Hanwha Vision

SIP MICROPHONE

User Manual

SPA-M2000

CE

SIP Microphone

User Manual

Copyright

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

CAUTION

RISK OF ELECTRIC SHOCK.
DO NOT OPEN

CAUTION : TO REDUCE THE RISK OF ELECTRIC SHOCK.
DO NOT REMOVE COVER (OR BACK).
NO USER SERVICEABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

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.

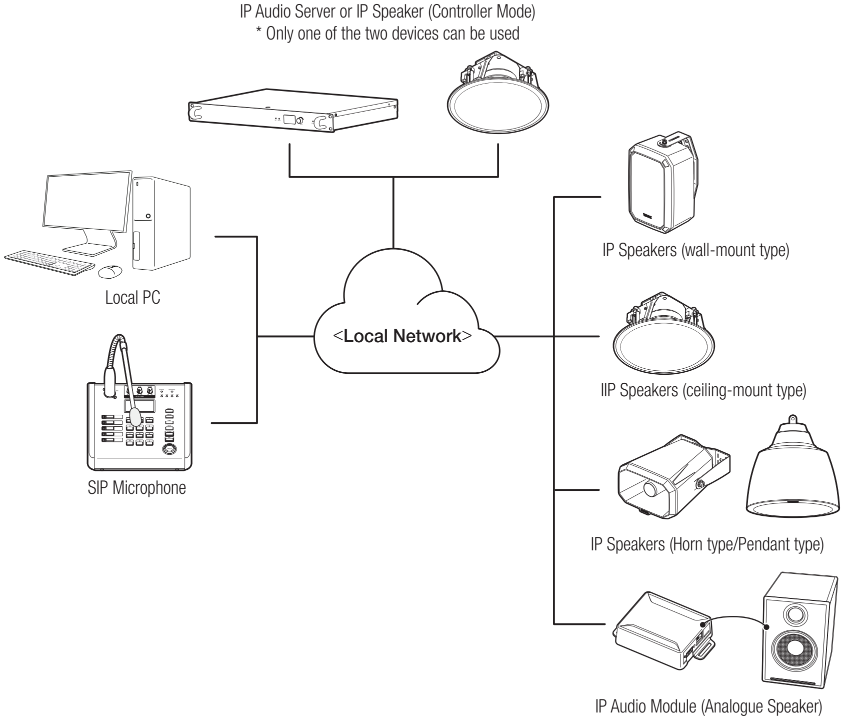
14. Unplug this apparatus during lighting storms or when unused for long periods of time.
15. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have 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) : 48V (⎓), max 250mA / DC 24V (⎓), max 500mA.
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.

FEATURES

- **Paging communication over the network**
  You can broadcast a variety of messages, such as announcements to a designated area within the network, using the paging system by connecting it to a network audio server or controller mode speaker.
- **Gooseneck microphone**
  You can use the gooseneck microphone conveniently by adjusting its position flexibly to fit a user environment.
- **Simple button operation**
  You can select the broadcasting area simply by using the buttons on the Number buttons or the ALL button, etc., and you can select the operation method of the TALK button and CHIME button based on your preferences.
- **2.42 inch OLED display**
  Through the OLED display, you can monitor the current status of the product and prevent errors when entering button inputs, such as when selecting a broadcasting area.
- **Level meter with an LED display**
  You can intuitively monitor the current volume level through the sound level meter with an LED display.
- **Monitoring speaker**
  You can monitor the current volume level using the monitoring speaker on the side of the product.
- **Input/output control volume**
  You can adjust the input volume of the microphone, the volume of the monitor speaker and chime, and the input volume of the connected external audio source.
- **DC 24V power input**
  A DC 24V power input terminal provides a stable power supply while using an adapter.
- **Power over Ethernet (PoE)**
  If you connect a PoE-enabled device to the NETWORK port of the product, power can be supplied without a separate power connection.

