

IP AUDIO BRIDGE

User Manual

SPA-B1000



IP Audio Bridge

User Manual

Copyright

©2024 Hanwha Vision Co., Ltd. All rights reserved.

Trademark

Each of trademarks herein is registered. The name of this product and other trademarks mentioned in this manual are the registered trademark of their respective company.

Restriction

Copyright of this document is reserved. Under no circumstances, this document shall be reproduced, distributed or changed, partially or wholly, without formal authorization.

Disclaimer

Hanwha Vision makes the best to verify the integrity and correctness of the contents in this document, but no formal guarantee shall be provided. Use of this document and the subsequent results shall be entirely on the user's own responsibility. Hanwha Vision reserves the right to change the contents of this document without prior notice.

※ Appearance, specification, etc. of the product is subject to change for performance improvements without prior notice.

The latest update is available on the official Hanwha Vision website. (www.HanwhaVision.com)

※ The ID for the initial login is "admin," and a password should be set.

Please change your password every three months to protect your personal data and prevent identity theft.

Please note that users are responsible for the security and other issues caused by insufficient password management.

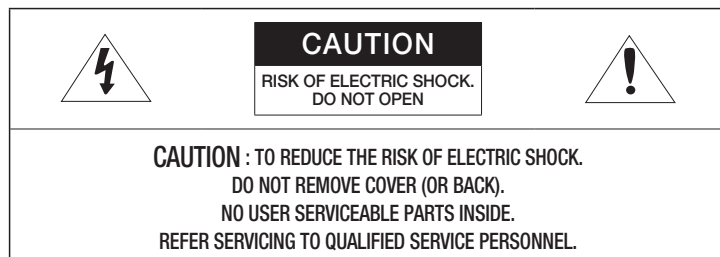
WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENINGS ON THE EQUIPMENT.

Apparatus shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the apparatus.

To prevent injury, this apparatus must be securely attached to the Wall/ceiling in accordance with the installation instructions.

CAUTION



EXPLANATION OF GRAPHICAL SYMBOLS



The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of “dangerous voltage” within the product’s enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

CAUTION

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

ATTENTION

IL Y A RISQUE D'EXPLOSION SI LA BATTERIE EST REMPLACÉE PAR UNE BATTERIE DE TYPE INCORRECT.

METTRE AU REBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS.

These servicing instructions are for use by qualified service personnel only.

To reduce the risk of electric shock do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.

The ITE is to be connected only to (PoE/PoE+) networks without routing to the outside plant.

The wired LAN hub providing power over the Ethernet (PoE/PoE+) in accordance with IEEE 802.3af/at shall be a UL Listed device with the output evaluated as a Limited Power Source as defined in UL60950-1 or PS2 as defined in UL62368-1.

Unit is intended for installation in a Network Environment 0 as defined in IEC TR 62102. As such, associated Ethernet wiring shall be limited to inside the building.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean the contaminated area on the product surface with a soft, dry cloth or a damp cloth.
(Do not use a detergent or cosmetic products that contain alcohol, solvents or surfactants or oil constituents as they may deform or cause damage to the product.)
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/ accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/ apparatus combination to avoid injury from tip-over.
13. To prevent injury, this apparatus must be securely attached to the Wall/ceiling in accordance with the installation instructions.
14. Unplug this apparatus during lightning storms or when unused for long periods of time.
15. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
16. This product is intended to be supplied by a Listed Power Supply Unit marked "Class 2" or "LPS" or "PS2" and rated from PoE(802.3af) : 44V-57V (), max 90mA / DC 24V (), max 110mA.
17. This product is intended to be supplied by isolation power.
18. If you use excessive force when installing the product, the product may be damaged and malfunction.
If you forcibly install the product using non-compliant tools, the product may be damaged.
19. Do not install the product in a place where chemical substances or oil mist exists or may be generated. As edible oils such as soybean oil may damage or warp the product, do not install the product in the kitchen or near the kitchen table.
This may cause damage to the product.
20. When installing the product, be careful not to allow the surface of the product to be stained with chemical substance.
Some chemical solvents such as cleaner or adhesives may cause serious damage to the product's surface.
21. If you install/disassemble the product in a manner that has not been recommended, the production functions/ performance may not be guaranteed.



22. Do not install on a surface where it is exposed to direct sunlight, near heating equipment or heavy cold area.
23. Do not place this apparatus near conductive material.
24. Do not attempt to service this apparatus yourself.
25. Do not place a glass of water on the product.
26. Do not install near any magnetic sources.
27. Do not place heavy items on the product.
28. Please wear protective gloves when installing/removing the product.
The high temperature of the product surface may cause a burn.
29. This device has been verified using STP cable. The use of appropriate GND grounding and STP cable is recommended to effectively protect your product and property from transient voltage, thunderstroke, communication interruption.
30. In particular installation environments, there might be interference in radio communications.
When interference of electromagnetic waves occurs between the product and radio communication device, it is recommended to keep a certain distance between the two or change the direction of the receiving antenna.
31. An apparatus with CLASS I construction shall be connected to a MAINS socket outlet with a protective earthing connection.
32. Batteries(battery pack or batteries installed) shall not be exposed to excessive heat such as sunshine, fire or the like. The battery cannot be replaced.
33. Disconnect the main plug from the apparatus, if it's defected. And please call a repair man in your location.
34. Select an installation site that can hold at least 5 times the product's weight.
35. Stuck-in or peeled-off cables can cause damage to the product or a fire.
36. For safety purposes, keep anyone else away from the installation site.
And put aside personal belongings from the site, just in case.
37. We do not guarantee the quality of third-party products (e.g. accessories) that you separately purchase.

