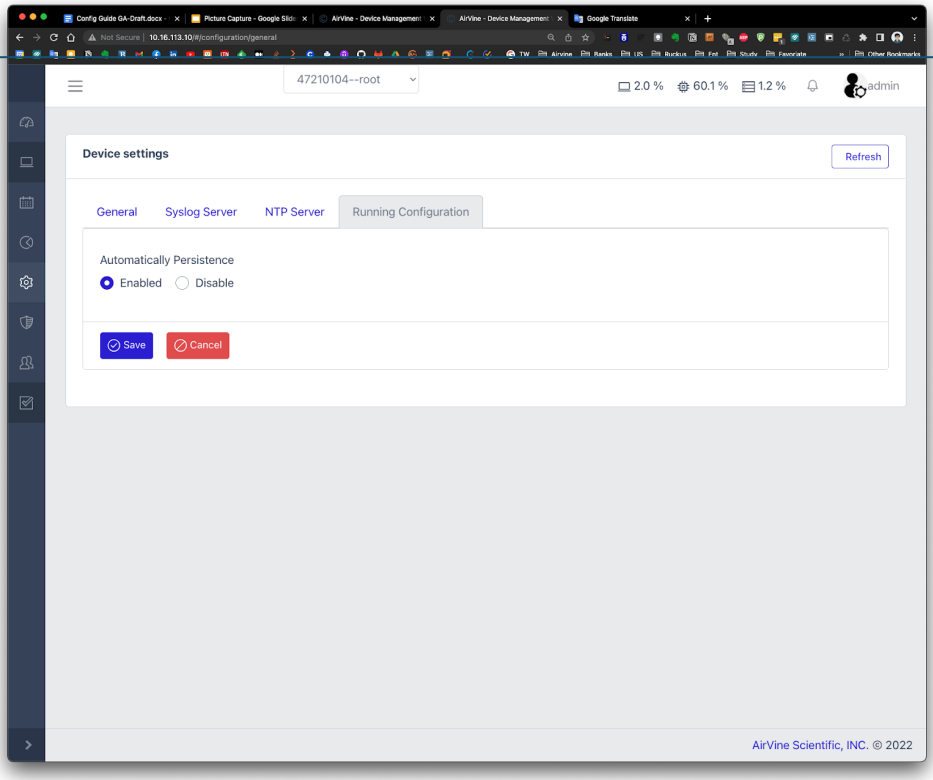
Description	Attribute Name	Current Value	Modified Value
NTP	enabled	Enabled	
Primary Server	server1	time.nist.gov	time1.nist.gov
Backup Server	server2	time.google.com	
TimeZone	timezone	America/Los_Angeles	

```
AVS(config-device-ntp)# save
```

Auto persistent settings

There is a mechanism in the WaveTunnel device which you can disable the persistence of configurations. This means the configurations are temporarily stored in memory as “running configuration”. It will be lost if you reboot the WaveTunnel device. It’s useful if you want to test some new functions. If the device runs into any issue, you can just reboot the device back to the previous good configurations.

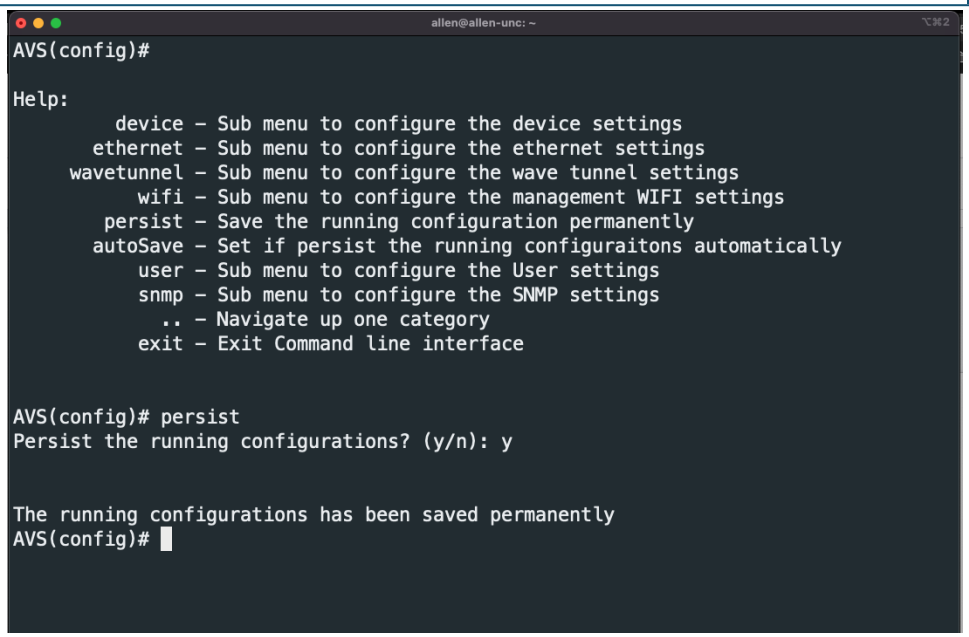
[WEB GUI]
Configuration-> General ->Running Configuration ->



[CLI]
Config -> autosave

```
allen@allen-unc: ~
AVS(config)#

Help:
        device - Sub menu to configure the device settings
      ethernet - Sub menu to configure the ethernet settings
    wavetunnel - Sub menu to configure the wave tunnel settings
          wifi - Sub menu to configure the management WIFI settings
       persist - Save the running configuration permanently
      autoSave - Set if persist the running configuraitons automatically
          user - Sub menu to configure the User settings
          snmp - Sub menu to configure the SNMP settings
            .. - Navigate up one category
          exit - Exit Command line interface


AVS(config)# autoSave

Set auto-save option as 'enabled' or 'disabled'

AVS(config)# autoSave enabled

The auto-save is set to enabled

AVS(config)#
```

Type persist command to save the configurations permanently.



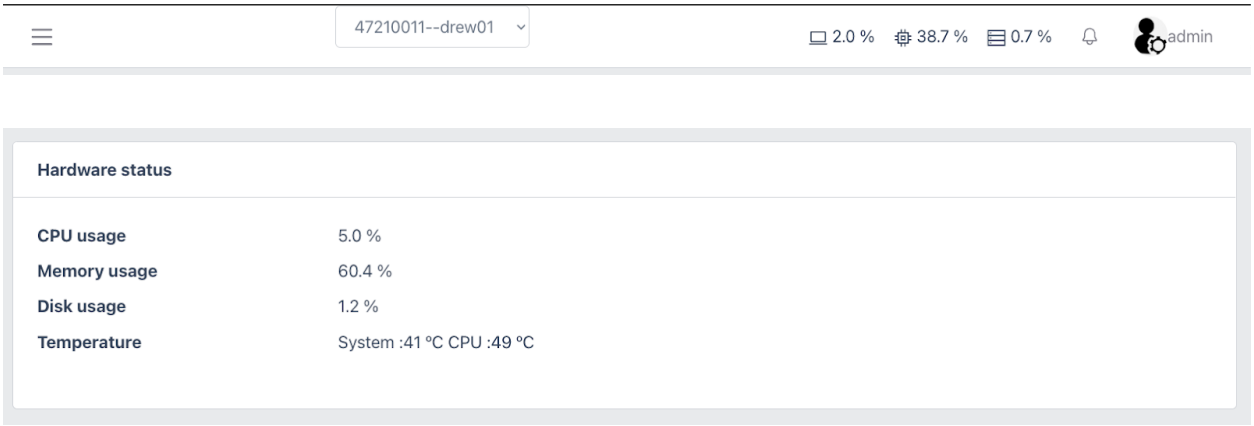
Monitor the WaveTunnel device

There are several pages in the system you can use to monitor the status of your WaveTunnel device. You can check these sections below for more information.

Check the system resource usages

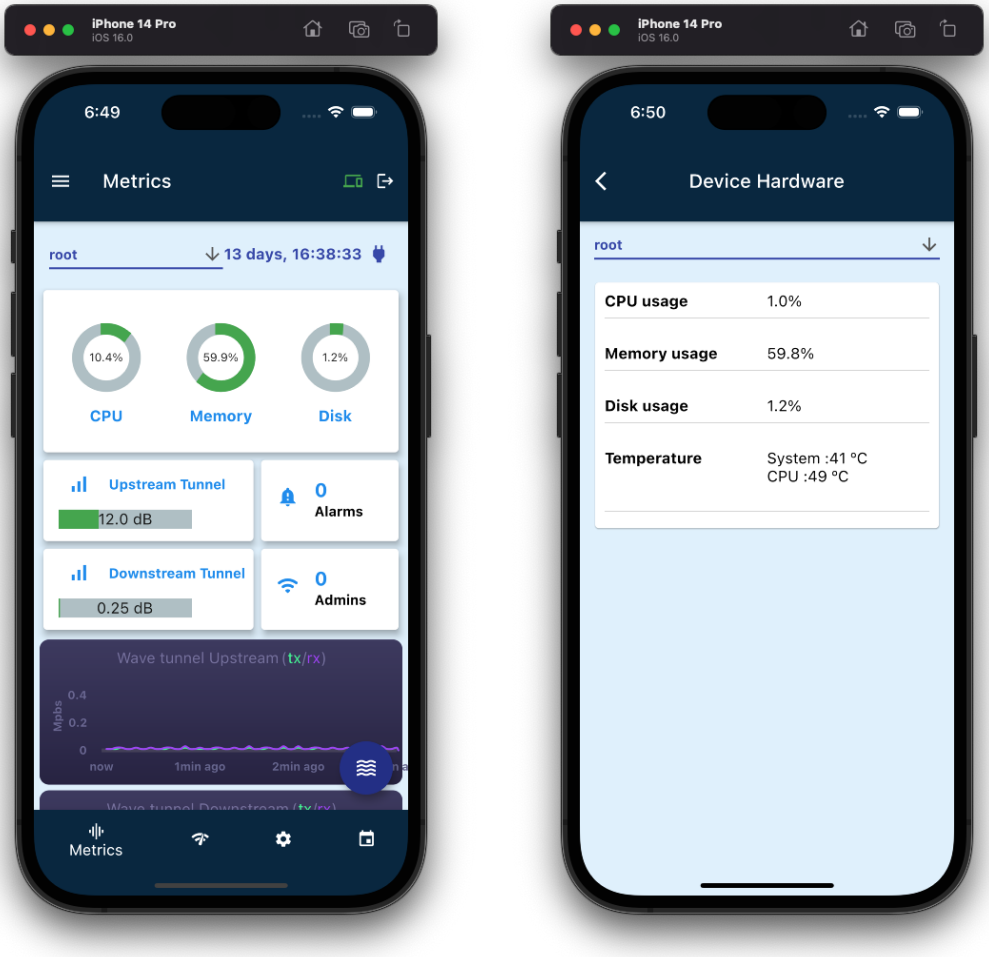
You can check the resource usages of System CPU, Memory, Flash Drive and Temperature on this page

[WEB GUI]
Monitoring -> Device -> General

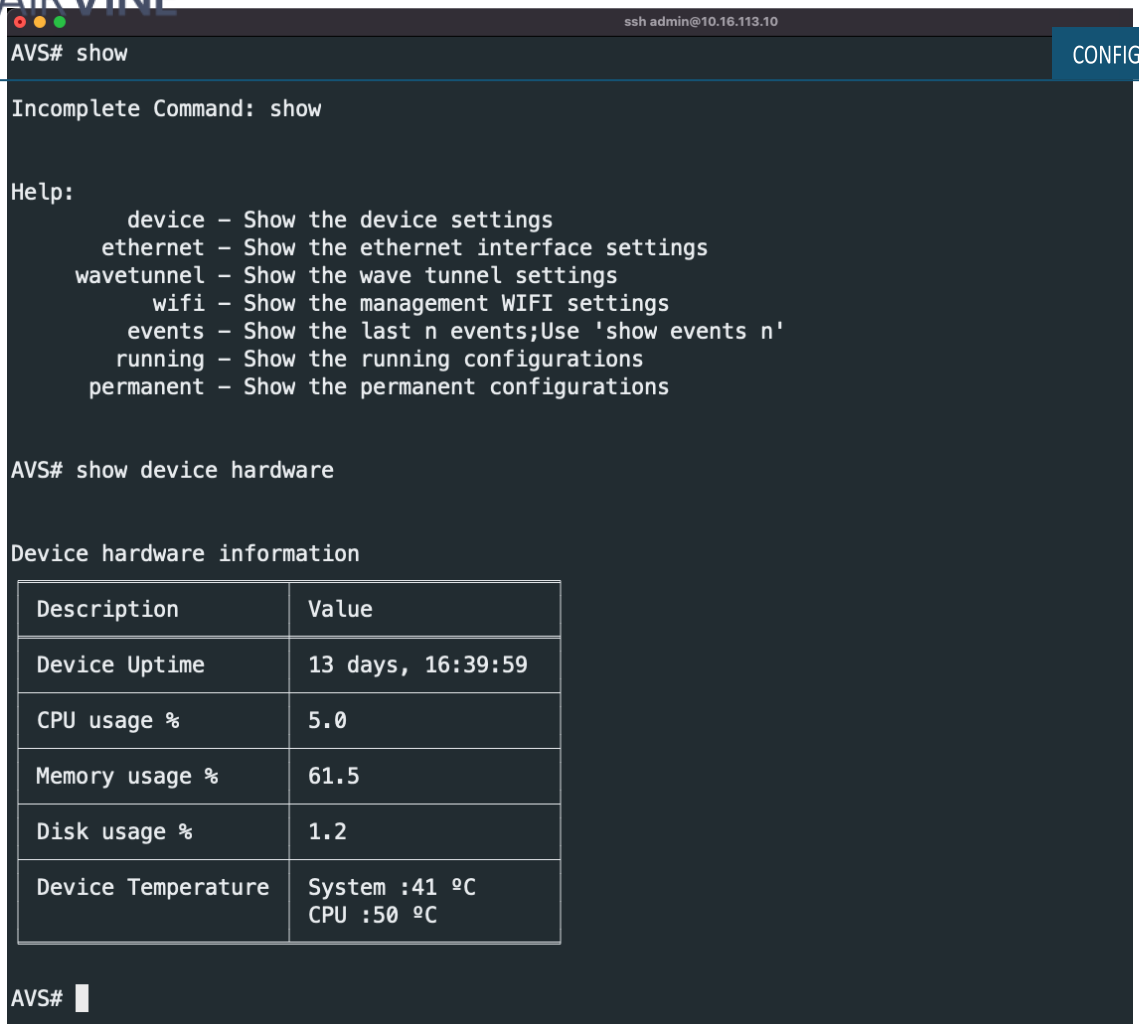


[Mobile App]
Dashboard

You can click the Dashboard widget to see the usage of system resources.