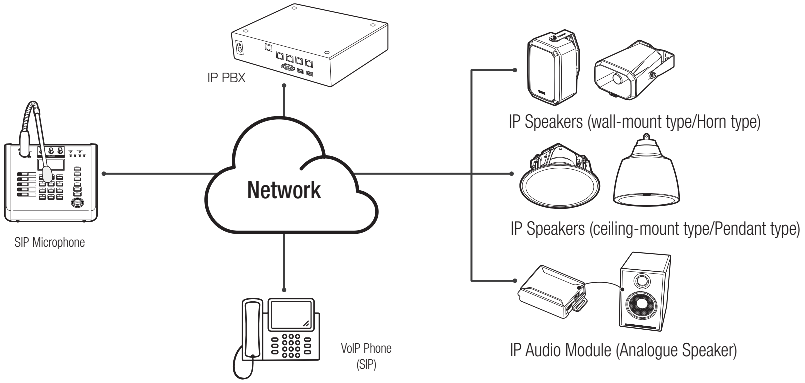
BROADCAST SYSTEM CONFIGURATION DIAGRAM

This product is a SIP microphone that is to be connected to the controller device (e.g., audio server, speaker/audio module set to controller mode) of the network audio system.
To use the microphone, you must connect it to the network and register a device via a web-based integrated control software and an RM source. You can set up your CP and VP numbers in the Events & Preset menu.
There should be only one controller mode device in the broadcast system.
If there are multiple controller mode speakers or audio servers and they are registered as the microphone more than once, proper broadcasting cannot be performed.


IP Audio Server or IP Speaker (Controller Mode)
* Only one of the two devices can be used
Local PC
<Local Network>
SIP Microphone
IP Speakers (wall-mount type)
IIP Speakers (ceiling-mount type)
IP Speakers (Horn type/Pendant type)
IP Audio Module (Analogue Speaker)

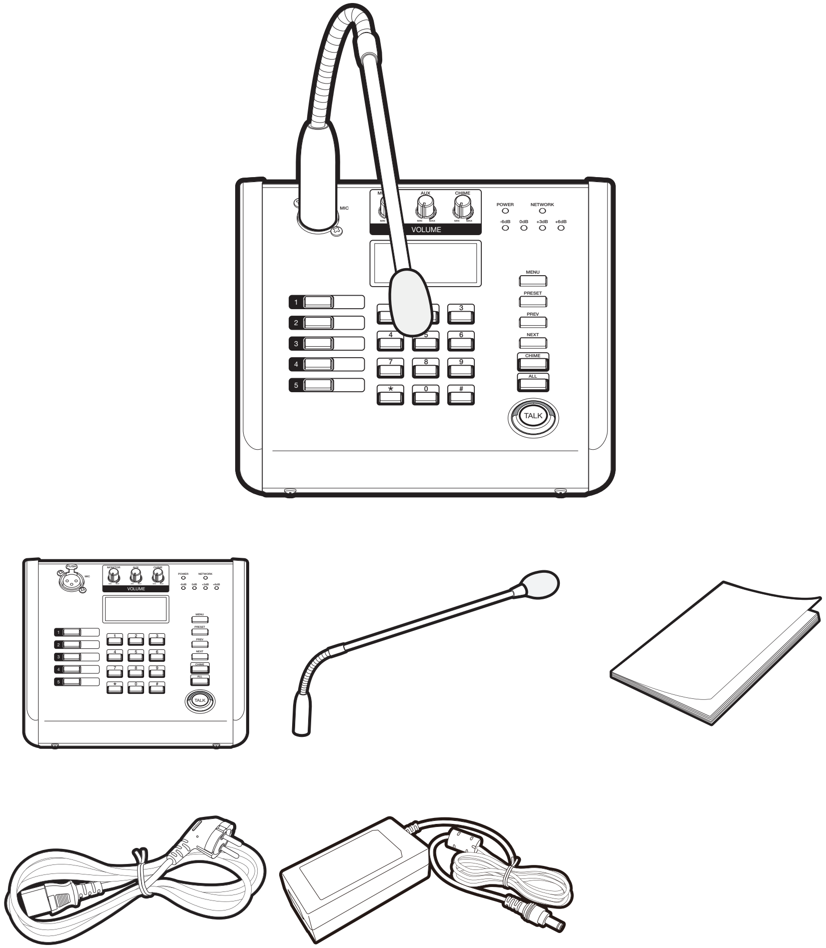
IP PBX Linkage Block Diagram

You can broadcast voice to each speaker with a VoIP phone which uses the SIP protocol by using the IP PBX server.