Table of Contents

OVERVIEW

3

4

6

6

7

Important Safety Instructions

At a glance

System configuration diagram

Connecting to other devices

STARTING

8

8

11

Connecting to a PC

Access Product

Logging In

ENVIRONMENT SETTINGS

12

12

15

15

16

16

17

17

18

System Management

Network Settings

Time Settings

snmp Action Settings

HTTPS Setting

IP Filtering Management

802.1x setting

Certificate management

USING THE IP AUDIO BRIDGE

19

19

19

23

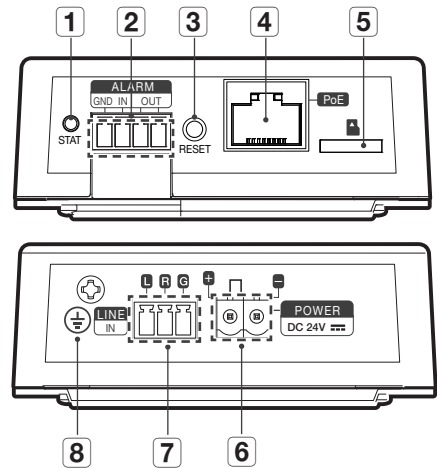
Home Screen Configuration

Operation Settings

Maintenance

AT A GLANCE

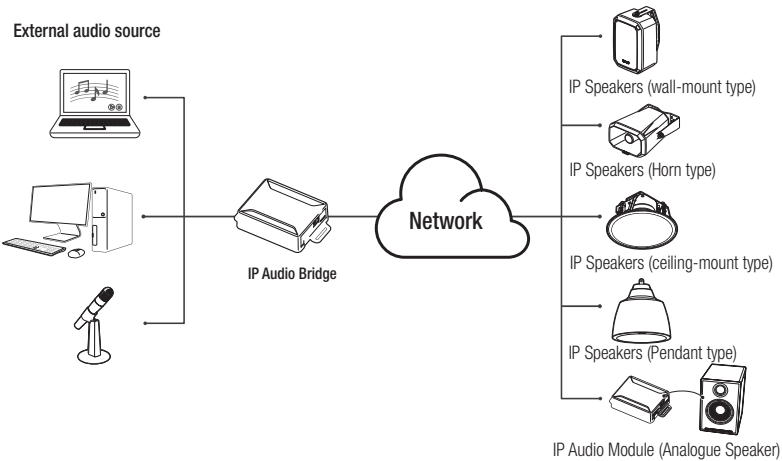
Side



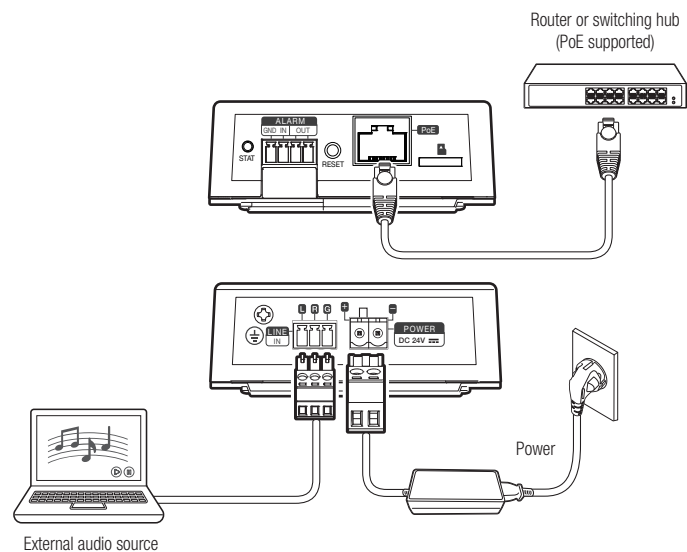
Name	Function Description
1 STATUS	When the initialization is in progress, the STATUS lamp blinks fast. When the initialization is completed, it blinks slowly in an interval of 1 second.
2 ALARM	ALARM IN: An alarm input terminal. ALARM OUT: An alarm output terminal. GND: It is a ground terminal.
3 RESET	A button that returns the product settings to the factory default values. Press the button for approximately 12 seconds, the STATUS lamp blinks at a fast speed, and when the reboot is completed after initialization, it blinks at a slow speed again. Do not disconnect the power until product resetting is complete. Doing so may cause malfunctions. It will take up to 10 minutes to reboot the product after initializing it.
4 Network Terminal	A terminal that connects a switching hub supporting PoE and a network cable for power and network connection.
5 micro SD card slot	A slot for a micro SD card.
6 POWER	Power input terminal (DC 24 V) DC
7 LINE IN	An input terminal used to connect to an external device.
8 Grounding port	Used for earth-grounding. Grounding serves to protect the product from lightning strikes. Before connection, be sure to turn off the power of the device.

SYSTEM CONFIGURATION DIAGRAM

Analog audio signals from the connected external devices can be transmitted to any IP speaker.



Connecting to other devices



Network Cable Specifications

Item	Specifications	Remark
Connector	RJ45 (10/100BASE-T)	
Ethernet	10/100Base-T	
Cable	Category 5e	
Max Distance	100 m	DC resistance ≤ 0.125 Ω/m
PoE Support	IEEE 802.3af	

! ■ When connecting to each device, be sure to power off the connected device before connecting.

Connecting to a Network

Connect the router or switching hub to the **NETWORK** port of the product using a network cable.

Network Connection to Power

Connect the router or switching hub using a network cable that provide PoE to the **NETWORK** port of the product.

- ! ■ For PoE, use equipment that supports the IEEE802.3af standard.
- If you connect to a PoE-supported switching hub, you can use the product without connecting a separate power source.
- To connect to the product's network, refer to "starting." (Page 8)

Connecting to Power

Connect the supplied power adapter's connector to the product's power input (DC 24V), and then connect the power cord to the power adapter.

CONNECTING TO A PC

The PC should be connected to the same network as the product when accessing the product for the first time. Use a network cable to connect the product's **NETWORK** port to the switching hub that is connected with the PC.



- The IP Audio Bridge can receive power via PoE, or the DC power adapter can be used.

ACCESS PRODUCT

Various functions, including Operation Mode, System Settings, Maintenance, Environment Setting, and Operation Settings, are available on the product website.

1. Set an IP address to 192.168.1.x, the same band as the product, in the Network Property of the PC.

2. Run a web browser on the PC.



- An available web browser is Google Chrome (Version 92.0.4515.131 or higher). Google Chrome is available at www.google.com/chrome.
- It can be used in Chrome as it is a supported web browser. For the computer OS, it can be used in Windows 10 or Mac 11.6 (Big Sur) or 12.2 (Monterey).

3. The initial IP address of all products is 192.168.1.100.
Before installing the product, it is recommended to set a static IP address for separate products.



- If multiple products are connected concurrently to the same switch hub with the initial IP addresses, the web page cannot distinguish the IP addresses, resulting in failing to set passwords.
Use Device Manager to set the initial password and IP address to use.

Registering using Device Manager

If the product is connected to a network which includes a computer where the device manager is installed, you can search products, set up passwords, change IP addresses, upgrade firmware, and access web pages.

Please refer to the manual of the Device Manager Program for more information.



- The Device Manager Program () is available on the official Hanwha Vision website (<https://www.HanwhaVision.com>) by clicking <Support> - <Online Tool>.

WISNET

Project | System | Network | Help

Search

Add Devices | Credentials | IP Assign

Report | FW | Config

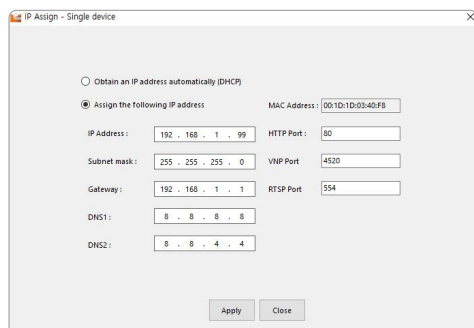
Tools

Save State | Save All | Save

- Select a product to set its IP address, and enter the IP address to use (e.g., Set Static IP).

When you select products one by one

- Select **<Assign the following IP address>** from the **[IP Assign]** menu, then set its IP address.
- The DNS server address is automatically set as the product's initial DNS address (DNS1 8.8.8.8, DNS2 8.8.4.4).



IP Assign - Single device

☐ Obtain an IP address automatically (DHCP)

☒ Assign the following IP address

MAC Address: 00:1D:03:40:F8

IP Address: 192 . 168 . 1 . 99 HTTP Port: 80

Subnet mask: 255 . 255 . 255 . 0 VNP Port: 4520

Gateway: 192 . 168 . 1 . 1 RTSP Port: 554

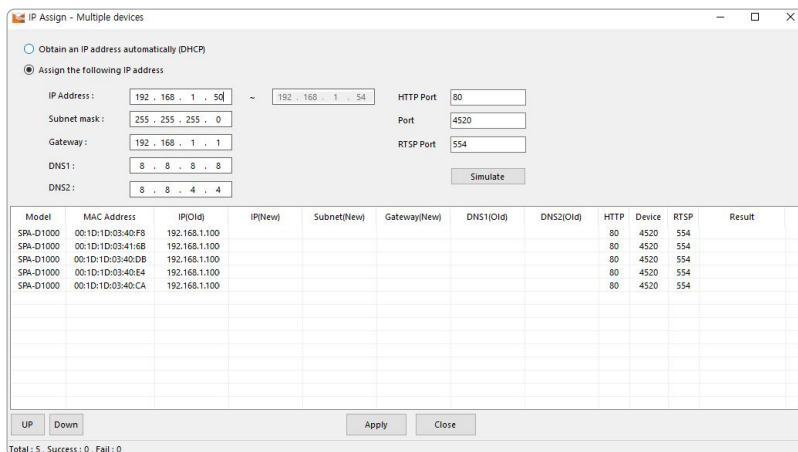
DNS1: 8 . 8 . 8 . 8

DNS2: 8 . 8 . 4 . 4

Apply Close

When you select multiple products

- Select **<Assign the following IP address>** from the **[IP Assign]** menu. Then apply the starting address in the range of IP addresses to be assigned.



IP Assign - Multiple devices

☐ Obtain an IP address automatically (DHCP)

☒ Assign the following IP address

IP Address: 192 . 168 . 1 . 54 ~ 192 . 168 . 1 . 54 HTTP Port: 80

Subnet mask: 255 . 255 . 255 . 0 Port: 4520

Gateway: 192 . 168 . 1 . 1 RTSP Port: 554

DNS1: 8 . 8 . 8 . 8

DNS2: 8 . 8 . 4 . 4

Simulate

Model	MAC Address	IP(Old)	IP(New)	Subnet(New)	Gateway(New)	DNS1(Old)	DNS2(Old)	HTTP	Device	RTSP	Result
SPR-D1000	00:1D:03:40:F8	192.168.1.100						80	4520	554	
SPR-D1000	00:1D:03:41:6B	192.168.1.100						80	4520	554	
SPR-D1000	00:1D:03:40:DB	192.168.1.100						80	4520	554	
SPR-D1000	00:1D:03:40:E4	192.168.1.100						80	4520	554	
SPR-D1000	00:1D:03:40:CA	192.168.1.100						80	4520	554	

UP Down Apply Close

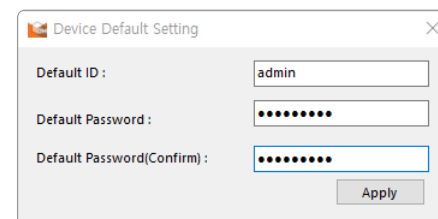
Total : 5 , Success : 0 , Fail : 0

- When you select **<Obtain an IP address automatically (DHCP)>** from the **[IP Assign]** menu, the DHCP IP address is automatically assigned.
- The HTTP port supports only the number 80, and the VNP and RTSP ports are not used in the IP audio product.