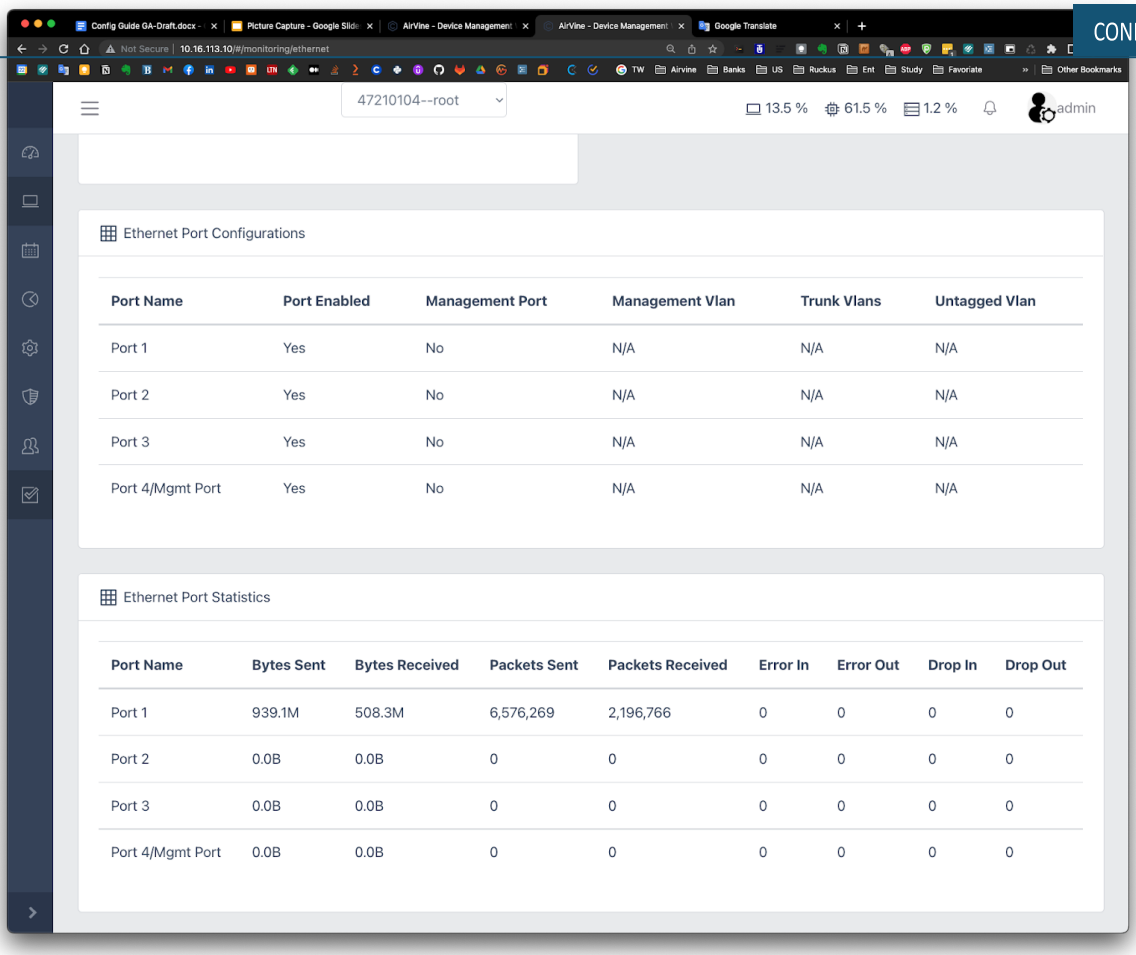
[CLI]
Show -> Device -> Hardware



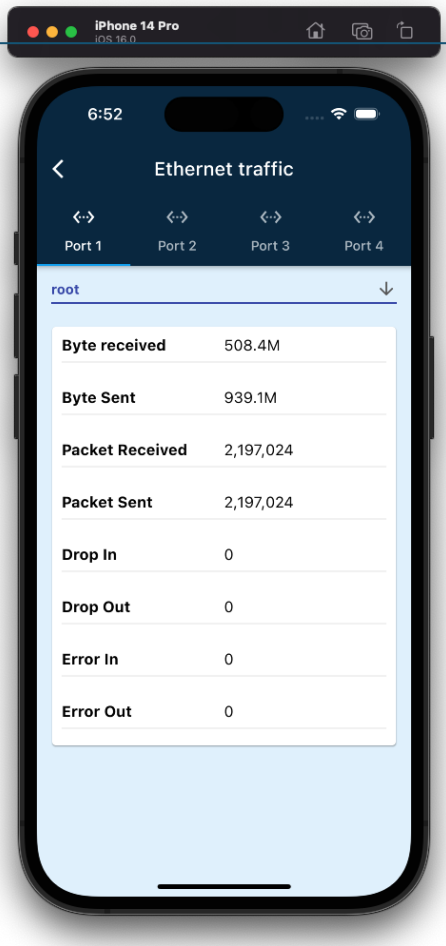
Check the accumulated traffics of ethernet ports

On this page, you can check the accumulated traffic statistics of each ethernet port since last boot up. It includes Bytes sent, Bytes received, Packets sent, Packets received, Error in, Error out, Drop in and Drop out. These values are reset when the system is rebooted.

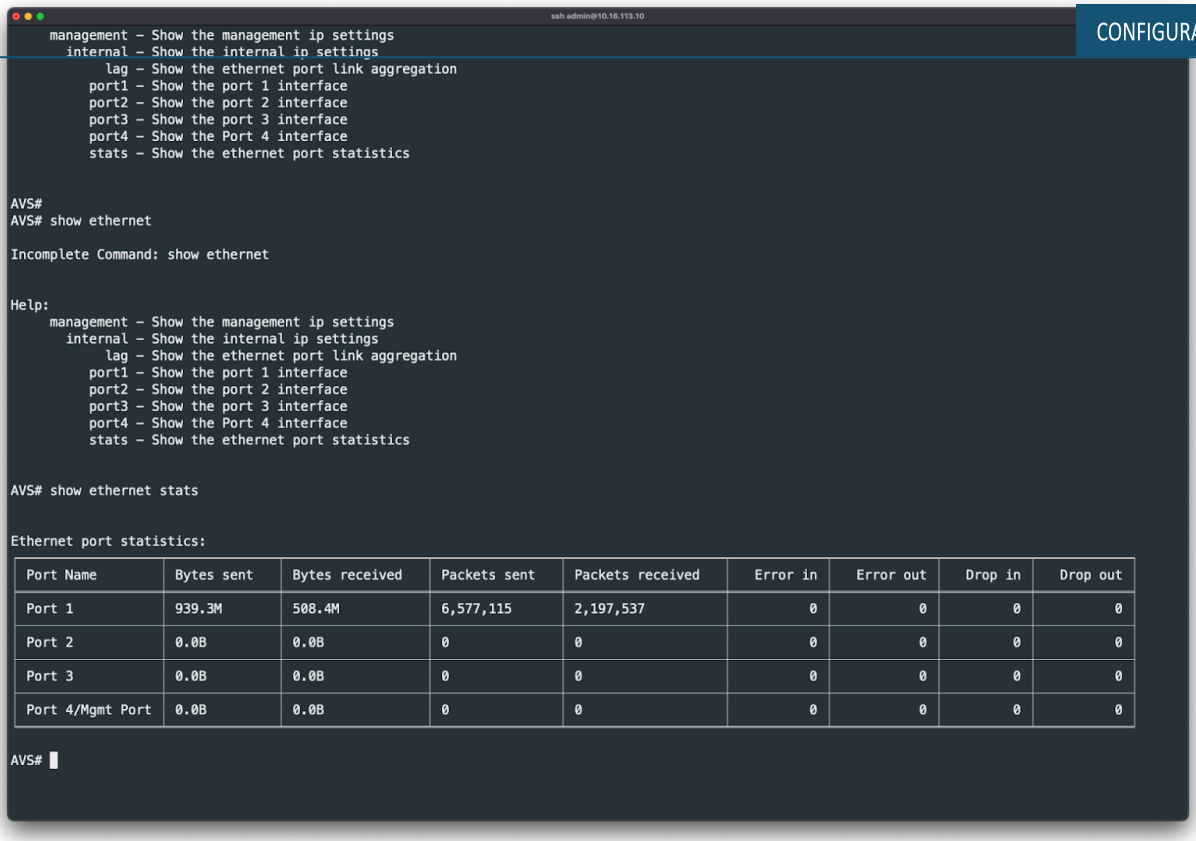
[WEB GUI]
Monitoring -> Ethernet



[Mobile App]
Monitoring - > Ethernet Port - >Traffic



[CLI]
Show -> ethernet -> stats



```
ssh admin@10.16.113.10
     management - Show the management ip settings
       internal - Show the internal ip settings
            lag - Show the ethernet port link aggregation
          port1 - Show the port 1 interface
          port2 - Show the port 2 interface
          port3 - Show the port 3 interface
          port4 - Show the Port 4 interface
          stats - Show the ethernet port statistics


AVS#
AVS# show ethernet

Incomplete Command: show ethernet


Help:
     management - Show the management ip settings
       internal - Show the internal ip settings
            lag - Show the ethernet port link aggregation
          port1 - Show the port 1 interface
          port2 - Show the port 2 interface
          port3 - Show the port 3 interface
          port4 - Show the Port 4 interface
          stats - Show the ethernet port statistics


AVS# show ethernet stats


Ethernet port statistics:
```

Port Name	Bytes sent	Bytes received	Packets sent	Packets received	Error in	Error out	Drop in	Drop out
Port 1	939.3M	508.4M	6,577,115	2,197,537	0	0	0	0
Port 2	0.0B	0.0B	0	0	0	0	0	0
Port 3	0.0B	0.0B	0	0	0	0	0	0
Port 4/Mgmt Port	0.0B	0.0B	0	0	0	0	0	0

```
AVS#
```

Check the historical statistic

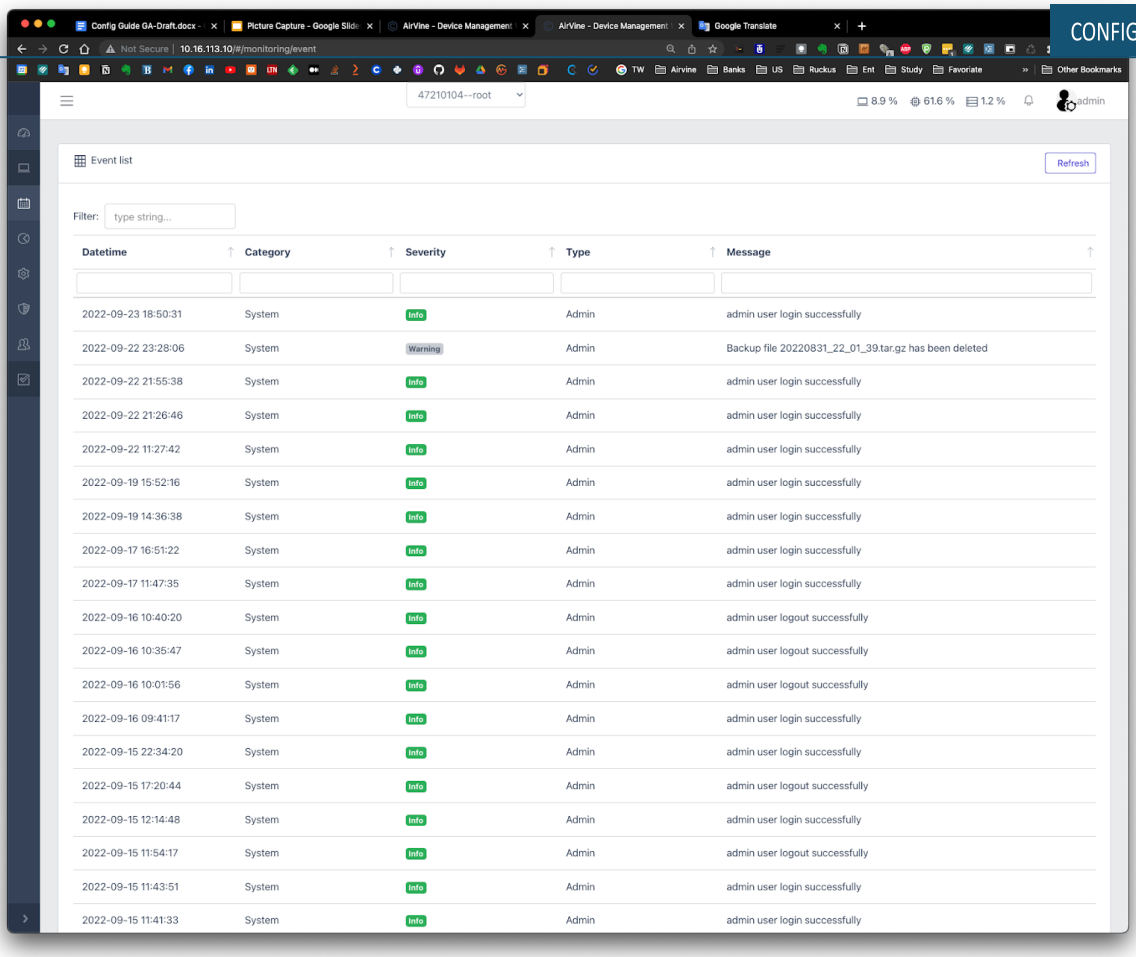
The WaveTunnel collects the historical statistics every 10 minutes, and the collected data last for 30 days. You can query the TX/RX traffic going through the WaveTunnel connection or ethernet ports with different criteria.

[WEB GUI]
Statistics

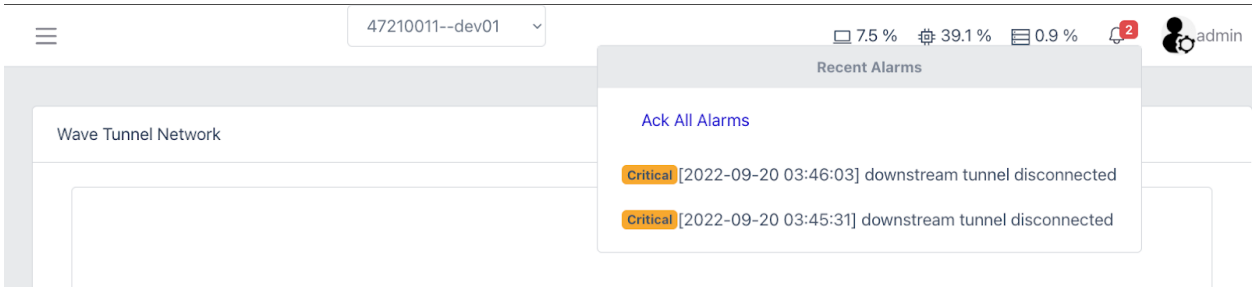
Check the events and alarms

The System events and user operations are logged in the event database. These events are classified by category, severity and type. You can do the full search or sorting to locate the events you want to check. For some critical events, it will be translated as an alarm to notify the user on the Dashboard banner or sending out the SNMP trap.

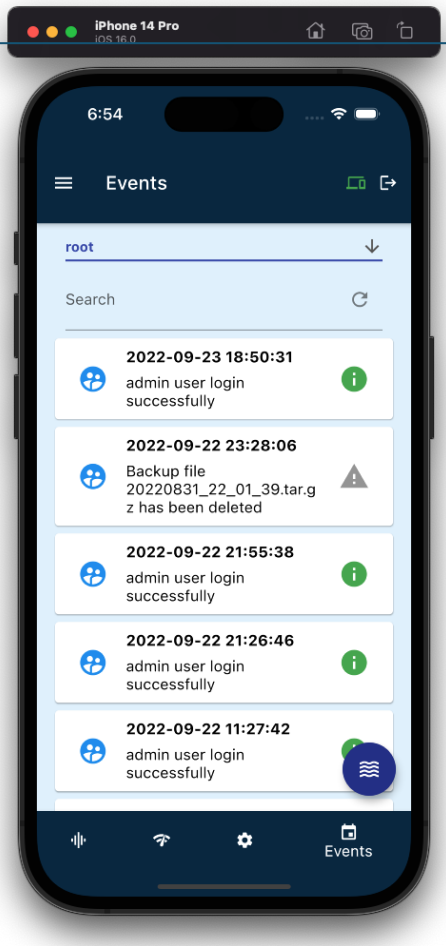
[WEB GUI]
Events



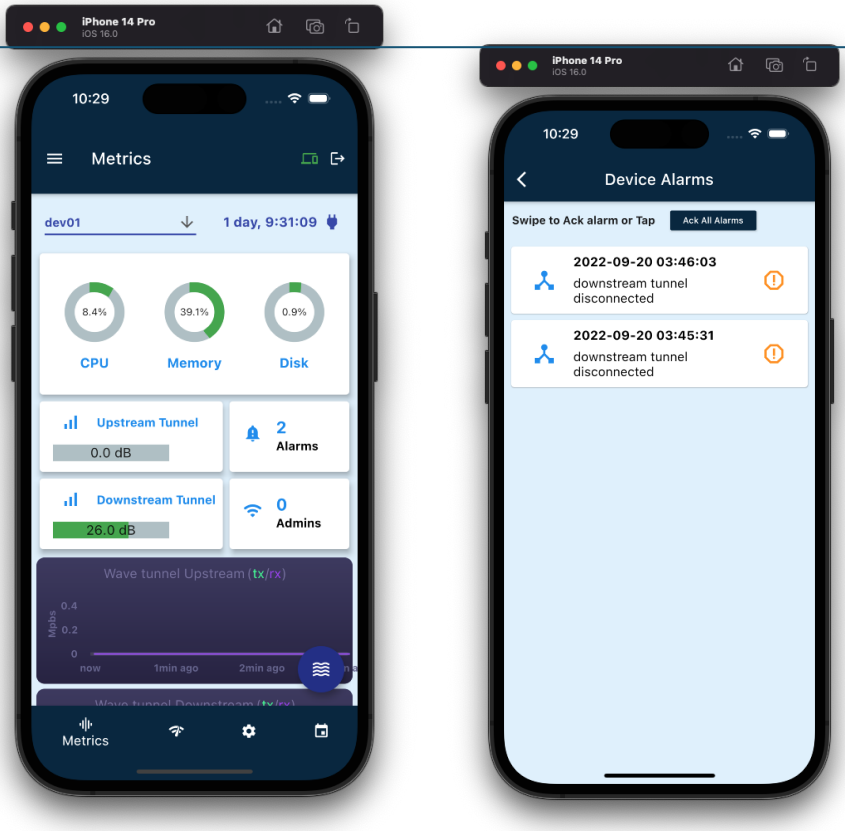
The alarms shown on the top banner. You can check the list and acknowledge it.