IP PBX
SIP Microphone
Network
VoIP Phone (SIP)
IP Speakers (wall-mount type/Horn type)
IP Speakers (ceiling-mount type/Pendant type)
IP Audio Module (Analogue Speaker)

CHECKING THE COMPONENTS

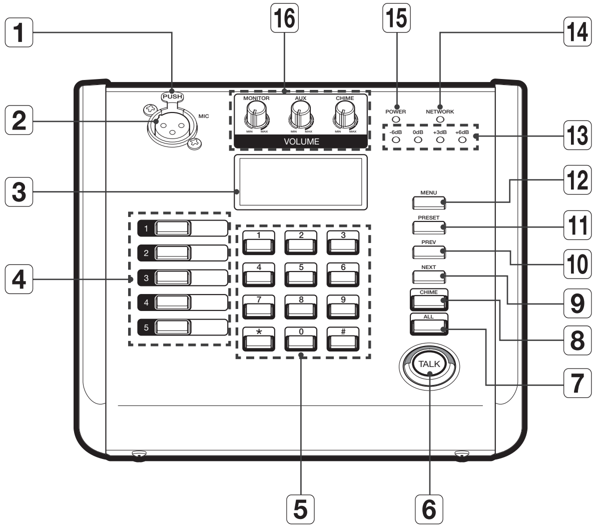
Make sure all of the following components are included.
(Accessories may vary by sales region.)



- The images used in the product manual may differ from the actual product.

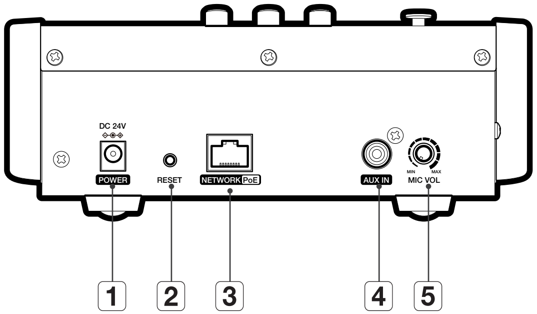
NAMES AND FUNCTIONS OF EACH PART

Front



Name	Function Description
1 Microphone release button	Releases the gooseneck microphone.
2 Microphone connection port	Connects the gooseneck microphone.
3 Status indicator	Indicates the settings and current status of the product.
4 CP event buttons	This is a CP event number (1 - 5) input button set in the <**All Event & Preset List**> of the controller device. It is also used as the SIP shortcut key.
5 Number buttons	Buttons used to select a broadcast area or mode number. This is also used as the VP event number button set in the <**All Event & Preset List**> of the controller device.
6 TALK button	The button used to start or end a broadcast with a microphone. For information on how to set the TALK button, refer to "**Talk Type Settings**". (Page 34)
7 ALL button	The button used to select all broadcast regions.
8 CHIME button	The button used to sound a chime to signal the start or end of a broadcast. For information on how to set up a chime, refer to "**Chime Settings**". (Page 33)
9 NEXT button	When entering numbers, if 8 or more numbers have already been entered, they cannot all be displayed on a single screen, so this button is used to return to the previous page.
10 PREV button	When entering numbers, if 8 or more numbers have already been entered, they cannot all be displayed on a single screen, so this button is used to return to the previous page. *Used as the Exit button for the Menu screen.
11 PRESET button	Button to switch to CP, Group, or Zone mode in the **<Talk Protocol>** menu.
12 MENU button	Use it to make settings for the TALK and CHIME buttons, or to check the product's network or firmware information. *The **[MENU]** button is also used as the Exit button for the Number input screen.
13 Level meter LED	Measures and displays the current volume level.
14 Network status LED	Indicates network connection status.
15 Power status LED	Indicates power connection.
16 Monitor speaker/AUX/Chime volume dial	Controls the volume of the monitor speaker, the input volume of the connected external audio source, and the chime volume.