- Products with IP addresses must be logged in from the **[Credential]** menu to be queried as **<Login OK>**.

- When you execute **<New Project>** → **<Search>**, authentication is canceled and the product is queried as **<Login Fail>**.

- If you apply the product password in **<System>** → **<Device Default Credential setting>** in the device manager, it is automatically queried as **<Login OK>** even when you search for it as a new project or re-execute the device manager.



Device Default Setting

Default ID : admin

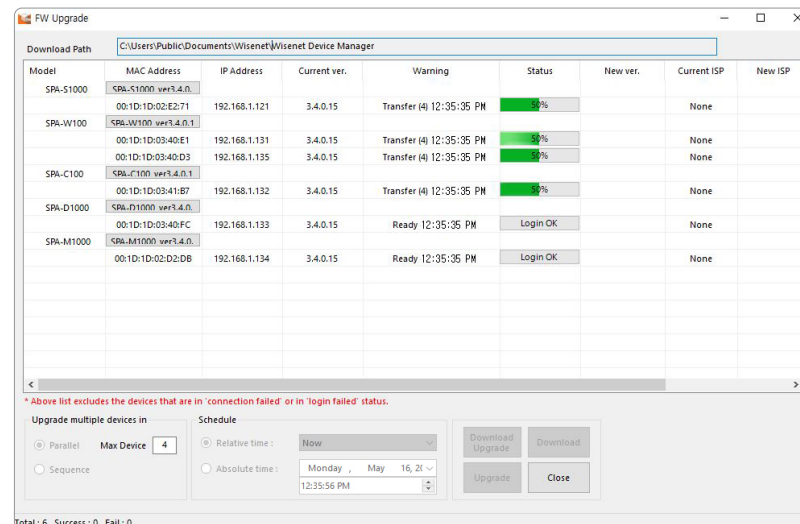
Default Password :

Default Password(Confirm) :

Apply

- You can update to the latest firmware for the product using the device manager. Select the searched product in the Device Manager and run **<FW Status Check>** in the **[FW]** menu to get the firmware status (the latest or previous version).
- Check the firmware distribution information for each product on the Hanwha Vision website (<https://www.HanwhaVision.com>) and download the latest firmware (modelname_version.imkp) to your PC. You can also download the latest firmware to your PC from Device Manager.

- When selecting firmware for each product and running **[Upgrade]**, the status will change from **<Login OK>** to **<Progress %>**.



FW Upgrade

Download Path: C:\Users\Public\Documents\Wisenet\Wisenet Device Manager

Model	MAC Address	IP Address	Current ver.	Warning	Status	New ver.	Current ISP	New ISP
SPR-S1000	SPR-S1000 ver3.4.0	192.168.1.121	3.4.0.15	Transfer (4) 12:35:35 PM	Progress		None	
SPR-W100	SPR-W100 ver3.4.0.1	192.168.1.131	3.4.0.15	Transfer (4) 12:35:35 PM	Progress		None	
	00:1D:03:40:E1	192.168.1.135	3.4.0.15	Transfer (4) 12:35:35 PM	Progress		None	
SPR-C100	SPR-C100 ver3.4.0.1	192.168.1.132	3.4.0.15	Transfer (4) 12:35:35 PM	Progress		None	
	00:1D:03:41:B7							
SPR-D1000	SPR-D1000 ver3.4.0	192.168.1.133	3.4.0.15	Ready 12:35:35 PM	Login OK		None	
	00:1D:03:40:FC							
SPR-M1000	SPR-M1000 ver3.4.0	192.168.1.134	3.4.0.15	Ready 12:35:35 PM	Login OK		None	
	00:1D:03:40:DB							

* Above list excludes the devices that are in 'connection failed' or in 'login failed' status.

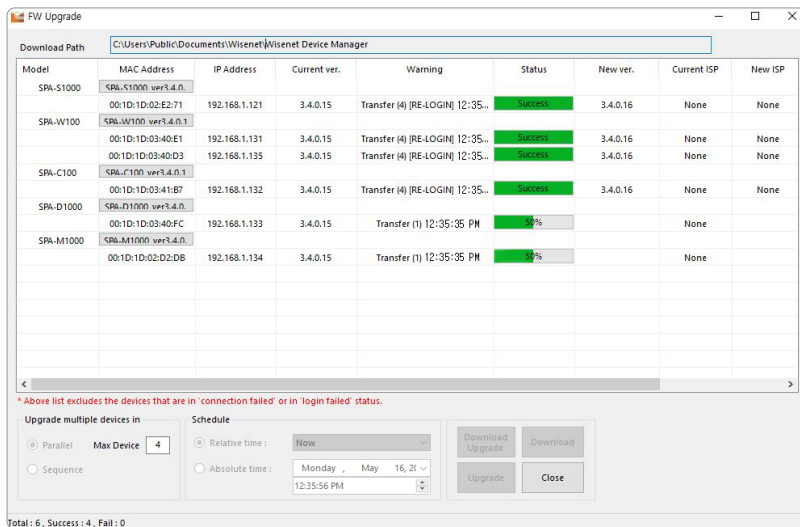
Upgrade multiple devices in: Parallel Max Device: 4

Schedule: Relative time: Now Absolute time: Monday, May 16, 2016 12:35:56 PM

Download Upgrade Download Upgrade Close

Total : 6 , Success : 0 , Fail : 0

- When the firmware update and reboot are complete, <Progress %> is displayed until 100% and then <Success> is displayed.
- If you update multiple products at the same time, the update will proceed sequentially by four units at a time.

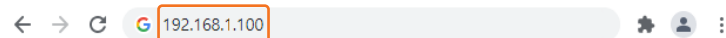


- The speakers and audio bridges share firmware, while the microphones and servers have their own firmware. The update will fail if inappropriate firmware is selected for the product. In such cases, please check whether suitable firmware has been chosen for the product and restart the update.
- The update failure status is indicated as follows:
Speaker/Audio Bridge: The status LED on the main body blinks rapidly.
Microphone: The 'Upgrading Wait' notification is displayed on the screen of the main body.
Server: The 'Upgrading Error' notification is displayed on the screen of the main body.

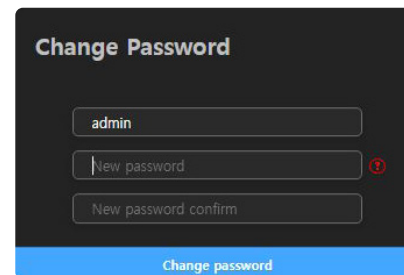
Registering with the product's initial IP address

If you connect only one product to the switch hub, it is possible to set up the password even on the web page.

- Enter the product's initial IP address into the web browser's address bar.

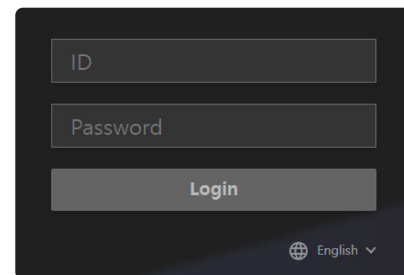


- The admin account password must be registered when accessing the product for the first time. When the <Change Password> window appears, please enter a new password.



- A password should contain 8 or more characters, and if it contains fewer than 9 characters, then a combination of 3 or more English uppercase/lowercase letters, numbers, or special characters must be used. If it includes 10 to 16 characters, a combination of 2 or more types must be used.
- It is recommended not to use the same character repeatedly or consecutive keyboard inputs as passwords for enhanced security.

- A product login screen appears after successfully setting the password.

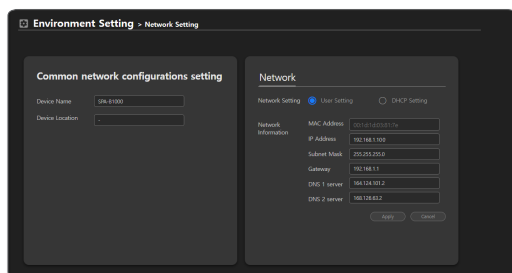


LOGGING IN

Use the password set for the admin account.

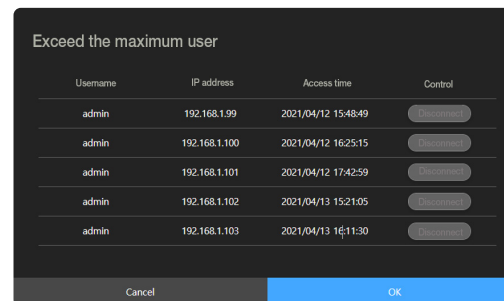
1. Enter "admin" in the <ID> field.
2. Enter a password in the <Password> field.
3. Click the [Login] button to move to the Home screen of the product.
After 30 minutes of inactivity on the website, you will be automatically logged out.