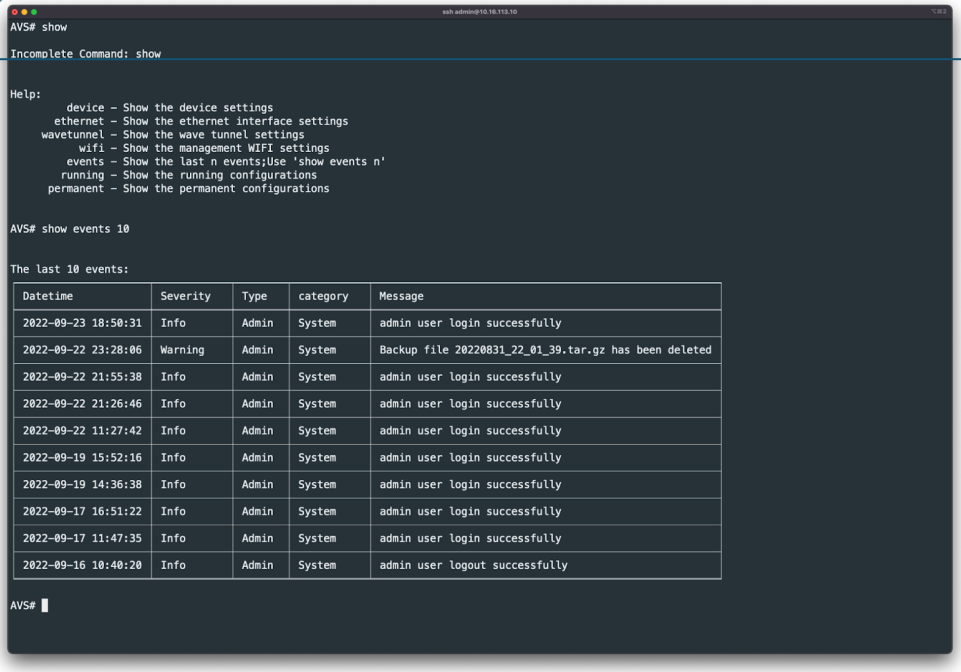
[Mobile App]
Events



The alarms shown on the top banner. You can check the list and acknowledge it.



[CLI]
Show -> events

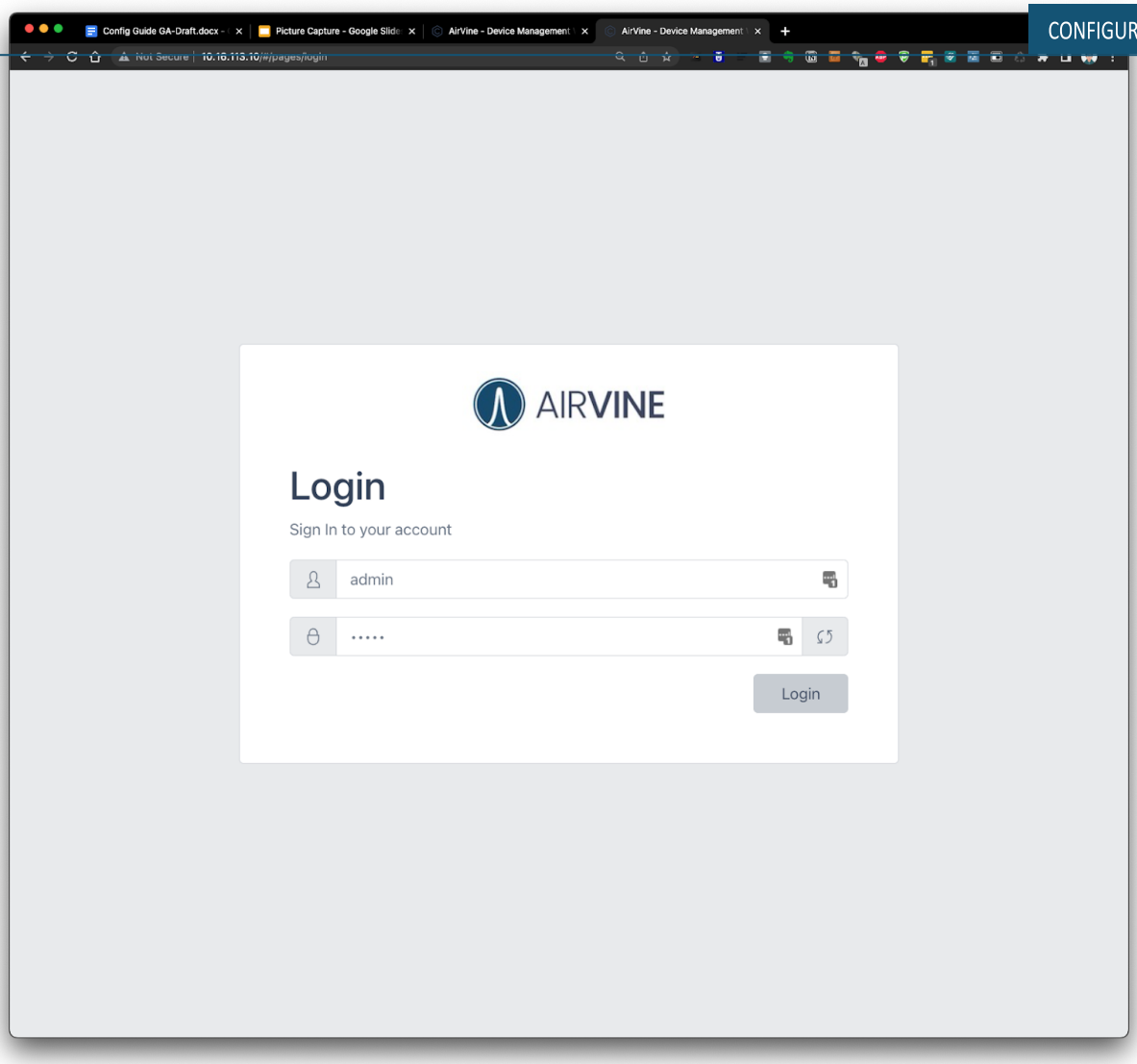


User Management

User Login

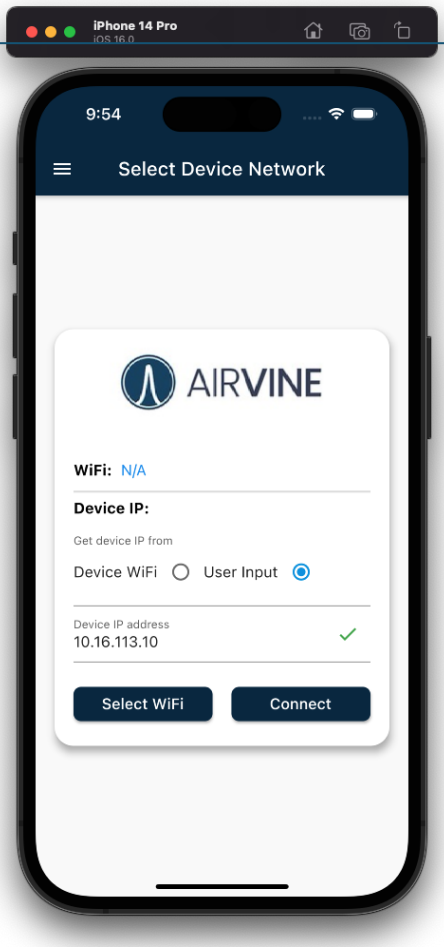
This is the page for the user to login to the management interface. The user authentication is provided by the Linux user database and the default user is “admin”. You can create more admin users based on your needs.

[WEB GUI]
Type the http://[management IP] on your browser

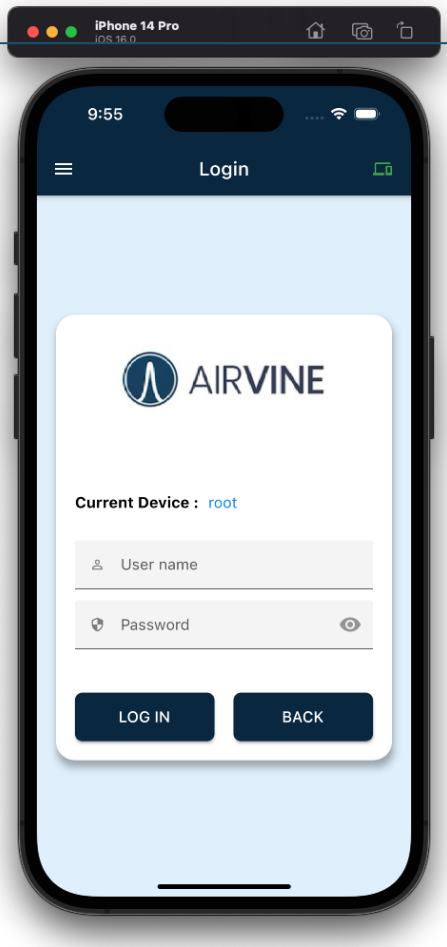


[Mobile App]

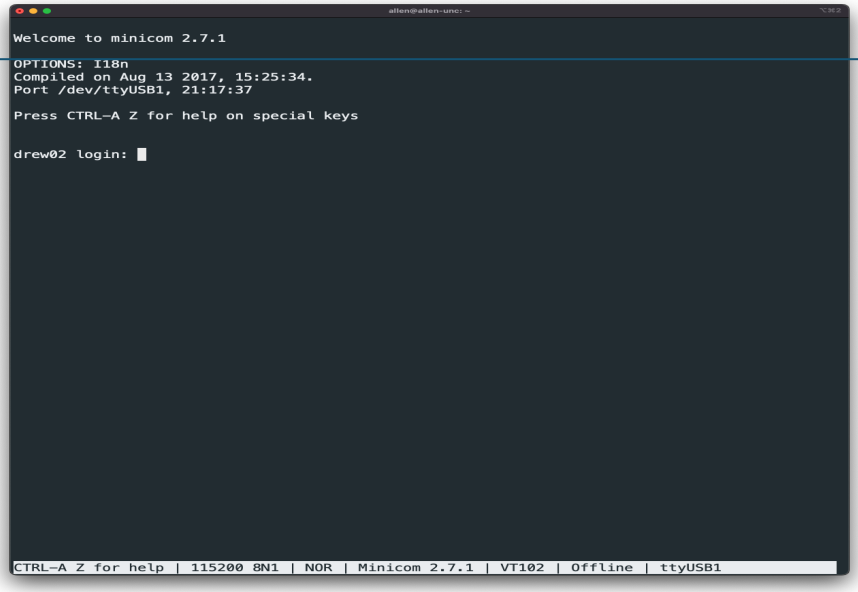
Select the device you want to connect via WIFI or management IP.



Input the username and password to login the Mobile App.



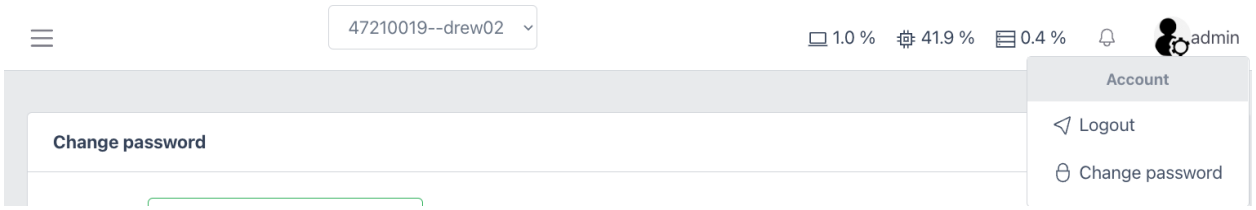
[CLI]
Use SSH client or Serial cable to connect to the CLI.



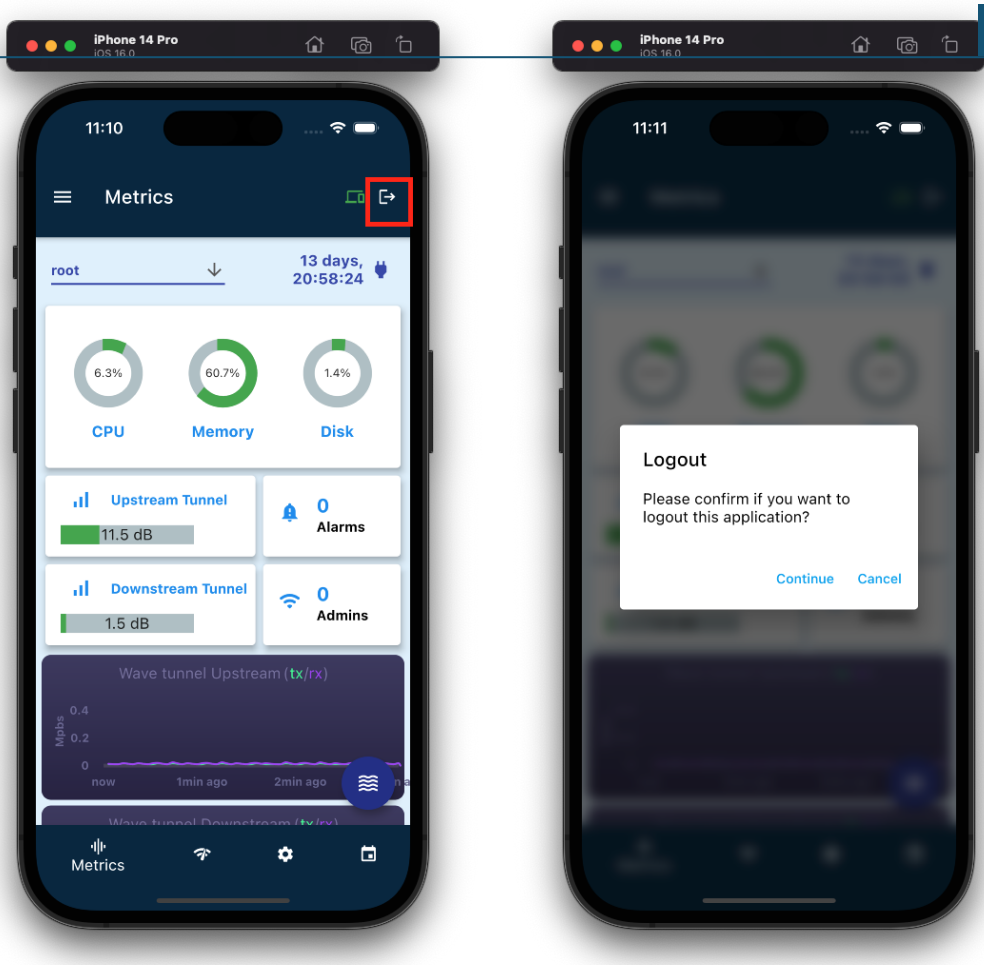
User Logout

There is a button on WEB GUI and Mobile for the user to logout the system. The user session is cleared after the logout.