Rear



Name	Function Description
1 POWER input terminal	Supplies DC 24V power by connecting to the supplied power adapter.
2 RESET switch	A button that returns the product settings to the factory default values. Press the button for approximately 12 seconds to reset and reboot the product. ! 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.
3 NETWORK terminal	Connects network cable. The microphone can be used when broadcasting through the integrated control software of the controller device within the same network. When connected to a PoE device (switching hub), power can be supplied without a separate power connection.
4 AUX IN port	Receives sound by connecting to an external audio source via an RCA cable.
5 MIC VOL dial	A dial that adjusts the microphone input volume level

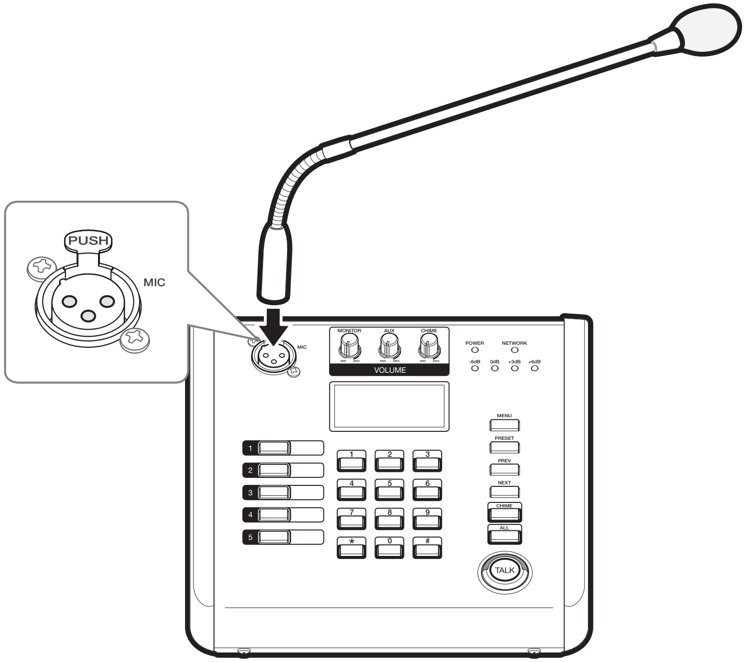
INSTALLATION

Precautions Before Installation

- Be careful that cables do not become stuck in the wrong places and that the covering of electric wires is not damaged, as this can cause product damage or fire.
- If the product is forcibly assembled by applying excessive force, the product may be damaged.
- Adjust the microphone volume to the minimum before plugging it into the power source.

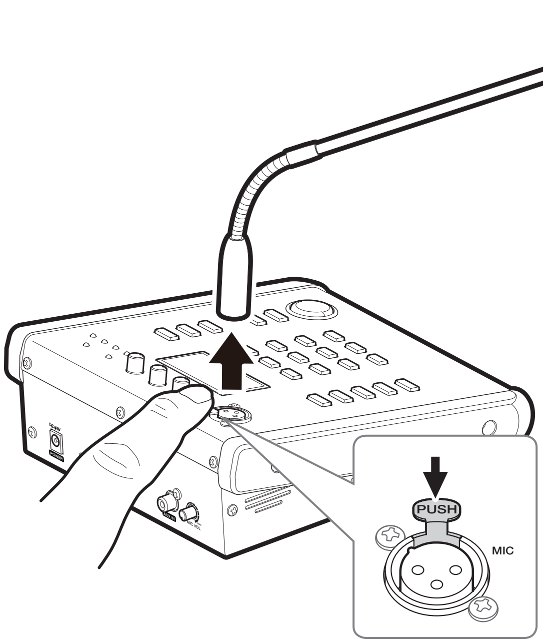
Connecting to the Gooseneck Microphone

Align the 3 pins on the bottom of the gooseneck microphone with the hole of the connection port, then push it in until you hear a click sound.