- If you forget the password, the product has to be initialized by pressing the RESET button for about 12 seconds. Therefore, make sure to write your password down or remember it.
If you have already logged in, the system can be initialized in the <Environment Setting> → <System Management> menu of the web page.
- Do not disconnect the power until the system initialization is complete after pressing the [RESET] button of the product or during product resetting. It will take up to 10 minutes to reboot the product after initializing it.
- To change the network settings according to the user's network connection configuration, use the <Network Setting> function in <Environment Setting>. (Page 15)



- Available accounts are divided into admin, setup, user, and guest by access authority level. Go to <Environment Setting> → <System Management> → <Change Password> to change the passwords of each account. (Page 12)

- A maximum of five users can log in to the product at the same time. The <Exceed the maximum user> screen will appear if there is an attempt to log in while the maximum number of users are logged in, and it will show the currently connected PC IP addresses.

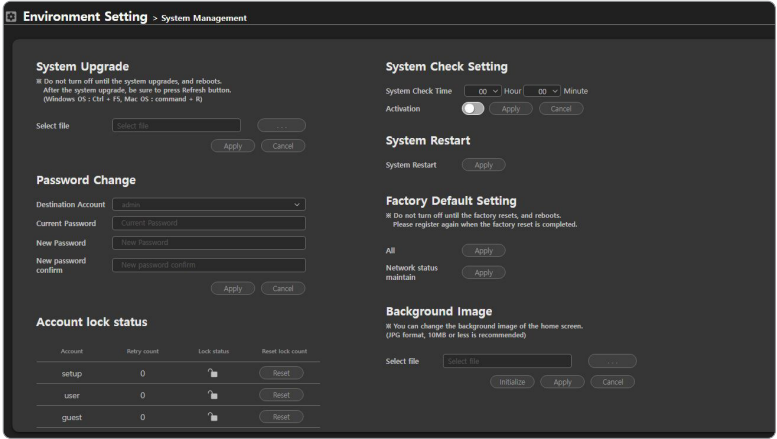


environment settings

The environment setting menu is a feature which is provided for both the controller-mode speaker and regular speaker.

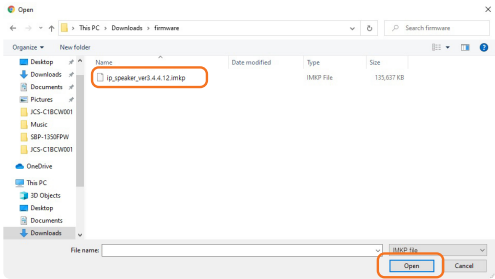
SYSTEM MANAGEMENT

Various functions are available, including System Upgrade, Change Password, System Check, Restart, and Reset.



Upgrading the System

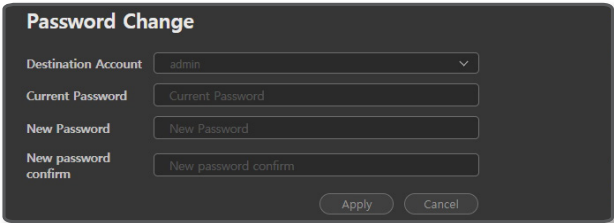
- Click <Environment Setting> → <System Management> on the Home screen.
- Click the [**System Upgrade**] button in <System Upgrade>.
- Select the upgrade file (model name_version.imkp) that you downloaded from the official Hanwha Vision website (<https://www.HanwhaVision.com>) in advance and click [Open].



- Click [Apply] to start System Upgrade. Click <OK> when the “System Restart” window appears after up to five minutes.
 - If you close the web browser or move to another menu before the “Restart the Program” message pops up, it may not be updated.
 - Do not disconnect the power in the middle of a system upgrade. Doing so may cause malfunctions.
- It will take up to 10 minutes to upgrade the system and reboot the product. The software version information of the product is available in the upper-right corner of the Home screen.

Changing the Password

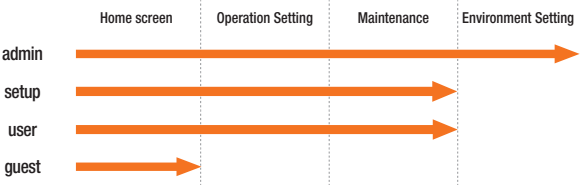
You can change the passwords of each account.



- On the Home screen, click <Environment Setting> → <System Management>.
- By clicking <Destination Account> from <Password Change>, select the account you want to change and set the password.
- Click the [Apply] button after entering a new password in the two input fields.
- The admin account can be changed if you enter the previous password. If you forgot the previous password, the product has to be initialized, and the passwords for all the accounts will be initialized during the process.
- The password of the setup, user, and guest accounts can be set, changed, or reset from the admin account if they are forgotten.

Viewing the supported menu by account

To prevent any confusion due to arbitrary changes to the settings and to continue stable maintenance of the system, access rights are differentiated by account, and all restricted features for each account are disabled on the screen.



- admin: You can use all the functions of the product.
- setup, user: You can use all the functions except for environment settings, such as System Upgrade, Change Network, Change Time, etc.
- guest: You can check the product information on the home screen.

Unlock Account

For all accounts except the admin account, if you enter the wrong password more than 5 times when logging in, the account will be locked for 30 seconds and you will not be able to log in. The admin account can reset the number of retries by checking the number of login retries for each account and whether the account is locked.

Account lock status			
Account	Retry count	Lock status	Reset lock count
setup	5		<button>Reset</button>
user	0		<button>Reset</button>
guest	0		<button>Reset</button>

1. On the Home screen, click <Environment Setting> → <System Management>.
2. Click [Reset] after checking the locked account on <Account lock status>. The lock icon is changed to unlocked and the number of retries for the account is reset.

Setting the System Check Time

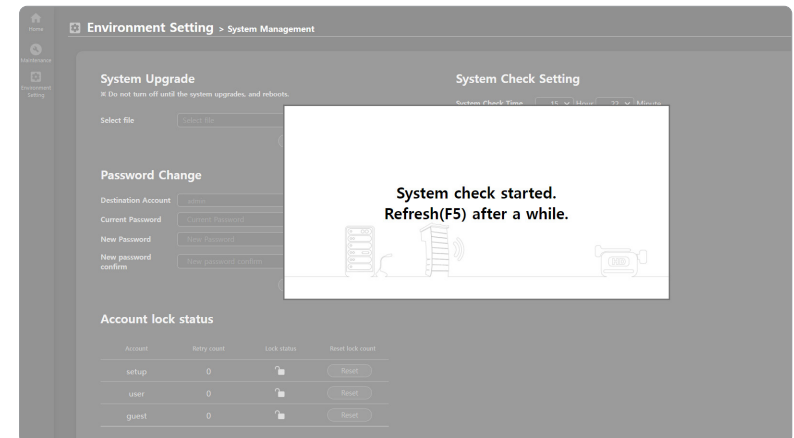
Sets the time for the system check. The system reboots automatically at the set time every day.

System Check Setting

System Check Time Hour Minute

Operation ☒ Apply Cancel

1. On the Home screen, click <Environment Setting> → <System Management>.
2. Set the time to start checking in <System Check Settings>.
3. Click [Apply] after clicking the ☒ button of <Operation>.
4. The system will be checked and be rebooted at the set time → it will take approximately 5 minutes.



Restarting System

You can restart the system without disconnecting the power when a system reboot is needed.



1. On the Home screen, click <Environment Setting> → <System Management>.
2. Click the [Apply] button in <System Restart>.
3. Click <OK> when the system restarting window appears.
It will take approximately 5 minutes to reboot the system.

Resetting the System

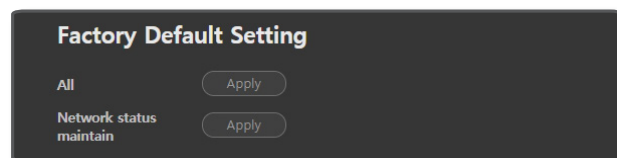
Initializes every system setting to the factory default values.

An IP address of the product is also initialized to the initial status, which is 192.168.1.100.

Please re-open the web page and access 192.168.1.100.

Even the power mode and operation mode become the PoE, which is the initial state and speaker mode.

1. On the Home screen, click <Environment Setting> → <System Management>.
2. If you click the [Apply] button of the <All> item on <Factory Default Setting>, all set values will be reset, and if you click the [Apply] button of the <Network status maintain> item, all set values except for network information will be reset.