[WEB GUI]



[Mobile App]



[CLI]

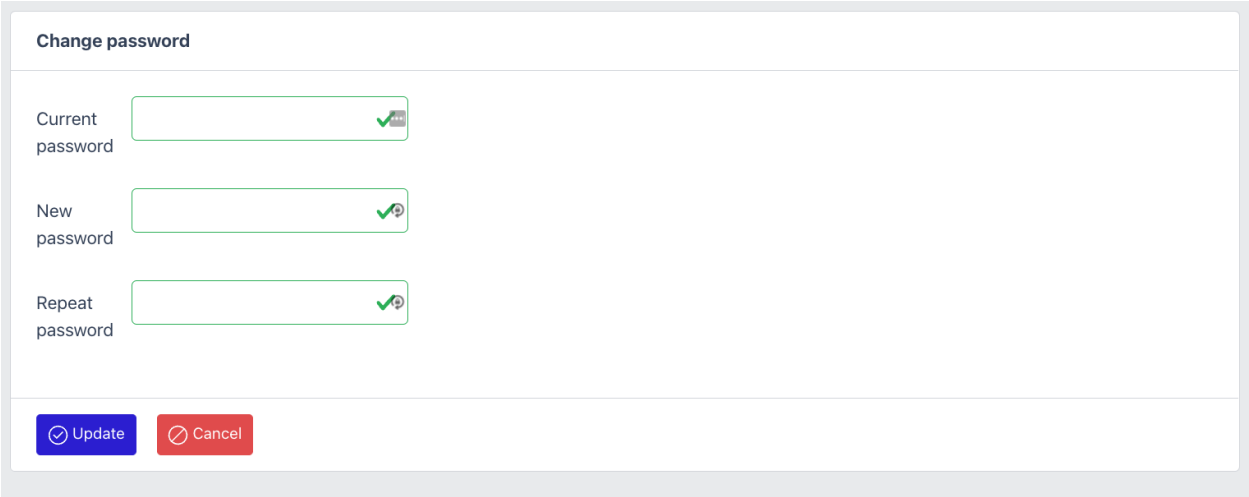
For CLI, type “exit” to logout the console.

```
allen@Allens-Mac-mini:~/bin
AVS> enable
Password:
AVS#

Help:
          show - Show the device status
        config - Enter configuration menu
      firmware - Enter firmware menu
     operation - Enter operation menu
            .. - Navigate up one category
          exit - Exit Command line interface


AVS# exit
Do you want to exit CLI? (y/n)?
y
Connection to 10.16.113.10 closed.
 allen@Allens-Mac-mini  ~/bin
```

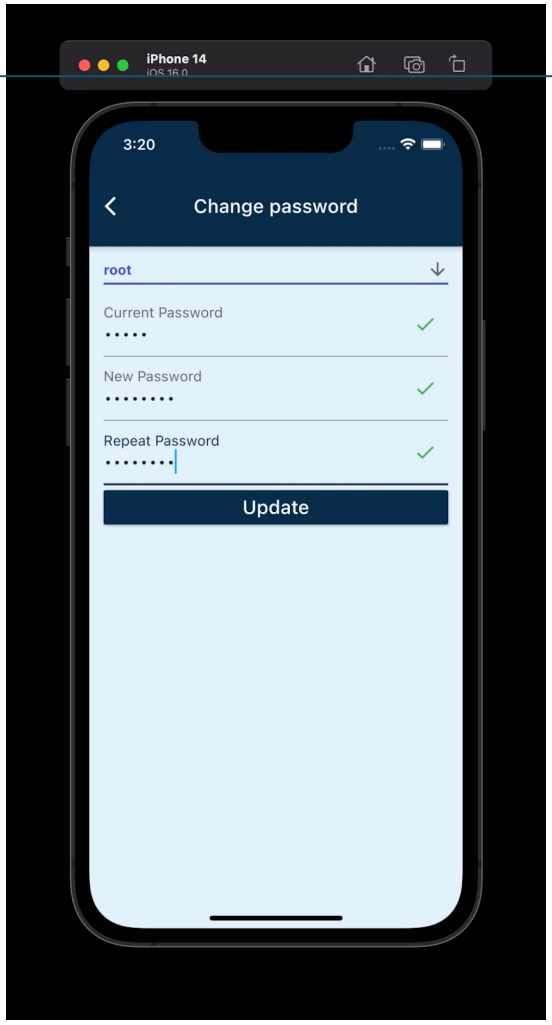
Change the user password

You can change the password on this page

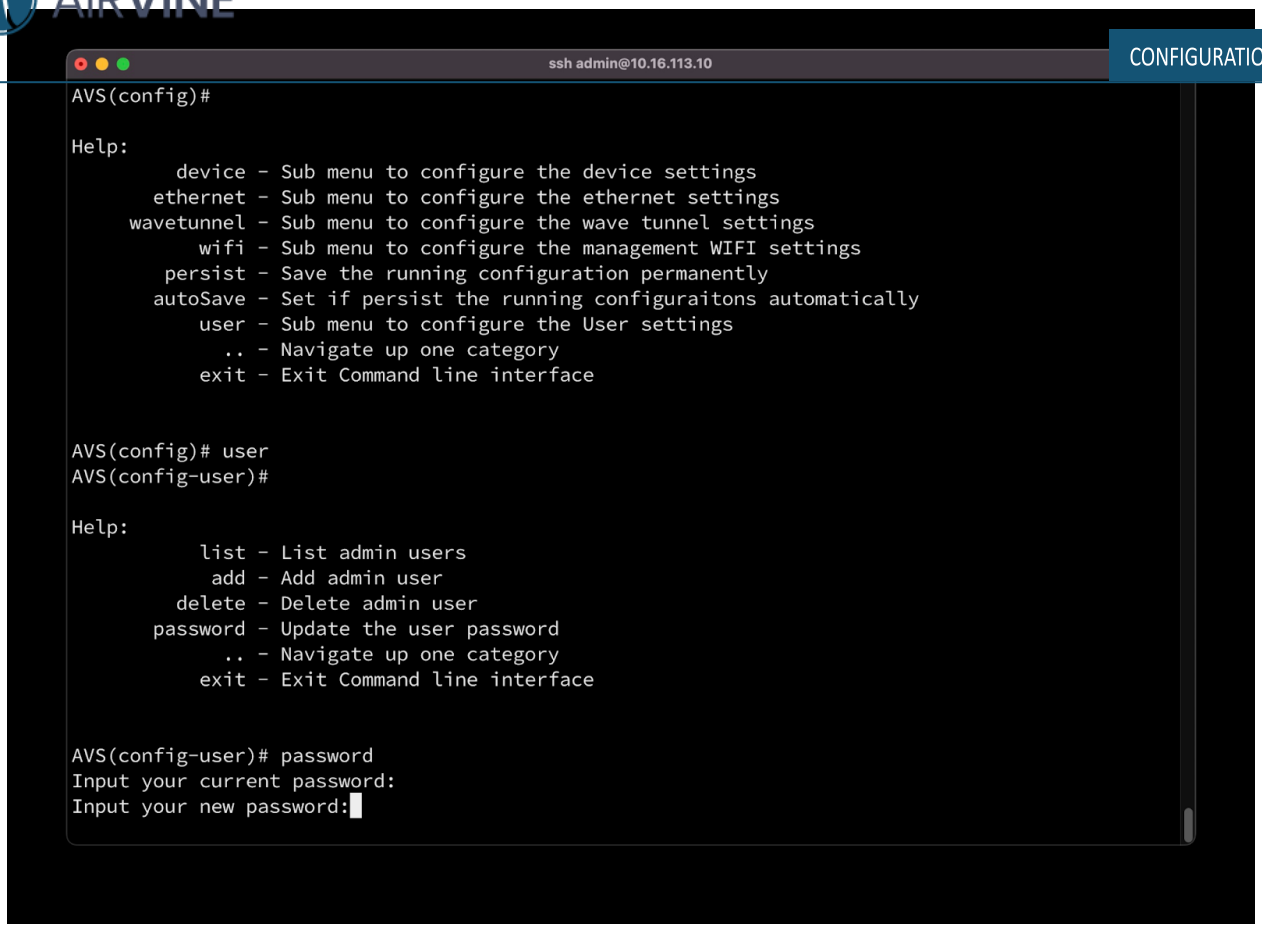
[WEB GUI]



[Mobile App]

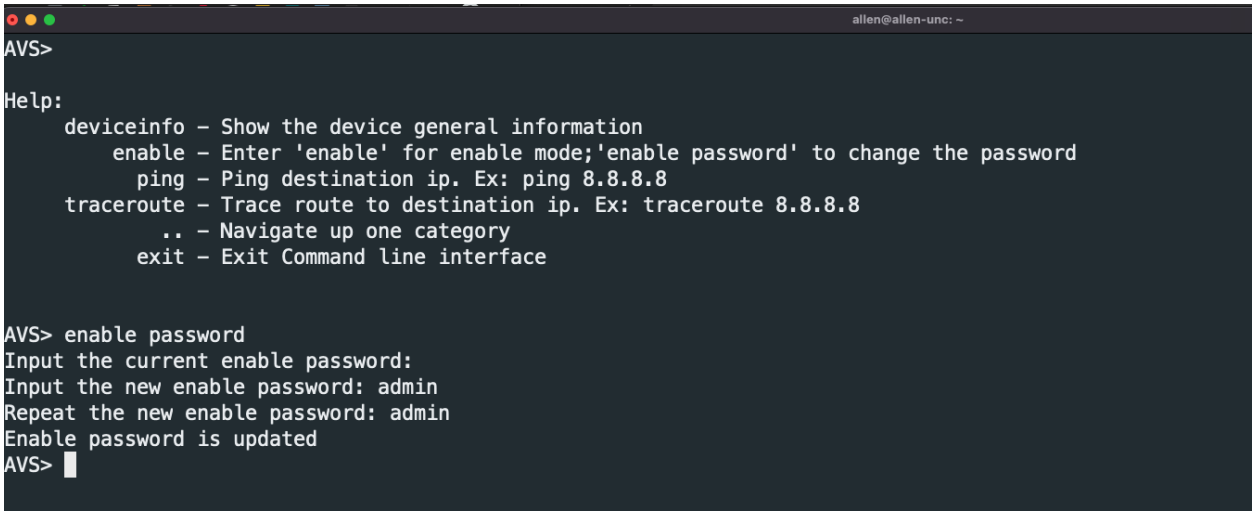

iPhone 14
iOS 16.0
3:20
Change password
root
Current Password
New Password
Repeat Password
Update

[CLI]



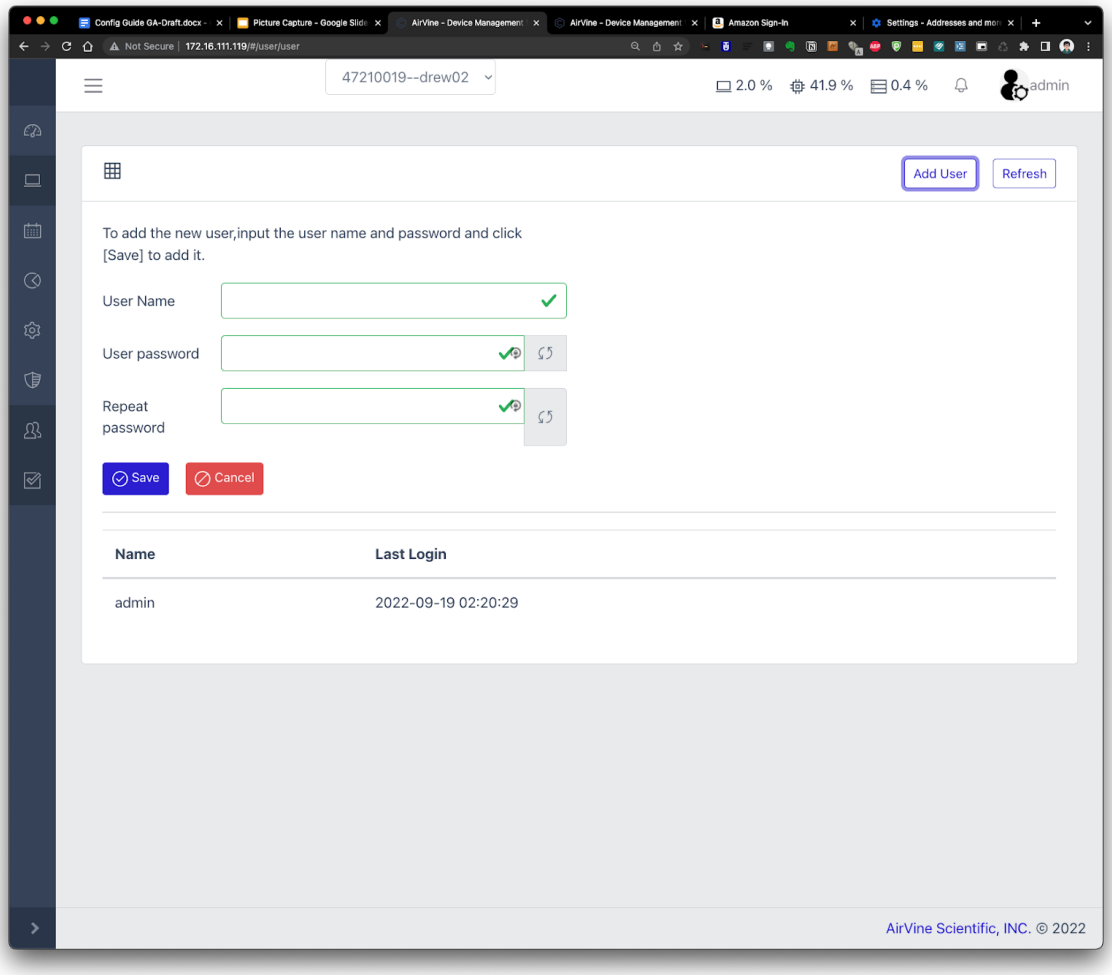
Change the enable password of CLI

For CLI, there are two levels of command set. To enter the second level, you need to input the “enable” password. The default password is blank but you can change it via the following commands.



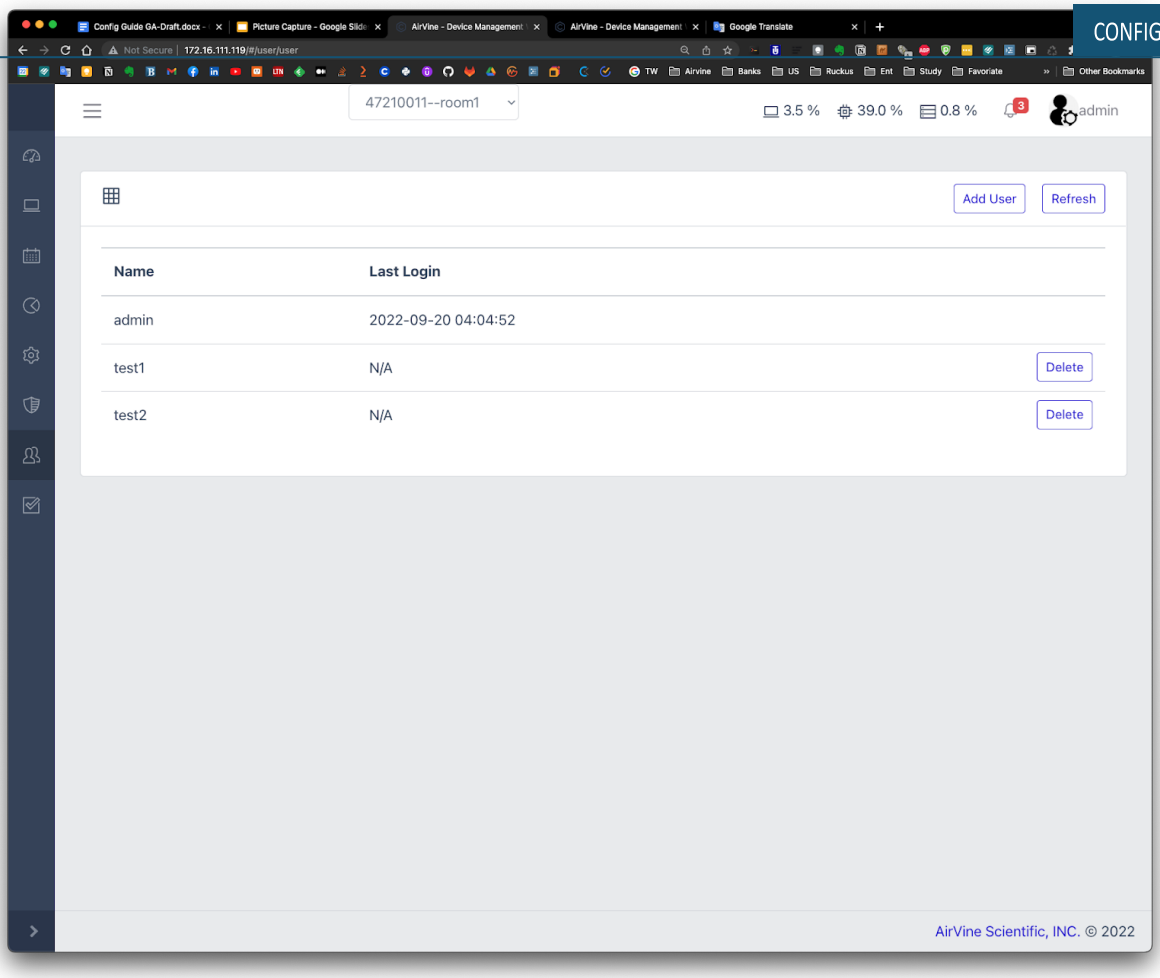
Add New User

Add a new admin user to the connected WaveTunnel device.