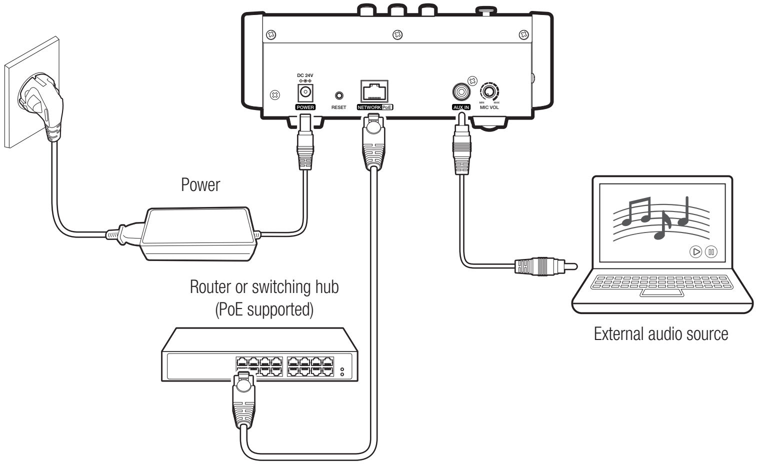


Disconnecting from the Gooseneck Microphone

Disconnect the gooseneck microphone from the device while pressing the **<PUSH>**button on top of the gooseneck microphone.



CONNECTING TO OTHER DEVICES



- 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 12)

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.

Network Cable Specifications

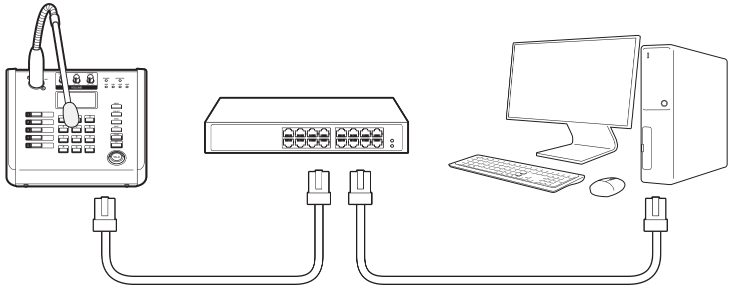
Item	Specifications	Remark
Connector	RJ45 (10/100BASE-T)	
Ethernet	10/100Base-T	
Cable	Category 5e	
Max Distance	100 m	DC resistance ≤ 0.125 Ω/m
PoE Support	IEEE 802.3af	

You can set the product's network environment according to the user's network connection configuration.
To change your product's network configuration settings, follow these instructions to access the product.

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.

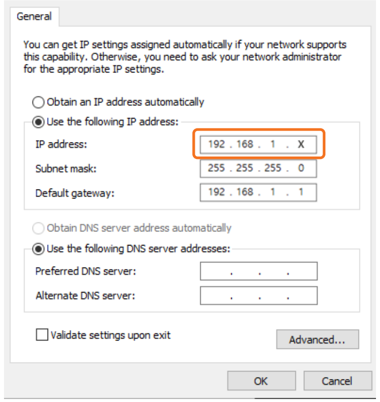


- Connect the supplied DC power cable to receive power, or connect a switching hub that supports PoE or PoE+

ACCESS PRODUCT

Various functions, including maintenance and environment 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.



General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . X

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2. Run a web browser on the PC.

- An available web browser is Google Chrome (Version 99.0.4844.82 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.