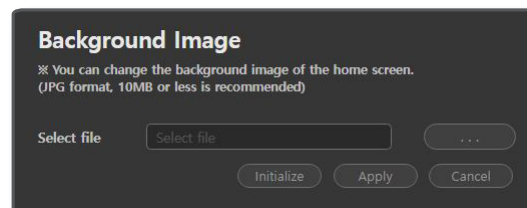
3. Click <OK> when the factory default window appears. Product initialization starts.
4. Click <OK> when the system start window appears on the web browser.

- **Do not disconnect the power** until the factory default settings are restored.
It will take up to 10 minutes to restart and complete the execution of the internal daemon program after product initialization.

- When the system initialization is completed, previously registered product information should be deleted from the controller mode speaker or audio server (SPA-S1000), and you must register if you wish to use the product.
- As the log information will be deleted when the product's system is initialized, please download it in advance.

Applying Background Images

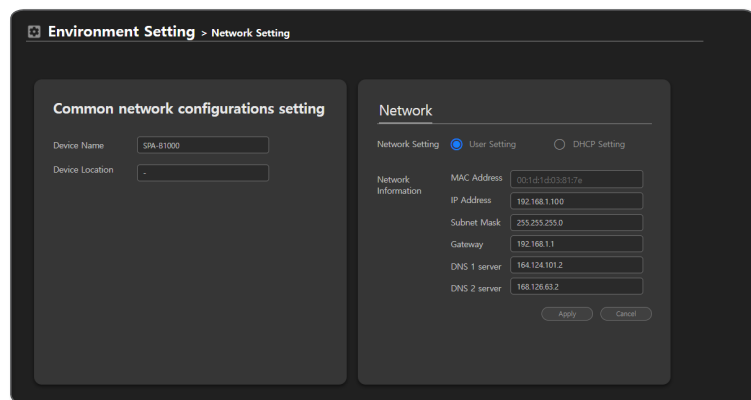
1. On the Home screen, click <Environment Setting> → <System Management>.
2. Under <Background Image>, press the [] button to select an image file, then click the [Apply] button.
3. Click the [Initialize] button to apply the initial image.



NETWORK SETTINGS

You can change the network settings according to the user's network connection configuration.

1. On the Home screen, click <Environment Setting> → <Network Setting>.



- On the <Common network configurations setting>, the <Device Name> is displayed as <Name> on the device manager's query list.
- You can enter the location of installation in <Device Location> in <Common network configurations setting> (e.g. 6th floor, Main Building)
- You can enter the IP address, subnet mask, gateway, DNS 1 and DNS 2 server addresses for the product by selecting <User Setting> in <Network Setting>.
 - MAC address: The unique physical address of the product. (e.g. Starts with 00:1d:1d.)
 - IP address: Enter the IP address available in your network band.
 - Subnet mask: The subnet mask of the set IP address is indicated.
 - Gateway: The gateway of the set IP address is indicated.
 - DNS 1 server, DNS 2 server: Enter the primary DNS address and secondary DNS address.
- The IP, subnet mask, gateway, DNS 1 and DNS 2 server addresses for the product will be allocated automatically from the DHCP server by selecting <DHCP Setting> in <Network Setting>.

■ When changing back to user settings after DHCP setting, you should enter an available IP address.

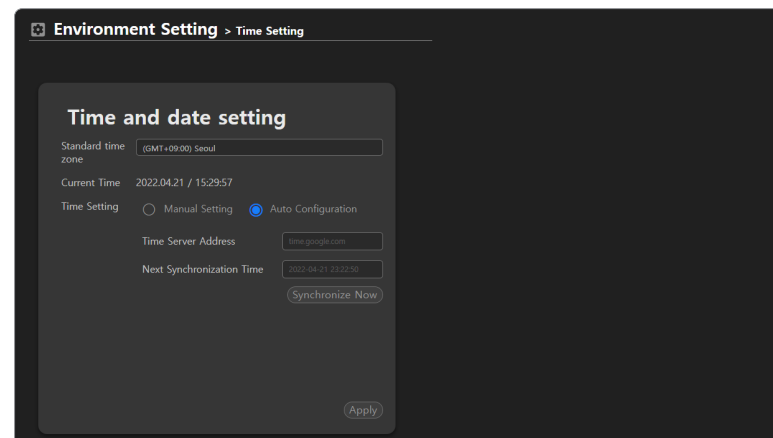
- Click [Apply] to apply the set network information to the product.
- Click [Cancel] to return to the most recent status before changing settings.

! ■ The system restarts automatically if the network settings are changed.

TIME SETTINGS

Set the time and date accurately or it may cause problems in operating the broadcast.

1. On the Home screen, click <Environment Setting> → <Time Setting>.



- The current time is set if you select GMT of your location on <Standard Time Zone>
- For the local network which is not connected to the external Internet, select <Manual Setting> in <Time Setting> and enter the time manually to use it.
- If it is connected to the external Internet, select <Auto Configuration> in <Time Setting> to synchronize the time to the standard time of the time server.
- For the domain address in the <Time Server Address> input field, use time.google.com / time.apple.com / pool.ntp.org / north-america.pool.ntp.org / time.bora.net / clock.isc.org. Please check if the domain address provides time information which reflects Daylight Saving Time.
- <Next Synchronization Time> automatically changes from the previously synced time every 8 hours.
- Click [Synchronize Now] to synchronize the time to the time server.

2. Click [Apply] to apply the set Time and Date information.

- ! ■ If the product is used in a local network environment without an external Internet connection, the time information may become incorrect due to the product's accumulated time errors. To accurately schedule the broadcasting time, we recommend installing a separate time server device using GPS signals or enter the audio server IP (SPA-S1000) with high time accuracy into the <Time Server Address> field of other products to synchronize the time information with the audio server.
- If there is a product connected to an external Internet, enter the IP address of the product in the <Time Server Address> field of other products before using them.
- IP audio products are not synchronized with the OS time of the PC.

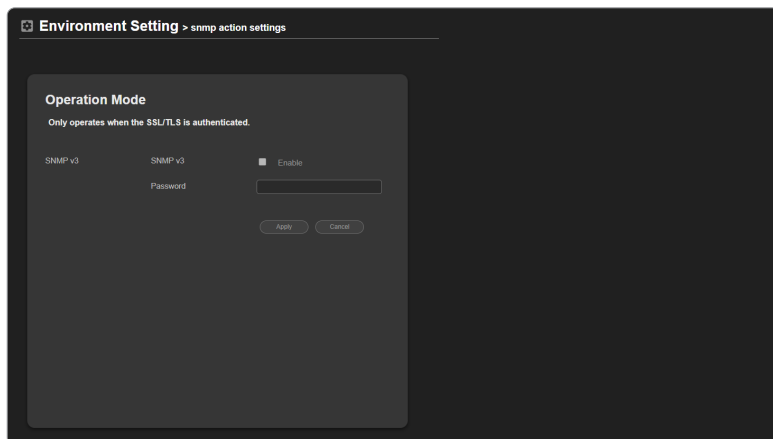


- If the product is used in a local network environment without the external Internet connection, Daylight Saving Time is not automatically reflected as it is not synchronized with an external time server.
- In countries where Daylight Saving Time is applicable, it is recommended for the system administrator to use the product by changing the time manually for the start and end dates of the Daylight Saving Time.

SNMP ACTION SETTINGS

The SNMP protocol allows system or network administrators to remotely monitor and configure the network devices.

1. On the Home screen, click <Environment Setting> → <snmp action settings>.

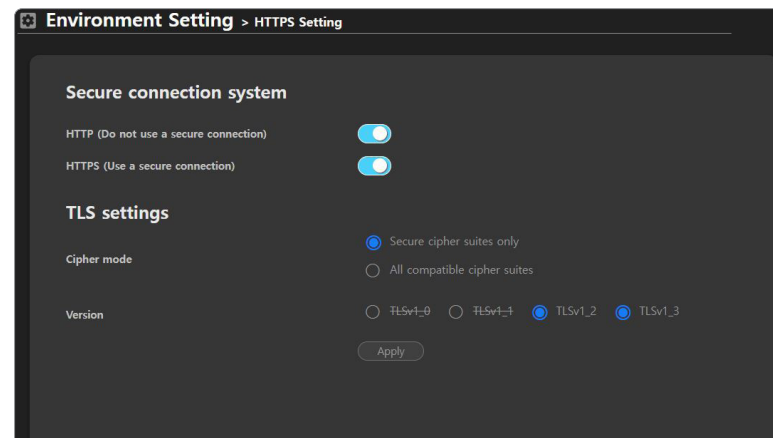


- Use SNMP v3: SNMP v3 is used.
 - Password : Set the initial user password for SNMP v3.
The initial password is insecure, so we recommend that you change it to a new password.
The password must be between 8 and 16 characters long, and some special characters (\, |, <, >, ', ", /, ?) are not allowed.
- To use SNMP v3, select <HTTPS (Use a secure connection)> from <Environment Setting> → <HTTPS Setting> → <Secure connection system>. If SNMP v3 is not used, it may result in a security issue.