Delete User

Delete a new admin user from the connected WaveTunnel device.

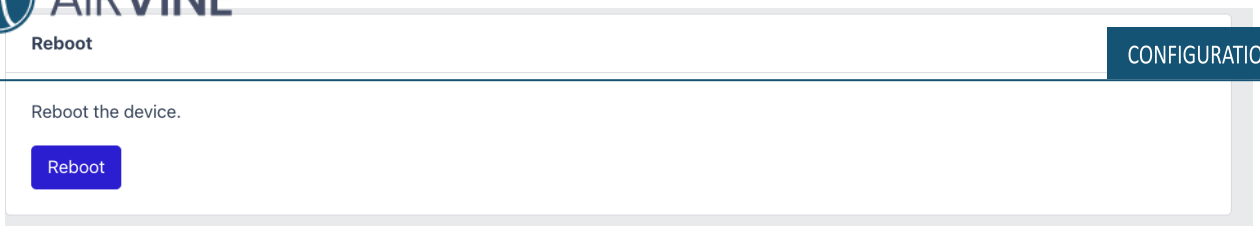


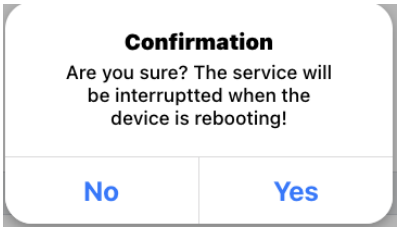
System Operations

Reboot the WaveTunnel device

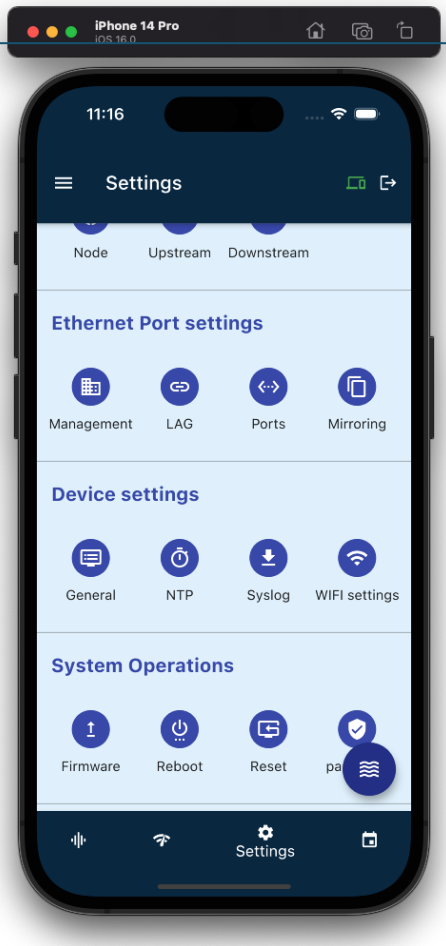
To reboot the WaveTunnel device, you can issue the request from the interfaces below. It takes a few minutes for the WaveTunnel device to come back.

[WEB GUI]
Operations-> System Operations-> Reboot





[Mobile App]
Settings -> Reboot



[CLI]

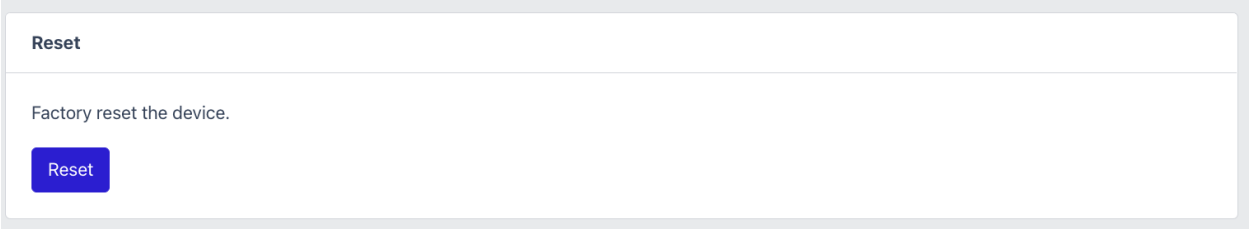
Operation-> reboot

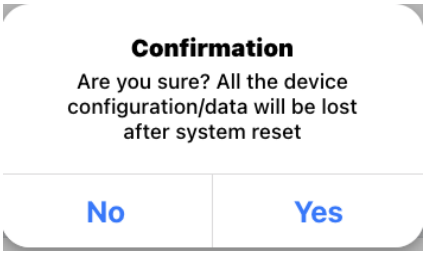
```
AVS> enable
Password:
AVS# operation
AVS(operation)#

Help:
         reboot - Reboot the device
          reset - Factory reset the device
           diag - Execute troubleshooting command
            log - Log files commands
         backup - Backup the device configurations
        restore - Restore the device configurations
         mirror - Port mirroring settings
             .. - Navigate up one category
           exit - Exit Command line interface


AVS(operation)# reboot
Do you want to reboot this device? (y/n):
```

Reset the WaveTunnel device

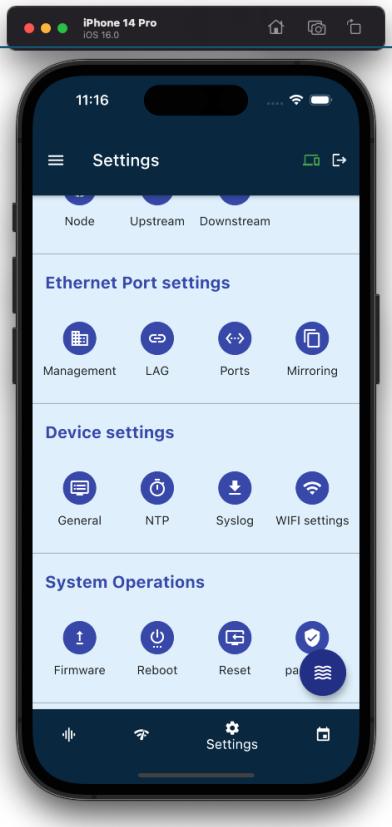
To reset the WaveTunnel device, you can issue the request from the interfaces below. To be aware that all the configurations and user data will be lost after this reset operation.

[WEB GUI]
Operations-> System Operations-> Reset





[Mobile App]
Settings -> Reset



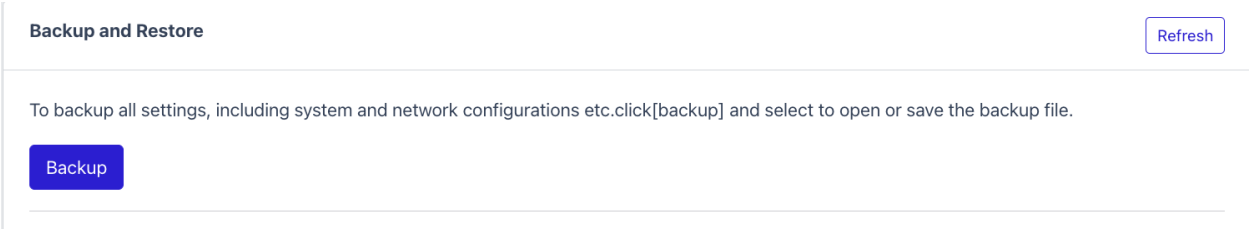
[CLI]
Operation -> reset

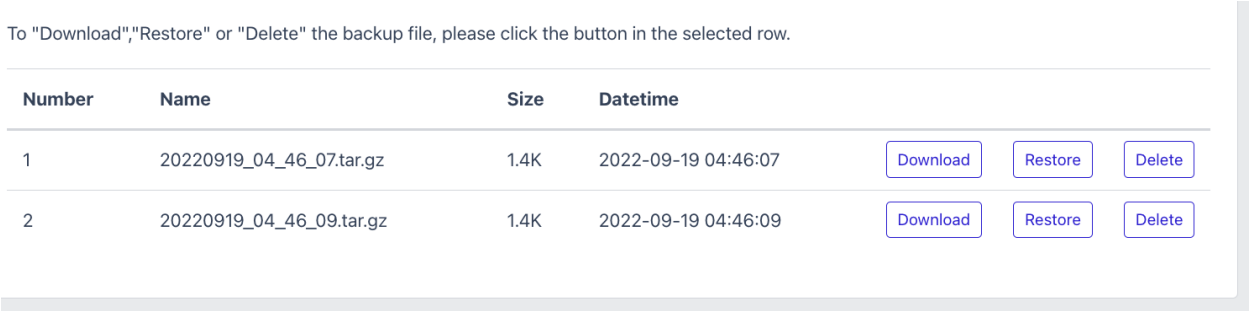
Backup the configurations of the WaveTunnel device

On this page, you can back up the configurations of the WaveTunnel device for future use.For example, rollback to the earlier settings or restore it to another replacement device. You can also download the backup file to your local computer to avoid losing the configurations if the

device runs into the abnormal state. The max. Number of configurations that can be backup is up to 10.

[WEB GUI]
Operations-> System Operations-> Backup





[CLI]
Operation -> backup

ssh admin@10.16.113.10

```
AVS(operation-backup)#

Help:
           list - List out the current backup files
        execute - Execute the backup command
         delete - Delete the backup file
             .. - Navigate up one category
           exit - Exit Command line interface


AVS(operation-backup)# execute
tar: removing leading '/' from member names

Backup the device configurations successfully
AVS(operation-backup)# list
```

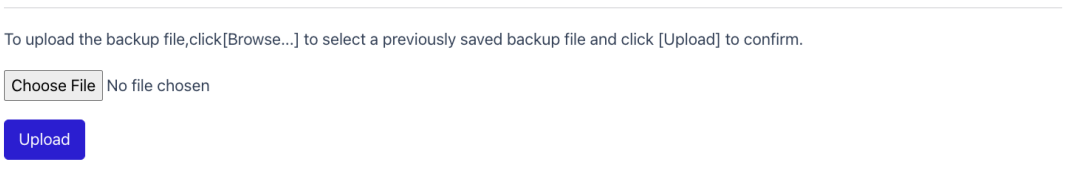
Number	Name	Size	Datetime
1	20220831_22_01_39.tar.gz	1.0K	2022-08-31 22:01:40
2	20220914_18_04_11.tar.gz	1.0K	2022-09-14 18:04:11
3	20220922_23_27_52.tar.gz	1.0K	2022-09-22 23:27:52

```
AVS(operation-backup)# delete 1

The backup file 20220831_22_01_39.tar.gz has been deleted
AVS(operation-backup)#
```

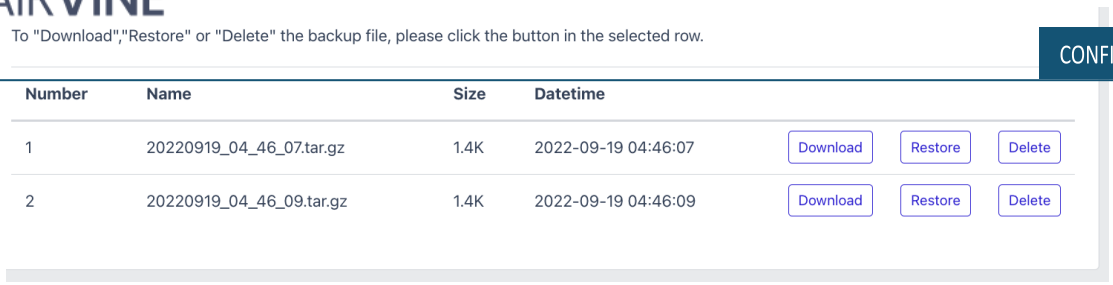
Restore the configurations from the Backup file

[WEB GUI]
Operations-> System Operations-> Restore

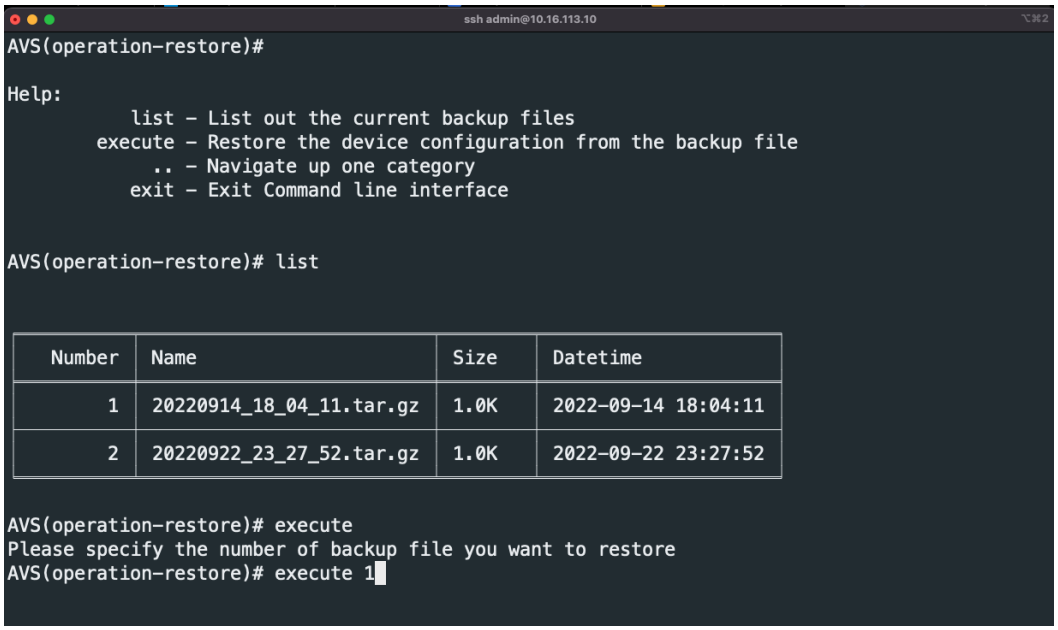
Upload the backup file from your laptop.



Restore the configurations from the old backup file.