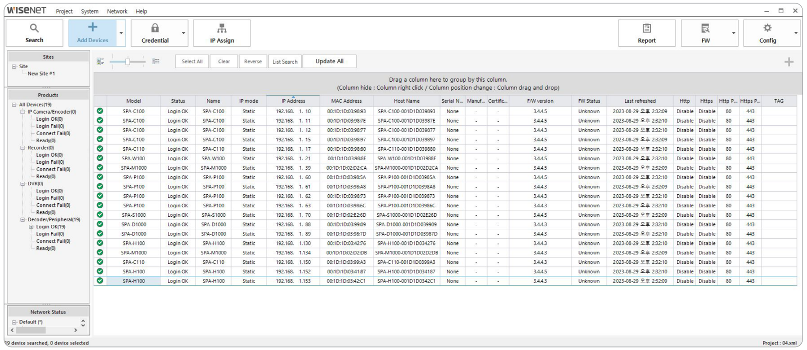
- If multiple products are connected concurrently to the same switch hub with the initial IP addresses, the web page cannot distinguish the IP addresses, resulting in failing to set passwords.
- Use Device Manager to set the initial password and IP address to use.

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**>.



Site
New Site #1

All Devices(19)
IP Camera/Encoder(0)
Login OK(0)
Login Fail(0)
Connect Fail(0)
Ready(0)
Recorder(0)
Login OK(0)
Login Fail(0)
Connect Fail(0)
Ready(0)
DVR(0)
Login OK(0)
Login Fail(0)
Connect Fail(0)
Ready(0)
Decoder/Peripheral(19)
Login OK(19)
Login Fail(0)
Connect Fail(0)
Ready(0)

Default (*)

Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drop)

	Model	Status	Name	IP mode	IP Address	MAC Address	Host Name	Serial N...	Manuf...	Certific...	F/W version	FW Status	Last refreshed	Http	Https	Http P...	Https P...	TAG
✓	SPA-C100	Login OK	SPA-C100	Static	192.168. 1. 10	00:1D:1D:03:98:93	SPA-C100-001D1D039893	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-C100	Login OK	SPA-C100	Static	192.168. 1. 11	00:1D:1D:03:98:7E	SPA-C100-001D1D03987E	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-C100	Login OK	SPA-C100	Static	192.168. 1. 12	00:1D:1D:03:98:77	SPA-C100-001D1D039877	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-C100	Login OK	SPA-C100	Static	192.168. 1. 15	00:1D:1D:03:98:97	SPA-C100-001D1D039897	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-C110	Login OK	SPA-C110	Static	192.168. 1. 17	00:1D:1D:03:98:80	SPA-C110-001D1D039880	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-W100	Login OK	SPA-W100	Static	192.168. 1. 21	00:1D:1D:03:98:8F	SPA-W100-001D1D03988F	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-M1000	Login OK	SPA-M1000	Static	192.168. 1. 39	00:1D:1D:02:D2:CA	SPA-M1000-001D1D02D2CA	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-P100	Login OK	SPA-P100	Static	192.168. 1. 60	00:1D:1D:03:98:5A	SPA-P100-001D1D03985A	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-P100	Login OK	SPA-P100	Static	192.168. 1. 61	00:1D:1D:03:98:A8	SPA-P100-001D1D0398A8	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-P100	Login OK	SPA-P100	Static	192.168. 1. 62	00:1D:1D:03:98:73	SPA-P100-001D1D039873	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-P100	Login OK	SPA-P100	Static	192.168. 1. 63	00:1D:1D:03:98:6C	SPA-P100-001D1D03986C	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-S1000	Login OK	SPA-S1000	Static	192.168. 1. 70	00:1D:1D:02:E2:6D	SPA-S1000-001D1D02E26D	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-D1000	Login OK	SPA-D1000	Static	192.168. 1. 88	00:1D:1D:03:99:09	SPA-D1000-001D1D039909	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-D1000	Login OK	SPA-D1000	Static	192.168. 1. 89	00:1D:1D:03:98:7D	SPA-D1000-001D1D03987D	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-H100	Login OK	SPA-H100	Static	192.168. 1.130	00:1D:1D:03:42:76	SPA-H100-001D1D034276	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-M1000	Login OK	SPA-M1000	Static	192.168. 1.134	00:1D:1D:02:D2:DB	SPA-M1000-001D1D02D2DB	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	
✓	SPA-C110	Login OK	SPA-C110	Static	192.168. 1.150	00:1D:1D:03:99:A3	SPA-C110-001D1D0399A3	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-H100	Login OK	SPA-H100	Static	192.168. 1.152	00:1D:1D:03:41:87	SPA-H100-001D1D034187	None	-	-	3.4.4.5	Unknown	2023-08-29 오후 2:32:10	Disable	Disable	80	443	
✓	SPA-H100	Login OK	SPA-H100	Static	192.168. 1.153	00:1D:1D:03:42:C1	SPA-H100-001D1D0342C1	None	-	-	3.4.4.3	Unknown	2023-08-29 오후 2:32:09	Disable	Disable	80	443	