HTTPS SETTING

Select a secure connection system. When you complete the configuration, click the [Apply] button.

1. On the Home screen, click <Environment Setting> → <HTTPS Setting>.



- Secure connection system : Select an appropriate secure connection system in consideration of the security level. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) sends and receives data through the process of encoding/decoding users' page requests over SSL sub layer under hypertext transport agreement layer. Therefore, this mode is safer than HTTP mode in terms of security.
 - HTTP (Do not use a secure connection) : Select this to send data without HTTP encryption.
 - HTTPS (Use a secure connection) : Select this to connect in HTTPS secure connection mode.
- TLS settings : Sets Cipher mode or TLS version to use for encrypted communication.
 - Cipher mode: Provides cipher suites by combining various algorithms to use for TLS-encrypted communications, such as key exchange, authentication, and encryption. To use only cipher suites with a high level of security, select <Secure cipher suites only>. To use cipher suites with backward compatibility although less secure, select <All compatible cipher suites>. <All compatible cipher suites> includes both secure and not secure cipher suites.
 - Version : Selects the TLS protocol version to use for encrypted communication.
If <Secure cipher suites only> is selected for <Cipher mode>, you can select only TLS 1.2 or TLS 1.3. If <All compatible cipher suites> is selected, you can select any option you want out of all TLS versions.

IP FILTERING MANAGEMENT

You can prepare an IP address list to allow or reject the connection for a specific IP.

1. On the Home screen, click <Environment Setting> → <IP Filtering management>.

	IP	Prefix	Filtering Range
Filtering List	192.168.1.90	24	192.168.1.0 ~ 192.168.1.255
		32	

- Filtering Type
 - Deny registered IP: Denies access for a registered IP.
 - Allow registered IP: Allows access for a registered IP
- Filtering List : Enter the IP and Prefix information. The filtering range for the entered information will be displayed.
 - IP address : Displays the registered IP address.
 - Prefix : Displays the prefix to be filtered.
 - Filtering range : If you enter an IP address or prefix, then the range of IP addresses blocked or permitted will be displayed.
- Click the **[Apply]** button to save the entered information in the list.

! ■ To register an access-allowed IP, you must register the IP currently connected to the device. The currently connected IP address cannot be registered as **[Deny registered IP]**.

802.1x SETTING

You can select whether or not to use the 802.1x protocol when connecting to a network.

1. On the Home screen, click <Environment Setting> → <802.1x setting>.

IEEE 802.1x

EAP type: EAP-TLS

EAPOL version: 1

ID:

Password:

CA certificate: -

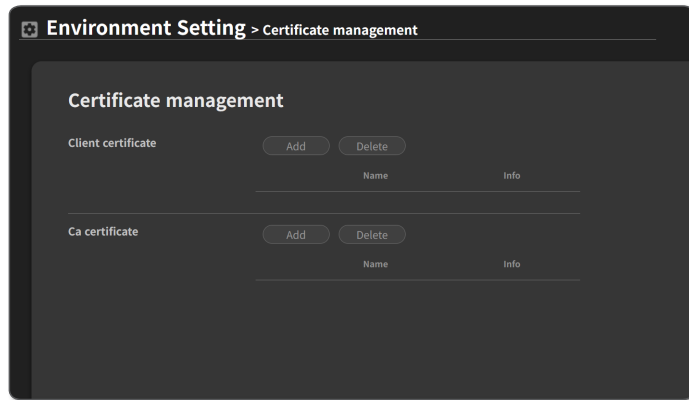
Client certificate: -

- IEEE 802.1x : To use the IEEE 802.1x protocol when connecting to a network, click the button to enable it.
- EAP Type : EAP (Extensible Authentication Protocol) is a protocol that allows easier extension using the authentication method defined by wireless network and Point-to-Point Protocol. It is recommended to be used only in an environment where EAP-TLS, PEAPv0/MSCHAPv2 cannot be used since LEAP is an insecure authentication method.
 - EAP-TLS: EAP-TLS (Transport Layer Security) carries out mutual authentication that requires a client certificate with the server→ a dynamic WEP key is used for security after connection is made.
 - LEAP: LEAP (Lightweight Extensible Authentication Protocol) does not require certificates and uses only a dynamic WEP key, so a strong password should be used.
 - PEAPv0/MSCHAPv2: PEAP/MSCHAPv2 (Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) authentication performs authentication based on the ID and password of user through an EAP-TLS session generated from the server-side authentication only.
- EAPOL version : Select the version of **[EAPOL]** (EAP over LANs) between <1> and <2>.
- ID : Enter your client certificate ID for **[EAP-TLS]** and enter your user ID for **[LEAP]** and **[PEAPv0/MSCHAPv2]**.
- Password: Enter your client private key for **[EAP-TLS]** and enter your user password for **[LEAP]** and **[PEAPv0/MSCHAPv2]**. This is not necessary if an unencrypted key is used in **[EAP-TLS]**.
- CA certificate : Select the CA certificate you want from the certificate list.
The CA certificate displayed is the one registered in <Environment Setting> → <Certificate management> → <CA certificate>.
- Client certificate : Select the client certificate you want from the certificate list. The client certificate is a certificate created/applied and used by users.
The client certificate displayed is the one registered in <Environment Setting> → <Certificate management> → <Client certificate>.

CERTIFICATE MANAGEMENT

Certificates may be added or deleted. They can be divided into either CA certificate or client certificate and managed separately.

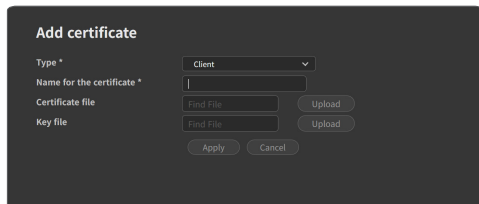
1. On the Home screen, click **<Environment Setting>** → **<Certificate management>**.



Client certificate

User certificate may be installed or deleted. If the user has a certificate file and key file, the certificate can be registered. The user can also create a certificate file by filling out the certificate details.

1. Clicking the button shows the certificate information.



Adding a client certificate

1. Click the **[Add]** button.
2. If you have a certificate file, select **<Client>** from the **<Type>** options in the **<Add certificate>** dialog, and perform the following:
 - Name for the certificate: Enter the certificate name. You can enter up to 31 characters, and special characters, Korean, Chinese, and blank spaces are not allowed.
 - Certificate file: Click **[Upload]** and select the certificate file.
 - Key file: Click **[Upload]** and select the auth key file.

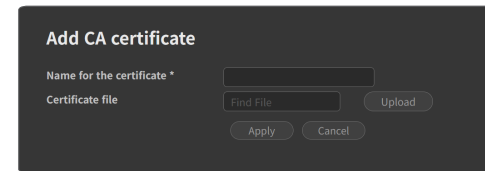
3. To create a certificate, select **<Self-signed>** among **<Type>** options in the **[Add certificate]** dialog and set each item.
4. In the **<Add certificate>** dialog, click the **<OK>** button to save the entered information in the list.

Deleting a client certificate

1. Select the client certificate to delete.
2. Click the **<Delete>** button.

CA certificate

CA certificate may be installed or deleted. CA certificate is a certificate issued by the Certificate Authority (CA). Clicking the button shows the certificate information.



Adding a CA certificate

1. Click the **[Add]** button.
2. In the **<Add CA certificate>** dialog:
 - Certificate name: Enter the certificate name.
 - Certificate file: Click **[Upload]** and select the certificate file.
3. In the **<Add CA certificate>** dialog, click the **[OK]** button to save the entered information in the list.

Deleting a CA certificate

1. Select the CA certificate to delete.
2. Click the **<Delete>** button.

HOME SCREEN CONFIGURATION

If you connect to the product using a web browser, you can check the operation settings, system management, network settings, time settings, logs, etc.