[CLI]
Operation-> restore

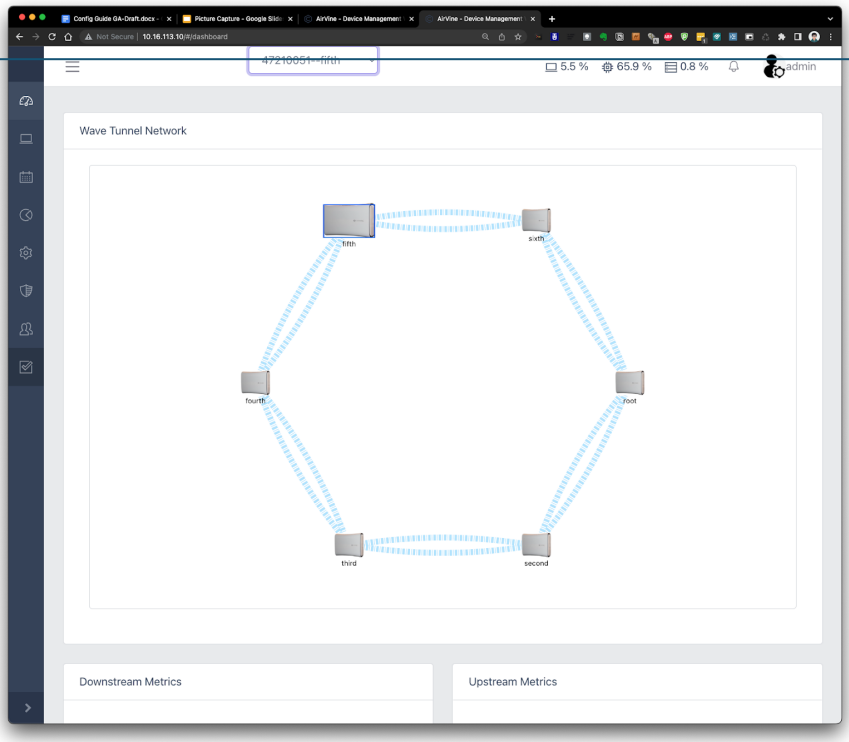


Diagnostic and troubleshooting

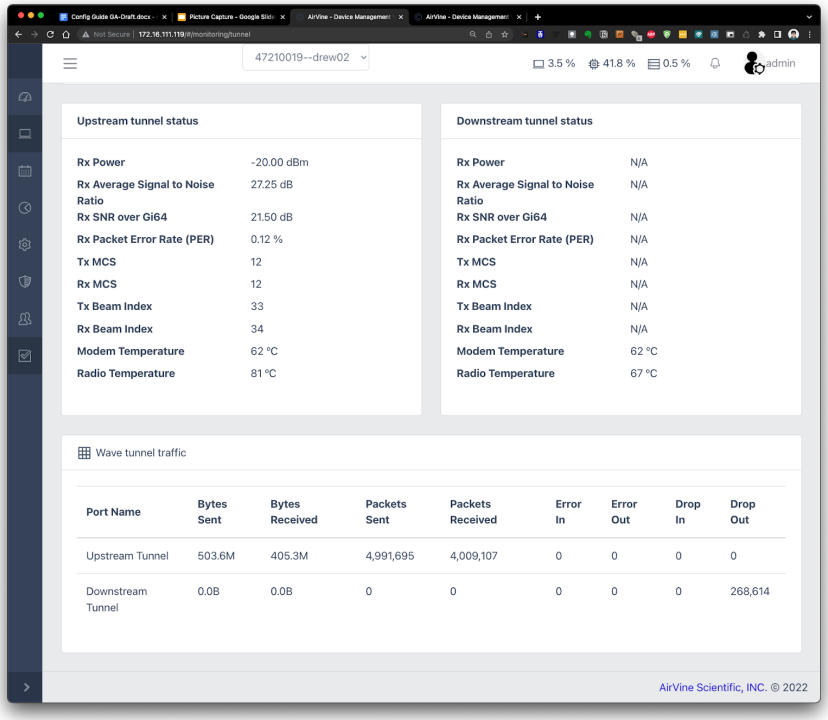
Checking the Status of the WaveTunnel connections

To check the status of the connections of WaveTunnel devices, there are several pages you can visit to get the information. See the explanations in the following sections.

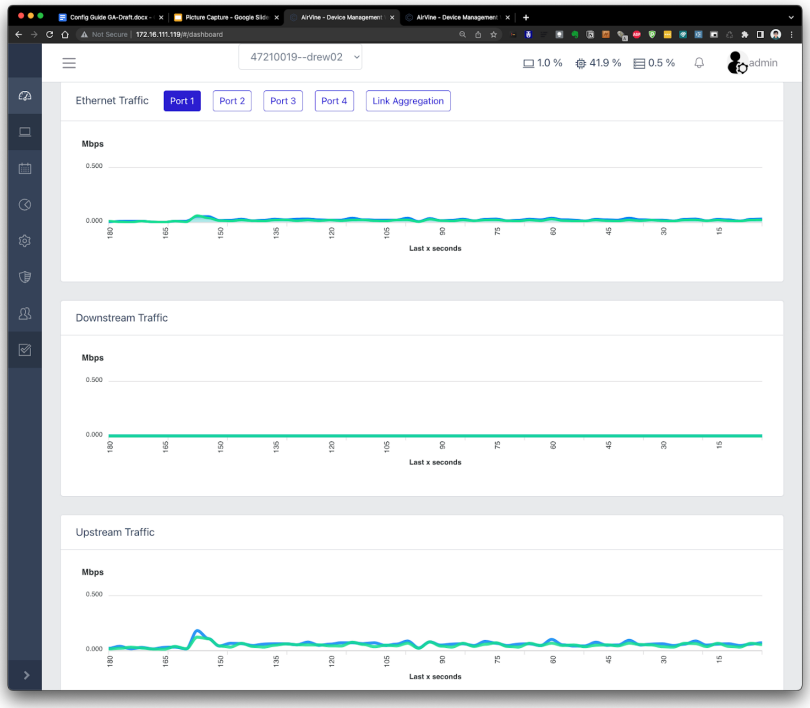
[WEB GUI]
Tunnel Topology
Check the status of connections of your devices and how they are connected. Mouse hover to the device or the link to see more information.



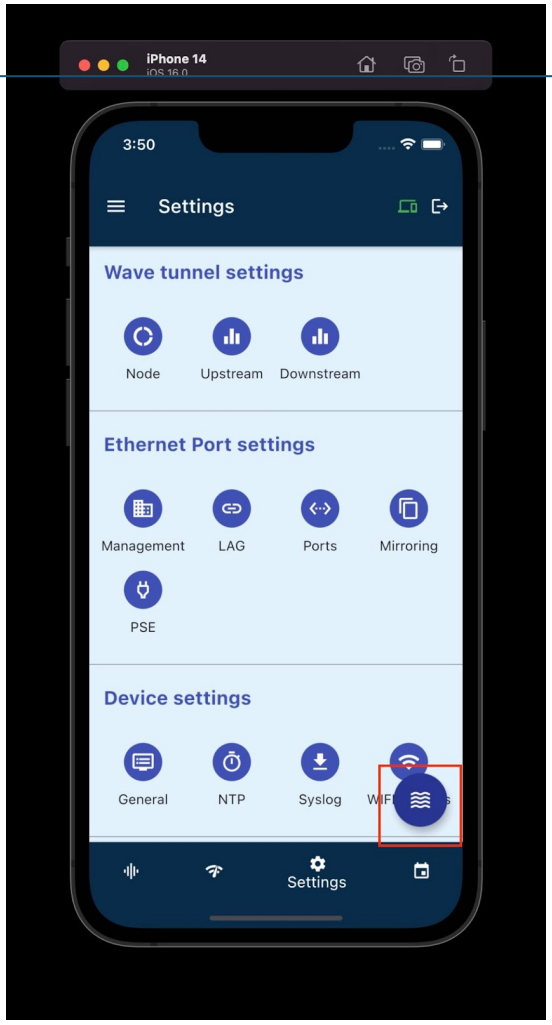
You can check the upstream/downstream tunnel metrics from the “Monitoring-> Wave Tunnel” page.

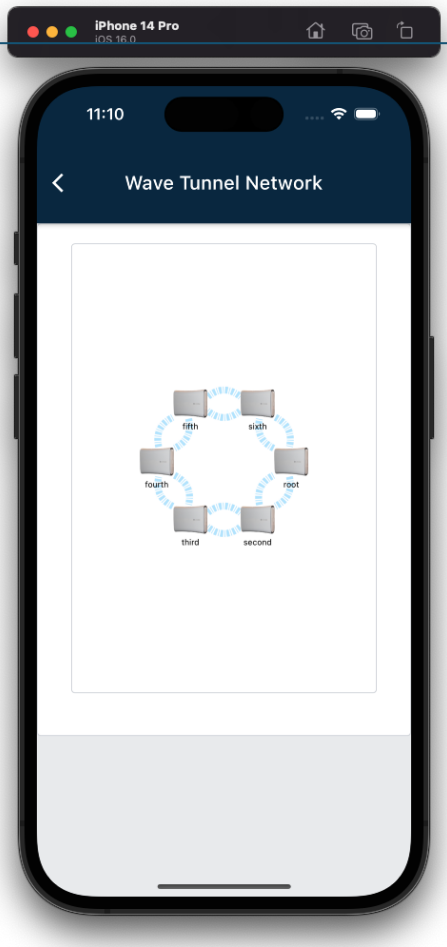


You can also check the realtime traffic widgets on the Dashboard to see the traffic/bandwidth of your wave tunnel connections.



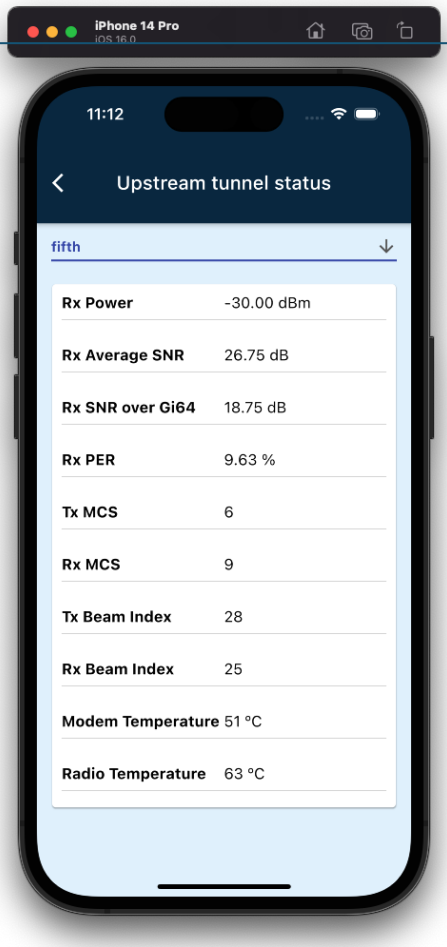
[Mobile App]
Click the button to check the WaveTunnel connection status.


iPhone 14
3:50
Settings
Wave tunnel settings
Node
Upstream
Downstream
Ethernet Port settings
Management
LAG
Ports
Mirroring
PSE
Device settings
General
NTP
Syslog
Settings

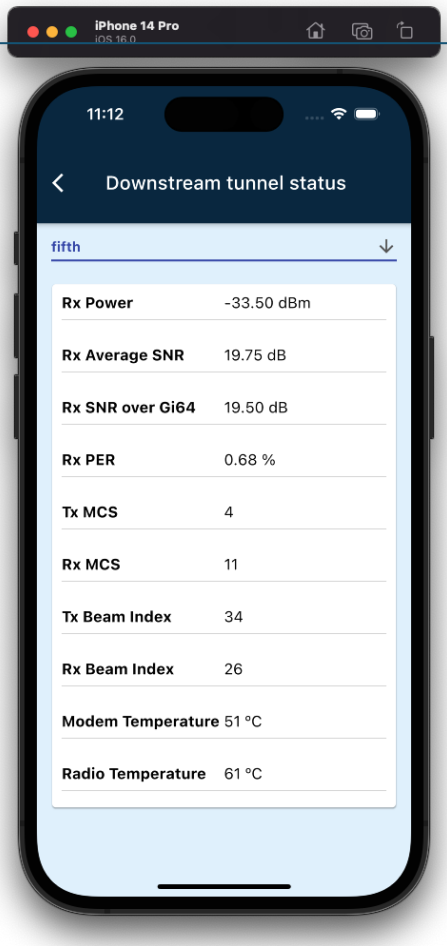


From Dashboard, you can check the real time traffic/bandwidth passing through the WaveTunnel connections.

Check the upstream connection metrics

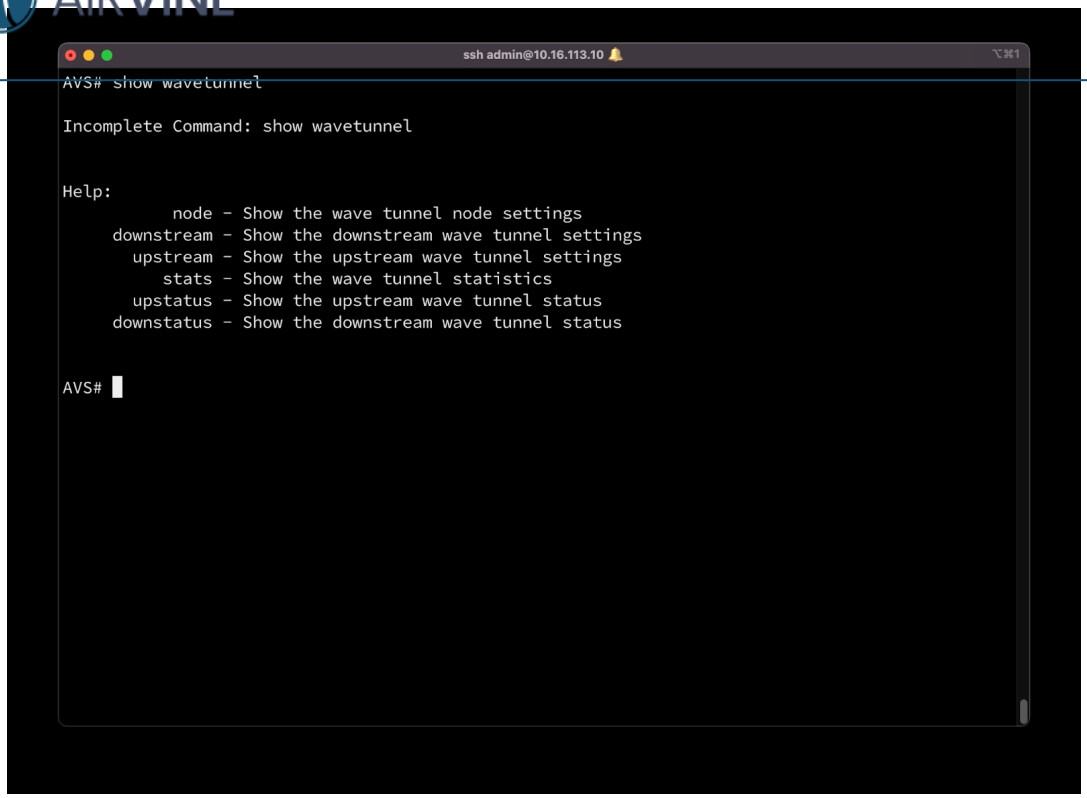


Check the downstream connection metrics



[CLI]

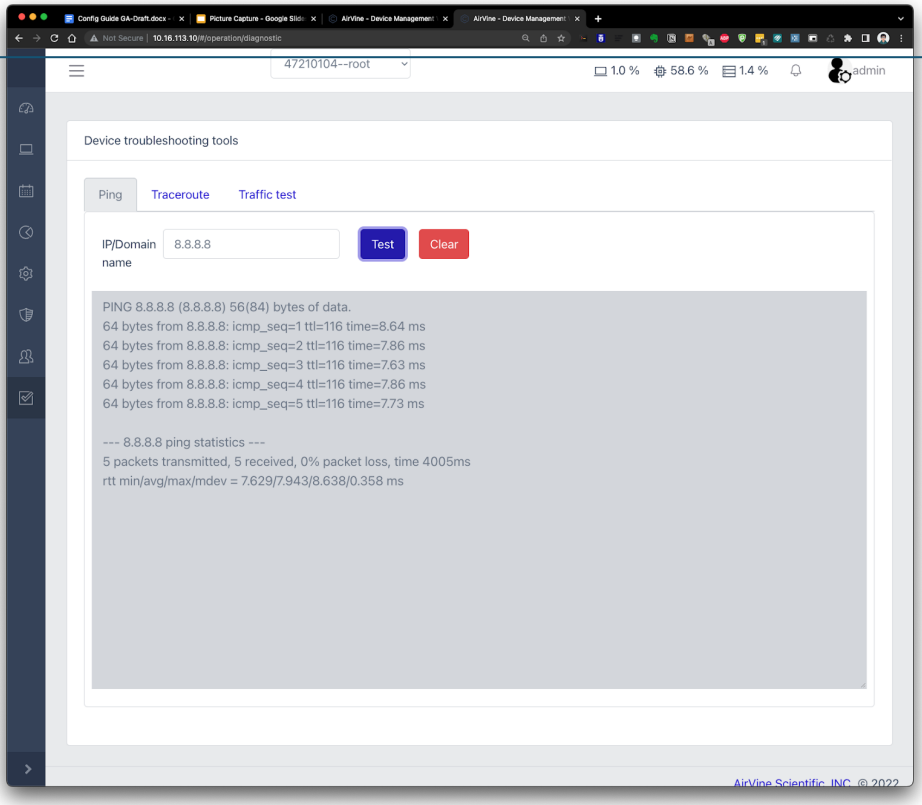
show wavetunnel stats
show wavetunnel upstatus
show wavetunnel downstatus



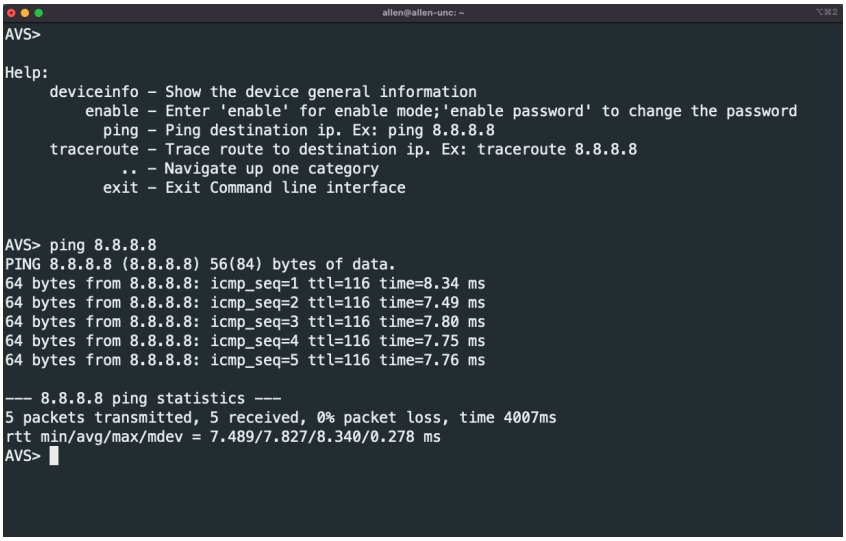
Ping Test

You can run a “Ping” test to check if the traffic can be sent to the destination.