19 device searched, 0 device selected

Project : 04.xml

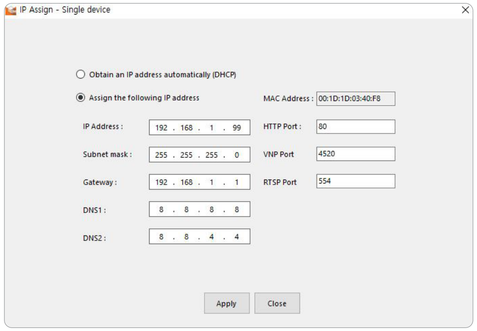
1. When you connect the product to the switch hub, its IP address is 192.168.1.100, and its status information is queried as <**Need PW**>.
2. Select one or multiple products and set a password to use for each product.
   - If they are not queried as <**Need PW**>, click <**New Project**> ➞ <**Search**>, and set the passwords after they are queried as <**Need PW**>.
   - If you set a password in the [**Credential**] menu and press [**Search**] on the list screen, the status information is queried as <**Connect Fail**>.
   - If you press <**New Project**> ➞ <**Search**>, the status information is queried as <**Ready**>. And if you press <**Search**> again, it is queried as <**Connect Fail**>.
3. When the password is set, the <**MAC Address**> of each product is queried.
   - The <**Host Name**> and <**Serial Number**> are queried when you log in using the [Credential] menu after an IP address is assigned to each product.

- 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.
- If the initial password setting in the [**Credential**] menu fails due to a <**Timeout**>, set the initial password again after assigning the IP addresses of other products with <**Success**> in password setting.

4. 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).

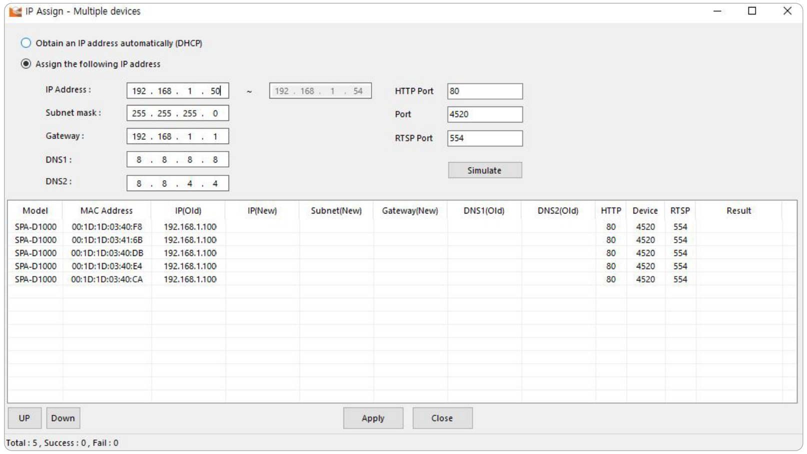


○ Obtain an IP address automatically (DHCP)
● Assign the following IP address

MAC Address : 00:1D:1D:03:40:F8
IP Address : 192 . 168 . 1 . 99
Subnet mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
DNS1 : 8 . 8 . 8 . 8
DNS2 : 8 . 8 . 4 . 4
HTTP Port : 80
VNP Port : 4520
RTSP Port : 554

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.