Name	Function Description
1 Home	Goes to the Home screen.
2 Operation Setting	You can set operations, such as audio settings, contact closures, broadcast audio sources, etc.
3 Maintenance	Logs generated in the product can be checked.
4 Environment Setting	The System Management, Network, Time, Device Information, HTTPS Setting, IP Filtering Management, 802.1x setting, Certificate management etc. can be set.
5 Product Model Name	Displays the device's model name.
6 Product Information	The IP address, device name, device location, and firmware version are displayed.
7 Connected Account/Login	Shows a connected account and its login status.
8 Time Information	The connection time to the web page menu, product cumulative operating time, and product time will be displayed.
9 License	The open source license notification is displayed.
10 Language	Shows language options supported on the website. (Korean, English supported)
11 Go to the Official Website	If you click <Hanwha>, the screen will move to the Hanwha Vision Official Website.

OPERATION SETTINGS

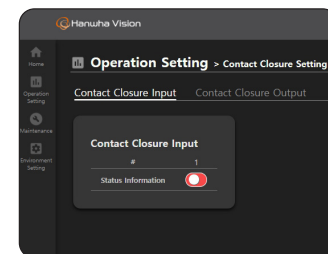
You can set the contact closures, audio and broadcast sound sources.

Contact Closure Settings

- On the Home screen, click <Operation Setting> → <Contact Closure Setting>.
- If you select the <Contact Closure Input> and <Contact Closure Output> tab, the status information will be displayed.
 - : When the input or output device is running,
 - : When the input or output device is not running,
- For Contact Closure Input, a real input signal has to occur to change the status information. Whether the Contact Closure Output is operating or not can be checked manually by clicking its status information on the screen.

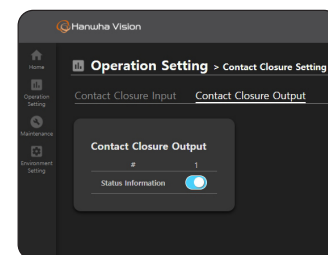
Contact Closure Input

- By connecting to the Contact Closure Output of an external device, such as an electrical switch, smoke detector, or motion detector, it can be used as the Contact Closure Input of the speaker.
 - You can perform a warning broadcast through the speaker when detecting a motion by connecting the motion detector to the contact closure signal.



Contact Closure Output

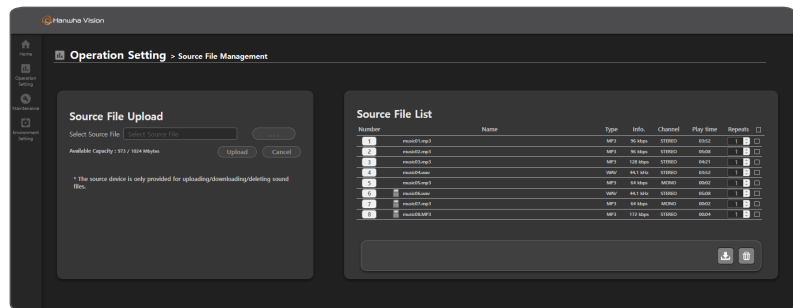
- A Contact Closure Output can send signals to the broadcast system or send a warning signal to an external device, such as a lightbar, by connecting to it.
- You can output the command for the contact closure of speakers by simply pressing the CP buttons on <Button Mode> → <Event & Preset> or the physical CP buttons on the microphone (SPA-M2000).



■ The optimal monitor resolution is 1920x1080.

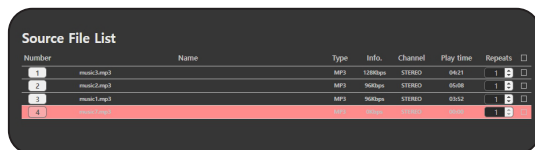
Source File Management

You can register an audio file for broadcasting.



1. On the Home screen, click <Operation Setting> → <Source File Management>.
2. Click the [] button to select the PC folder containing the sound source files to be uploaded.

- The internal storage has an available capacity of up to 1GBytes, and there are no restrictions on the size and number of sound files within the capacity.
- Supported source types: WAV (16bit), MP3
- Supported MP3 bit rates: Only MP3 (mono/stereo) in the range of 64kbps to 320kbps
- Supported WAV Sampling Rate: 44.1Khz, 48Khz
- PCM-type WAV files without header information cannot be used.
- If the sound source file name contains special characters, it may not be uploaded. Please change the file name (remove special characters) and upload again.
- Please delete audio files which cannot be played as they will be displayed as "unable to use" on the screen if they are uploaded or played.



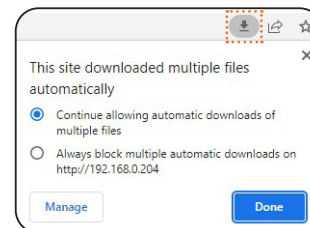
Number	Name	Type	Info	Channel	Play time	Repeats	
1	music1.mp3	MP3	128Kbps	STEREO	04:31	1	
2	music2.mp3	MP3	96Kbps	STEREO	05:08	1	
3	music1.mp3	MP3	96Kbps	STEREO	05:02	1	
4	music1.mp3	MP3	96Kbps	STEREO	05:02	1	

3. Click the [Upload] button after selecting source files to upload.
 - You can select External Storage (SD) and upload if the product has a microSD card.
 - The available capacity of the internal and external storage is displayed and an upload unavailable window appears when they are smaller than the source files to be uploaded.
 - Insert or remove the microSD card while the product is turned off.
 - Duplicate sound source file names are not allowed, so a pop-up window will appear saying that it cannot be uploaded.

- Be sure to format the microSD card in FAT32 (file system) before inserting it into the audio bridge.
- NTFS and exFAT (file systems) are not supported.
- A microSD card capacity of up to 32 GB is supported (SDHC, MLC, Class 10 or higher).
- We recommend Sandisk and Transcend products.
- Compatibility by manufacturer and product type may vary.

4. Uploaded source files are displayed on the right <Source File List>. Various information is provided, and repeated playback of audio (up to 99 times) is also possible.
 - A microSD card icon is displayed with the file name for the files saved to external storage (SD)
5. You can download the uploaded sound source or delete it.

- When you try to download two or more audio resources, the pop-up window granting permission will appear. If you have pressed the permission-block button, click the top right button on the web page (shown with the icon) to select <Allow downloading multiple files automatically>.



6. Click the number of the source file list to play through the PC speaker.

Using the audio bridge (SPA-B1000)

Method to directly control the <Audio Server> settings with SPA-B1000 for broadcasting to the specific zone speaker.

1. Connect an audio device to transmit to the SPA-B1000 input terminal (LINE IN) for playback.
2. Access the SPA-B1000 web page.
3. On the Home screen, click <Operation Setting> → <Audio Server>.
4. On the <Audio Server Settings> screen, configure the settings for transmission method, encoding method, playback data, operation information, etc.
5. Click the [Apply] button to go to <Audio Server Operation information> and then check the audio server settings.
6. On the operation screen, check whether the level meter for incoming audio signals appears.

Method to register the SPA-B1000 as a source by using the controller and broadcast to the specific zone speaker.

1. Connect an audio device to transmit to the SPA-B1000 input terminal (LINE IN) for playback.
2. Access the web page of the controller to link to.
3. On the Home screen, go to <System Setting> → <Device Registration> and then register SPA-B1000 and a single output device.
4. On the Home screen, go to <System Setting> → <Source Registration> and then register SPA-B1000 as a source. At this time, select <BGM> as the source type, enter a desired transmission method, address and port, and then click the [Apply] button.
5. On the Home screen, go to <System Setting> → <Zone Registration> and then register a single output device as a zone.
6. On the Home screen, go to <Operation Mode> → <Button Mode>, select a source and zone registered in Step 4 and 5, and then click the [Start Broadcasting] button.
7. The notes being broadcast appears on the set zone button, and the sound source connected to the SPA-B1000 audio input terminal (LINE IN) is output from the zone's device.

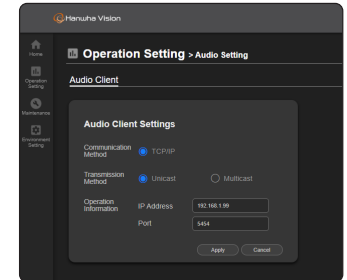
- Access the web page of the SPA-B1000 registered as a source, go to <Operation Setting> → <Audio Server>, and then check whether the device information registered as a zone appears in the client connection list at the bottom.

Audio Server

- You can send sound source to the IP speaker through <Audio Server Settings>.

1. On the Home screen, click <Operation Setting> → <Audio Server>.
2. The <Audio Server Settings> screen appears.

- Communication Method: Supports TCP/IP
- Transmission Method: Select between Unicast and Multicast
You can select both Unicast and Multicast.
 - Unicast: Up to 20 speakers can be connected to send sound source.
 - Multicast: Sound source can be sent to up to 256 speakers.
- Encoding Method: Only PCM is available.
 - PCM : High quality sound is provided with uncompressed audio data but a large amount of traffic is caused.
- Play information : The provided sampling rate and channel are 48,000 Hz and Mono only.