[WEB GUI]
System > Operations > Diagnostic > Ping



[CLI]

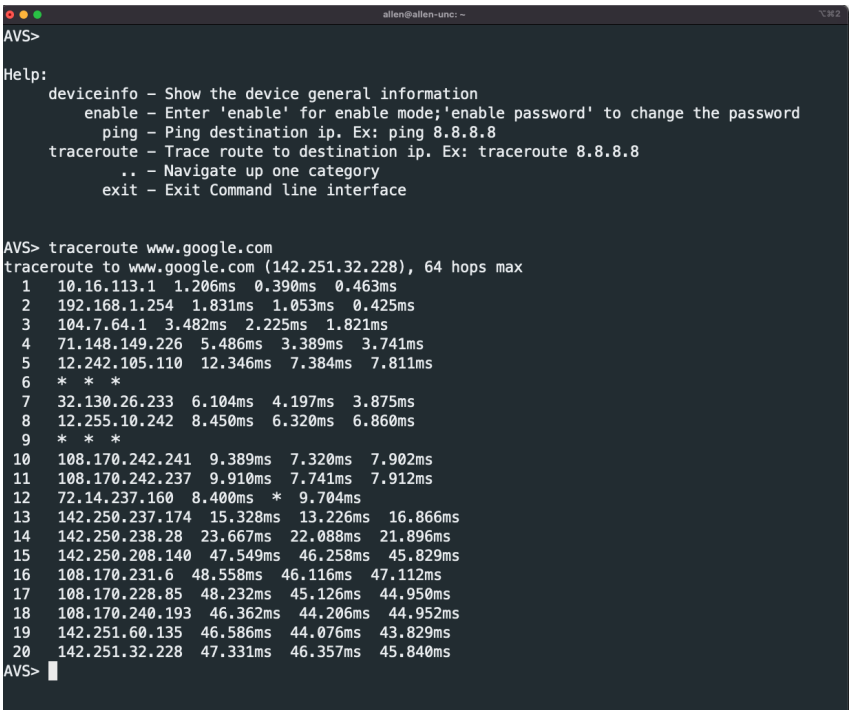


Traceroute Test

You can run a “Traceroute” test to check how the packets are routed to the destination.

[WEB GUI]

[CLI]

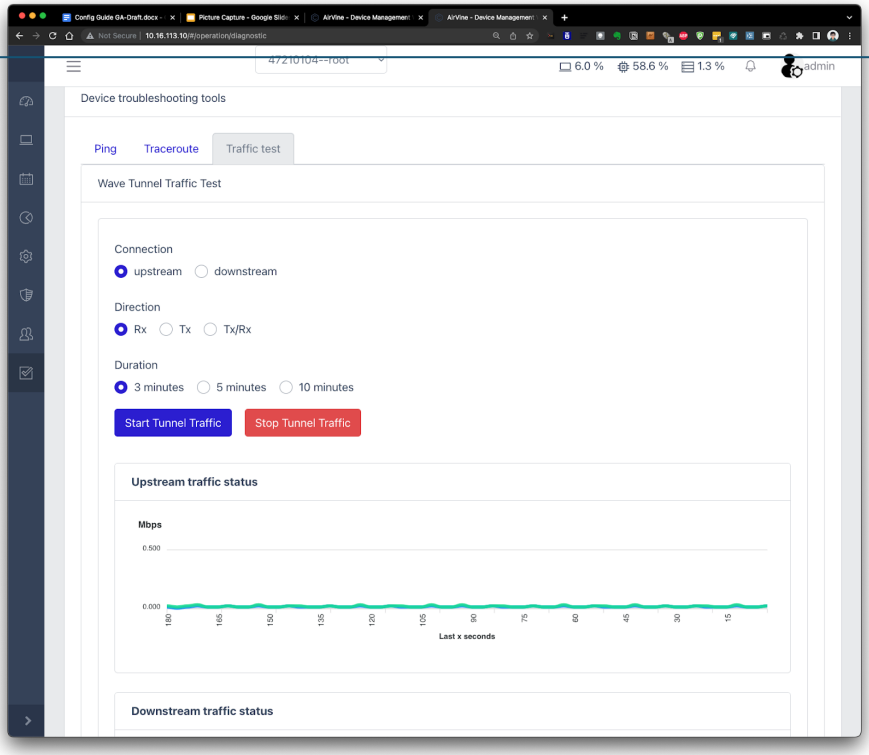


Traffic Test

There is an internal tool in the WaveTunnel we can use to generate the traffic on the WaveTunnel connections.

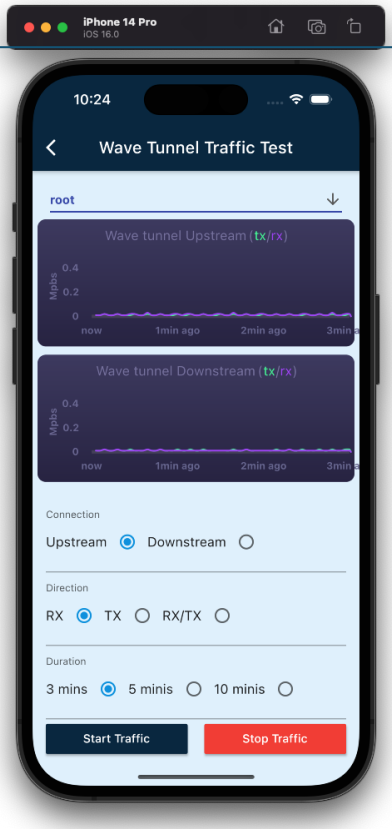
[WEB GUI]
System > Operations > Diagnostic > Traffic Test

Specify the criteria before generating the traffic and monitor the result on the widgets.



[Mobile App]
Monitoring > Link Traffic

Specify the criteria before generating the traffic and monitor the result on the widgets.



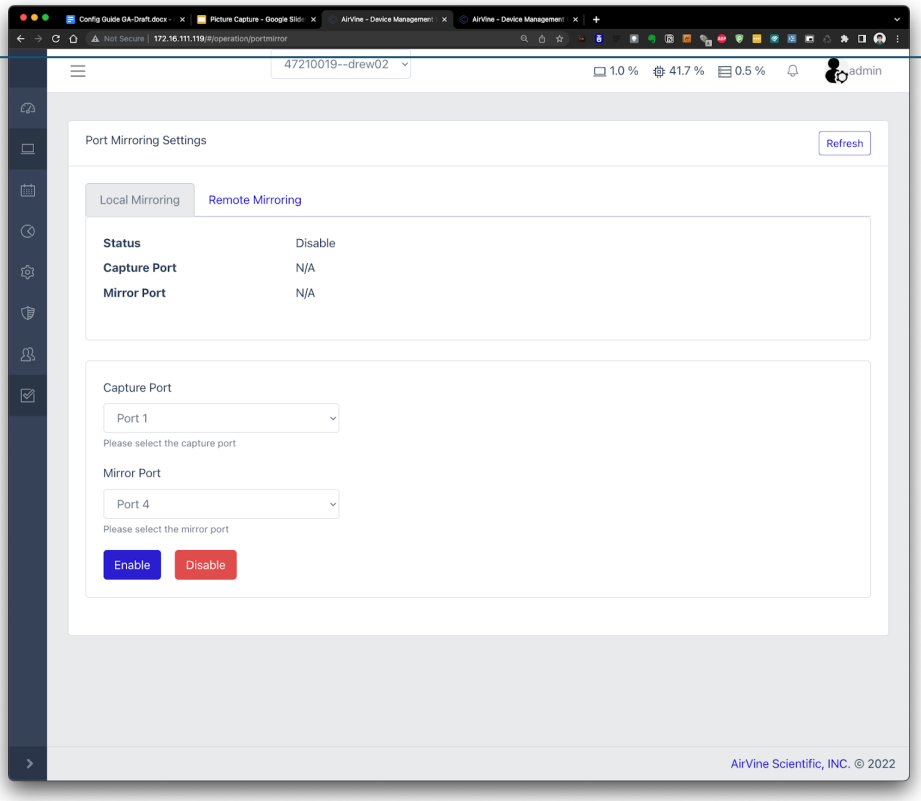
Mirroring the Ethernet Port traffic

For the troubleshooting purposes, this function provides the capability to mirror the packets on a specific port to another port in the local or neighboring device. To be aware, the settings are not persisted which are cleaned up after system reboot.

[WEB GUI]
System > Operations > Port Mirroring

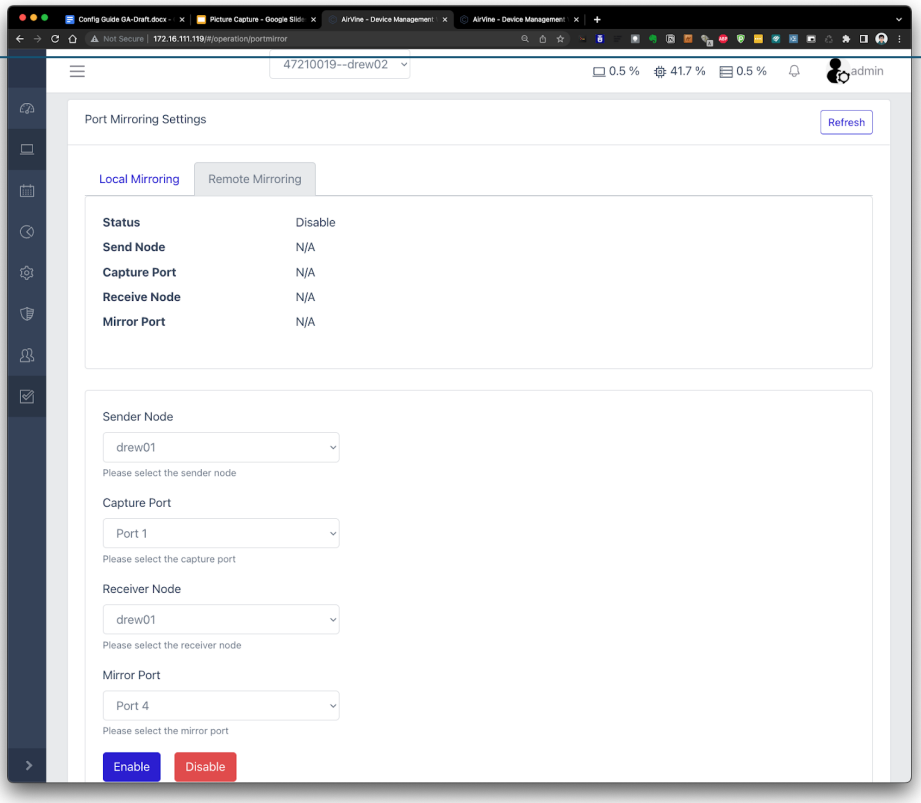
Local Port Mirroring

Operations-> Port Mirroring-> Local



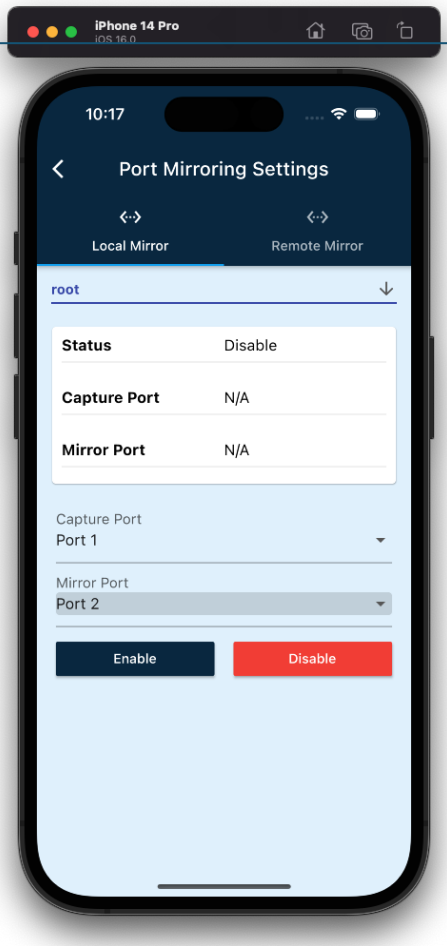
Remote Port Mirroring

Operations-> Port Mirroring-> Remote

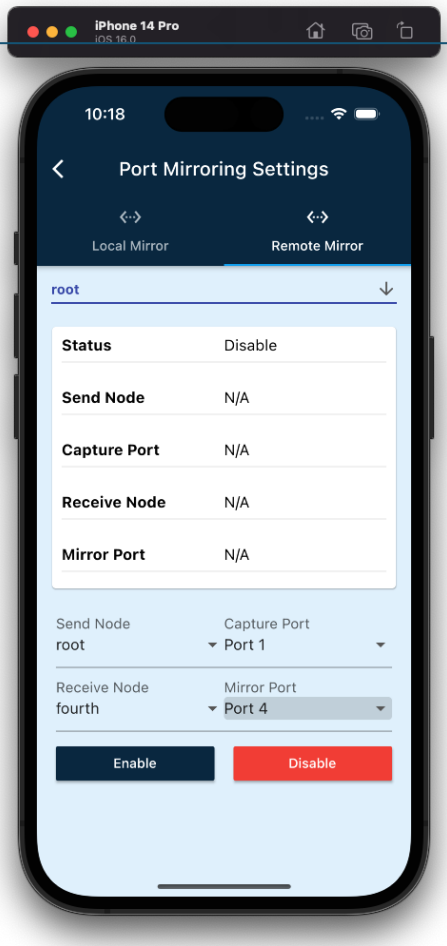


[Mobile App]

Settings > Mirroring > Local Mirroring

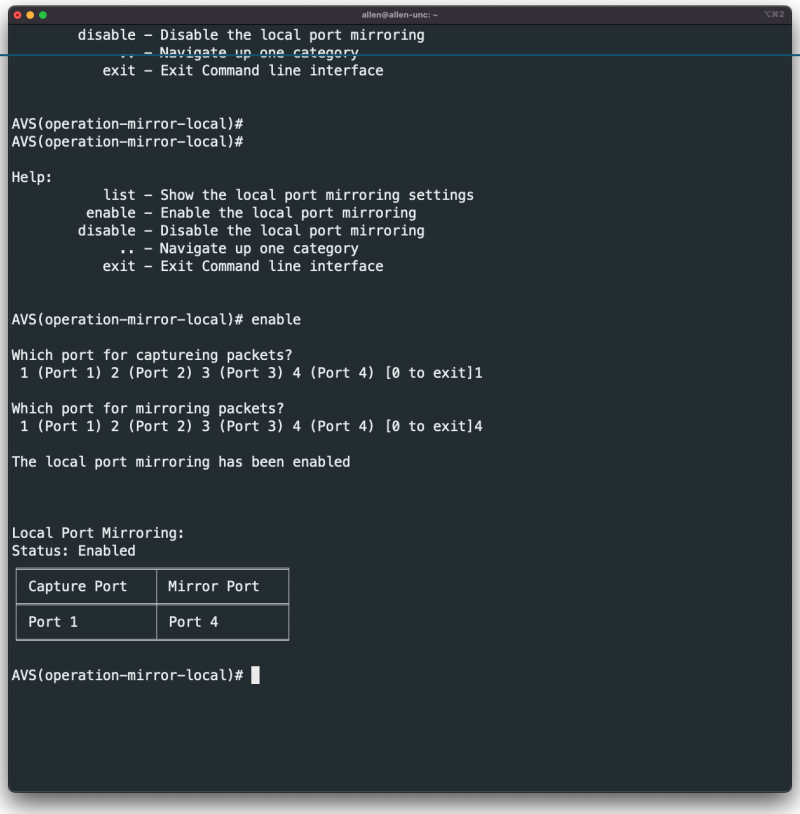


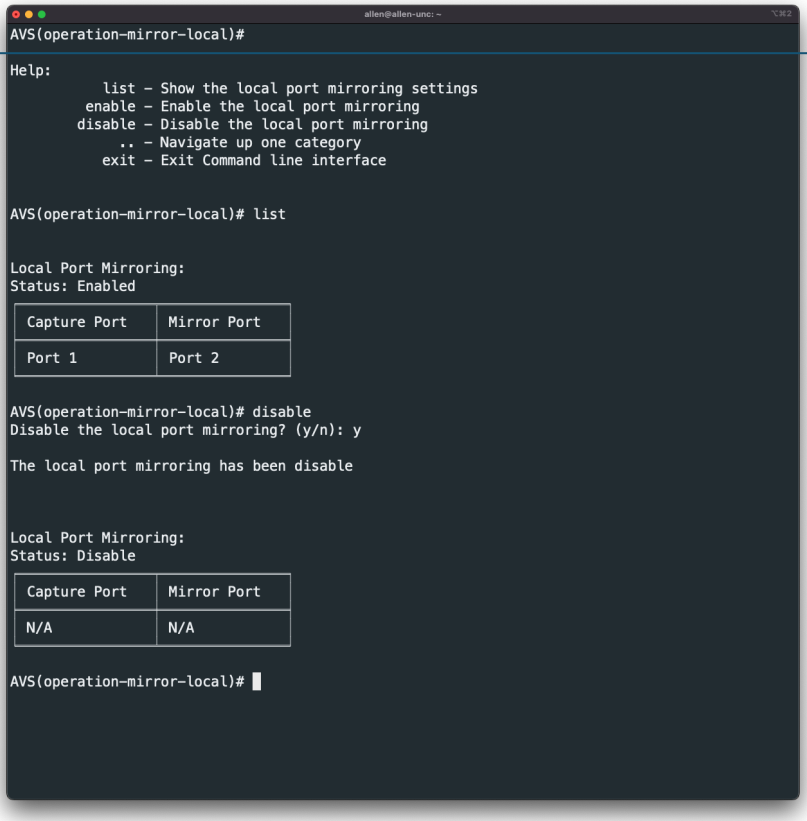
Settings > Mirroring > Remote Mirroring



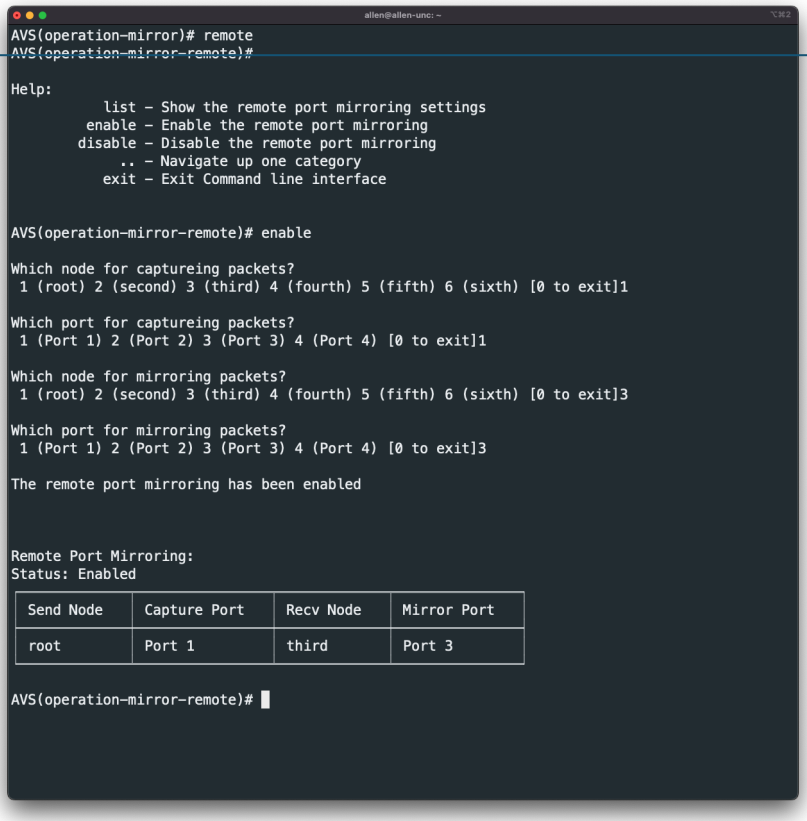
[CLI]

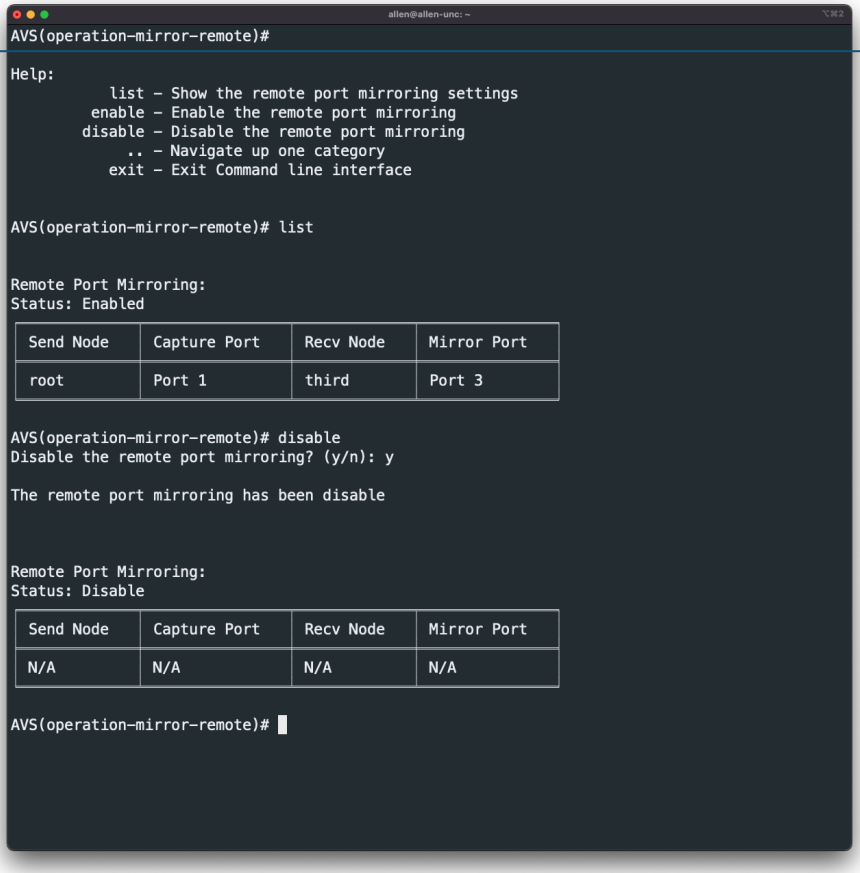
AVS(operation-mirror-local)#


allen@allen-unc: ~
disable – Disable the local port mirroring
.. – Navigate up one category
exit – Exit Command line interface
AVS(operation-mirror-local)#
AVS(operation-mirror-local)#
Help:
list – Show the local port mirroring settings
enable – Enable the local port mirroring
disable – Disable the local port mirroring
.. – Navigate up one category
exit – Exit Command line interface
AVS(operation-mirror-local)# enable
Which port for captureing packets?
1 (Port 1) 2 (Port 2) 3 (Port 3) 4 (Port 4) [0 to exit]1
Which port for mirroring packets?
1 (Port 1) 2 (Port 2) 3 (Port 3) 4 (Port 4) [0 to exit]4
The local port mirroring has been enabled
Local Port Mirroring:
Status: Enabled
Capture Port
Mirror Port
Port 1
Port 4
AVS(operation-mirror-local)#



AVS(operation-mirror-remote)#

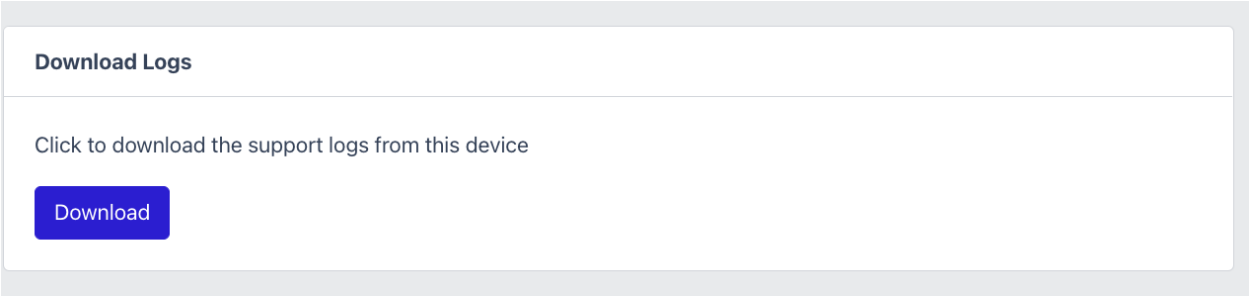

allen@allen-unc: ~
AVS(operation-mirror)# remote
AVS(operation-mirror-remote)#
Help:
list - Show the remote port mirroring settings
enable - Enable the remote port mirroring
disable - Disable the remote port mirroring
.. - Navigate up one category
exit - Exit Command line interface
AVS(operation-mirror-remote)# enable
Which node for captureing packets?
1 (root) 2 (second) 3 (third) 4 (fourth) 5 (fifth) 6 (sixth) [0 to exit]1
Which port for captureing packets?
1 (Port 1) 2 (Port 2) 3 (Port 3) 4 (Port 4) [0 to exit]1
Which node for mirroring packets?
1 (root) 2 (second) 3 (third) 4 (fourth) 5 (fifth) 6 (sixth) [0 to exit]3
Which port for mirroring packets?
1 (Port 1) 2 (Port 2) 3 (Port 3) 4 (Port 4) [0 to exit]3
The remote port mirroring has been enabled
Remote Port Mirroring:
Status: Enabled
Send Node
Capture Port
Recv Node
Mirror Port
root
Port 1
third
Port 3
AVS(operation-mirror-remote)#

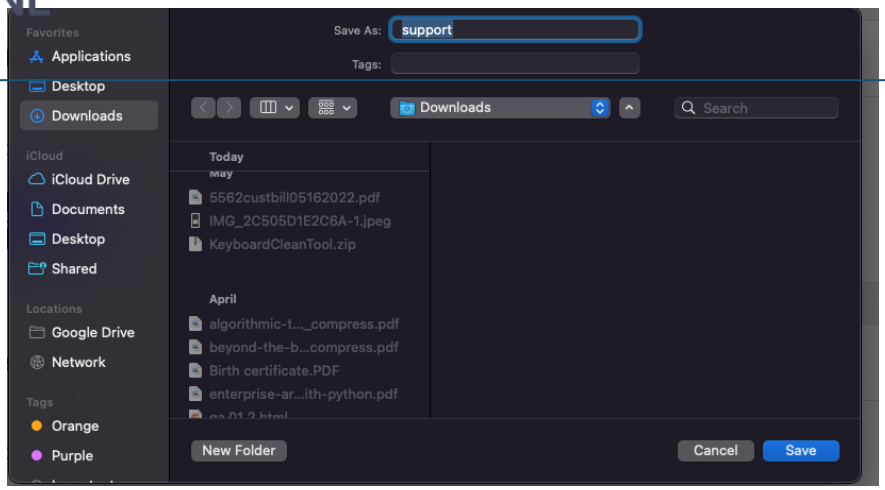


Download the Support Logs

You can download the support logs from this page and send it to Airvine support for further investigations.

[WEB GUI]
System > Operations > System Operation > Download Logs





Appendix

Event Code definition


```
{
 "101": {
  "description": "update configuration successfully",
  "type": "Admin",
  "severity": "Info",
  "notification": "False",
  "category": "Configuration"
 },
 "102": {
  "description": "update configuration failed",
  "type": "Admin",
  "severity": "Error",
  "notification": "True",
  "category": "Configuration"
 },
 "103": {
  "description": "country code changed",
  "type": "Admin",
  "severity": "Warning",
  "notification": "False",
  "category": "Configuration"
 },
 "104": {
```

```
    "description": "timezone changed",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "Configuration"
  },
  "105": {
    "description": "user added",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "User"
  },
  "106": {
    "description": "user deleted",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "User"
  },
  "107": {
    "description": "configuration backup",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "Configuration"
  },
  "108": {
    "description": "configuration restored successfully",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "Configuration"
  },
  "109": {
    "description": "configuration restored failed",
    "type": "Admin",
    "severity": "Error",
    "notification": "True",
    "category": "Configuration"
  },
  "110": {
    "description": "Device support log files have been downloaded",
    "type": "Admin",
```

```
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "111": {
    "description": "firmware upgraded successfully ",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "112": {
    "description": "firmware upgraded failed",
    "type": "Admin",
    "severity": "Error",
    "notification": "True",
    "category": "System"
  },
  "113": {
    "description": "firmware image corrupted",
    "type": "Admin",
    "severity": "Error",
    "notification": "True",
    "category": "System"
  },
  "114": {
    "description": "Configuration rollback",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "Configuration"
  },
  "115": {
    "description": "Change primary firmware blank",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "116": {
    "description": "Change primary firmware blank failed",
    "type": "Admin",
    "severity": "Critical",
    "notification": "True",
```

```
    "category": "System"
  },
  "117": {
    "description": "Download the firmware image from server",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "118": {
    "description": "Download the firmware image from server failed",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "System"
  },
  "119": {
    "description": "Delete the firmware image file from the device",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "120": {
    "description": "Download the backup file",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "121": {
    "description": "Delete the backup file",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "System"
  },
  "122": {
    "description": "Set DHCP IP failed",
    "type": "Admin",
    "severity": "Critical",
    "notification": "True",
    "category": "System"
  },
```

```
  "201": {
    "description": "high CPU usage",
    "type": "Device",
    "severity": "Critical",
    "notification": "False",
    "category": "System"
  },
  "202": {
    "description": "high memory usage",
    "type": "Device",
    "severity": "Critical",
    "notification": "False",
    "category": "System"
  },
  "203": {
    "description": "insufficient disk space",
    "type": "Device",
    "severity": "Critical",
    "notification": "True",
    "category": "System"
  },
  "301": {
    "description": "upstream tunnel disconnected",
    "type": "Device",
    "severity": "Critical",
    "notification": "True",
    "category": "System"
  },
  "302": {
    "description": "downstream tunnel disconnected",
    "type": "Device",
    "severity": "Critical",
    "notification": "True",
    "category": "System"
  },
  "303": {
    "description": "weak upstream tunnel signal",
    "type": "Device",
    "severity": "Warning",
    "notification": "False",
    "category": "System"
  },
  "304": {
    "description": "weak downstream tunnel signal",
```

```
    "type": "Device",
    "severity": "Warning",
    "notification": "False",
    "category": "System"
  },
  "305": {
    "description": "upstream tunnel connected",
    "type": "Device",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "306": {
    "description": "downstream tunnel connected",
    "type": "Device",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "401": {
    "description": "new wifi client",
    "type": "Device",
    "severity": "Info",
    "notification": "False",
    "category": "User"
  },
  "402": {
    "description": "management SSID disable",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "Configuration"
  },
  "501": {
    "description": "device reboot",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "502": {
    "description": "device critical reboot",
    "type": "Device",
    "severity": "Warning",
```

```
    "notification": "False",
    "category": "System"
  },
  "601": {
    "description": "user login success",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "602": {
    "description": "use login failed",
    "type": "Admin",
    "severity": "Warning",
    "notification": "False",
    "category": "System"
  },
  "603": {
    "description": "user logout",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "604": {
    "description": "Add User",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  },
  "605": {
    "description": "Delete User",
    "type": "Admin",
    "severity": "Info",
    "notification": "False",
    "category": "System"
  }
}
```