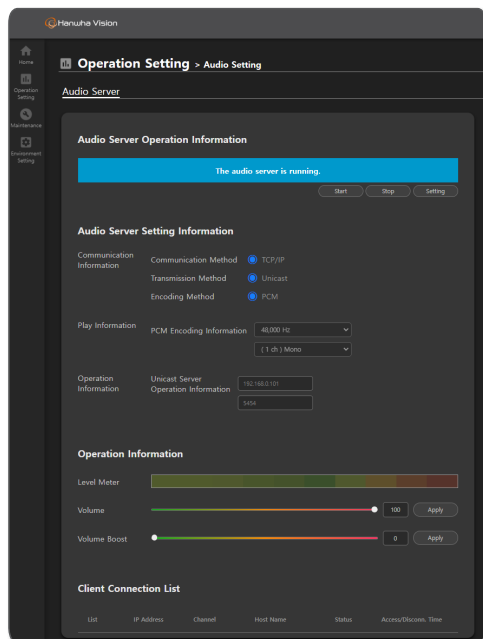
- Operation Information: Enter the server's IP address or port.
 - Use port information that does not overlap with the audio broadcasting port.
- Click the [Apply] button to save the settings and move to the Audio Server information screen.

- If you manually control the audio server of the audio bridge while running all the broadcasts through the server or controller, malfunctions may occur, so please be cautious.

Using the IP audio bridge

Audio Server Operation information

When you click the [Apply] button in <Audio Server Settings>, the audio server runs and it switches to the following screen that displays the audio server's operations and settings.



1. In <Audio Server Operation information>, you can select whether or not to operate the audio server.
 - Click the [Start], [Stop] buttons to select whether to operate the broadcast server.
 - Click the [Settings] button to move to the <Audio Server Settings> screen.
2. <Audio Server Settings information> displays the audio server's settings.
3. <Operation information> displays the level meter and volume of the transmitted audio, and you can adjust the volume by using the mouse or keyboard. You can adjust the Volume Boost (0 dB to 6 dB) to set to a volume louder than the default.

■ When you set the Volume Boost 1 or more, it may cause input audio clipping and severe sound distortion.

4. <Client Connection List> displays the devices connected to the active audio server.

■ The device list appears only when the transmission method is set to Unicast.

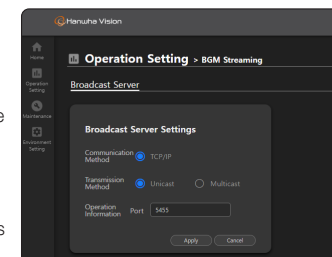
BGM Streaming

- As It uses audio uploaded to Source File Management, you cannot upload or delete audio on BGM Streaming.

1. On the Home screen, click <Operation Setting> → <BGM Streaming>.
2. The <Broadcast Server Settings> screen appears.

Broadcast Server Settings

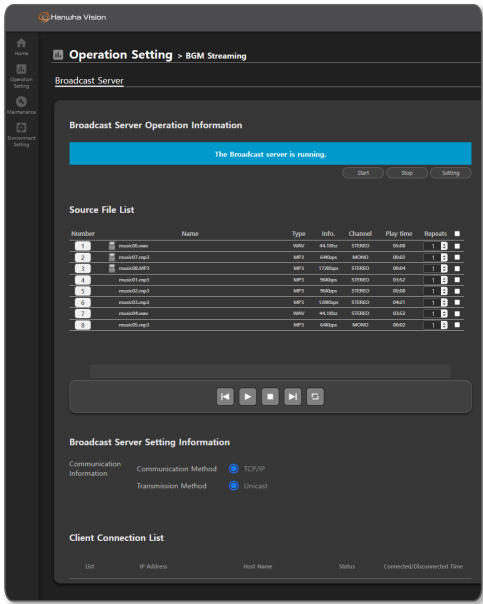
- Communication Method: Supports TCP/IP
- Transmission Method: Select between Unicast and Multicast
You can select both Unicast and Multicast.
 - Unicast can transfer the audio up to 1:20 speakers while Multicast can transfer audio up to 1:256 speakers.
 - You have to select the transmission method in consideration of the network environment being used.
- Operation Information: Sets the port where the server operates
The basic streaming port is set as 5455.
 - Be careful that the port does not overlap with that of the audio server.
- Click the [Apply] button to save the settings and move to the Broadcast Server information screen.



■ If you manually control the BGM Streaming of the audio bridge while running all the broadcasts through the server or controller, malfunctions may occur, so please be cautious.

Broadcast Server Operation Information

When you click the **[Apply]** button on **<Broadcast Server Settings>**, the server begins operation, and you will be moved to the following screen which shows the source file list, playback information & server settings, and the client connection list.



1. In **<Broadcast Server Operation Information>**, you can select whether or not to operate the audio server.
 - Click the **[Start]**, **[Stop]** buttons to select whether to operate the broadcast server.
 - Click the **[Settings]** button to move to the **<Broadcast Server Settings>** screen.
2. You can check the information of source files on the Source File List.
Click the number of the source file lists to play through the PC speaker.
3. In the source file list, you can play the source file selected in the checkbox on the right with the **[Play/Pause]** button.
4. Communication information and operation information are displayed in **<Broadcast Server Settings Information>**.
5. **<Client Connection List>** displays the devices connected to the active audio server.

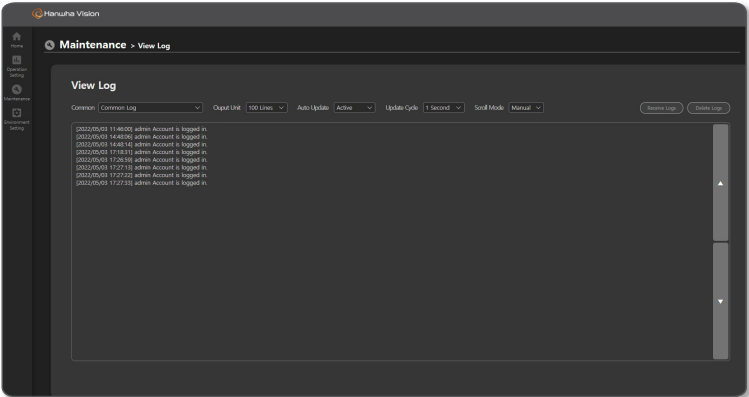
 The device list appears only when the transmission method is set to Unicast.

MAINTENANCE

View Log

You can check logs generated in the product.

The log items are different for each product, and they are recorded when the log operation occurs.



1. On the Home screen, click **<Maintenance>** → **<View Log>**.
2. The action log history for the device is shown by item.
Log Menu appears on View Log when its function is activated.
 - The logs of each menu are queried up to 1000 lines, and if they exceed 1000 lines, the oldest logs are deleted first.
3. If you click the **[Receive Logs]** button, a file can be downloaded in HTML format.
Check HTML files via Google Chrome.
 - As the log information will be deleted when the product's system is initialized, please download it in advance.
4. If you click the **[Delete Logs]** button, all logs displayed on the screen will be deleted.
5. Output Unit, Auto Update, Update Period, and Scroll Mode can be set.
If you activate **<Auto Update>**, logs will be displayed according to the **<Update Cycle>**.
 - If you auto-select **<Scroll Mode>**, the screen will be moved downward to show recent logs.
 - Press the **[Top/Bottom]** button to view the upper and lower logs.



Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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.



Hanwha Vision cares for the environment at all product manufacturing stages, and is taking measures to provide customers with more environmentally friendly products. The Eco mark represents Hanwha Vision's devotion to creating environmentally friendly products, and indicates that the product satisfies the EU RoHS Directive.



Correct Disposal of This Product (Waste Electrical & Electronic Equipment)

(Applicable in the European Union and other European countries with separate collection systems)

This marking on the product, accessories or literature indicates that the product and its electronic accessories (e.g. charger, headset, USB cable) should not be disposed of with other household waste at the end of their working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate these items from other types of waste and recycle them responsibly to promote the sustainable reuse of material resources.

Household users should contact either the retailer where they purchased this product, or their local government office, for details of where and how they can take these items for environmentally safe recycling.

Business users should contact their supplier and check the terms and conditions of the purchase contract. This product and its electronic accessories should not be mixed with other commercial wastes for disposal.



Correct disposal of batteries in this product

(Applicable in the European Union and other European countries with separate battery return systems.)

This marking on the battery, manual or packaging indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in EC Directive 2006/66. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.

To protect natural resources and to promote material reuse, please separate batteries from other types of waste and recycle them through your local, free battery return system.