○ Obtain an IP address automatically (DHCP)
● Assign the following IP address

IP Address : 192 . 168 . 1 . 50 ~ 192 . 168 . 1 . 54
Subnet mask : 255 . 255 . 255 . 0
Gateway : 192 . 168 . 1 . 1
DNS1 : 8 . 8 . 8 . 8
DNS2 : 8 . 8 . 4 . 4
HTTP Port 80
Port 4520
RTSP Port 554

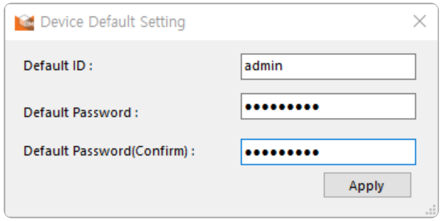
Model	MAC Address	IP(Old)	IP(New)	Subnet(New)	Gateway(New)	DNS1(Old)	DNS2(Old)	HTTP	Device	RTSP	Result
SPA-D1000	00:1D:1D:03:40:F8	192.168.1.100						80	4520	554	
SPA-D1000	00:1D:1D:03:41:6B	192.168.1.100						80	4520	554	
SPA-D1000	00:1D:1D:03:40:DB	192.168.1.100						80	4520	554	
SPA-D1000	00:1D:1D:03:40:E4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

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 network audio product.

5. 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

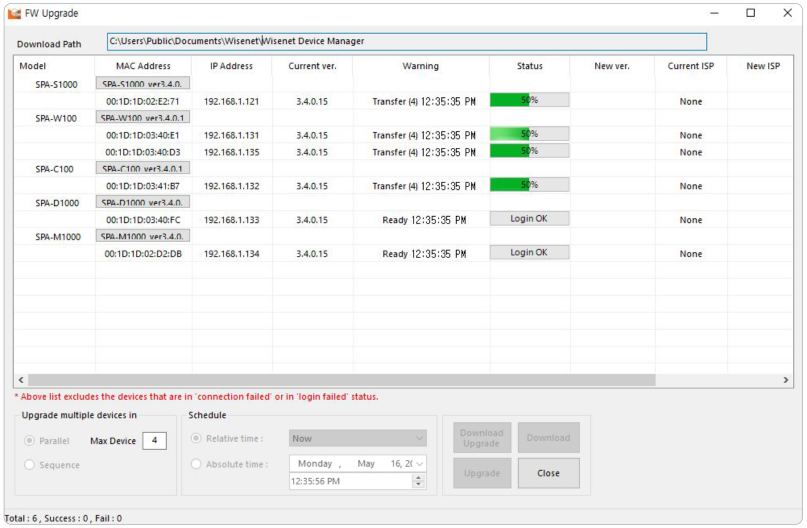
Default ID : admin

Default Password : ●●●●●●●●●

Default Password(Confirm) : ●●●●●●●●●

- 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.

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



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
SPA-S1000	SPA-S1000_ver3.4.0.							
	00:1D:1D:02:E2:71	192.168.1.121	3.4.0.15	Transfer (4) 12:35:35 PM	50%		None	
SPA-W100	SPA-W100_ver3.4.0.1							
	00:1D:1D:03:40:E1	192.168.1.131	3.4.0.15	Transfer (4) 12:35:35 PM	50%		None	
	00:1D:1D:03:40:D3	192.168.1.135	3.4.0.15	Transfer (4) 12:35:35 PM	50%		None	
SPA-C100	SPA-C100_ver3.4.0.1							
	00:1D:1D:03:41:B7	192.168.1.132	3.4.0.15	Transfer (4) 12:35:35 PM	50%		None	
SPA-D1000	SPA-D1000_ver3.4.0.							
	00:1D:1D:03:40:FC	192.168.1.133	3.4.0.15	Ready 12:35:35 PM	Login OK		None	
SPA-M1000	SPA-M1000_ver3.4.0.							
	00:1D:1D:02:D2:DB	192.168.1.134	3.4.0.15	Ready 12:35:35 PM	Login OK		None	

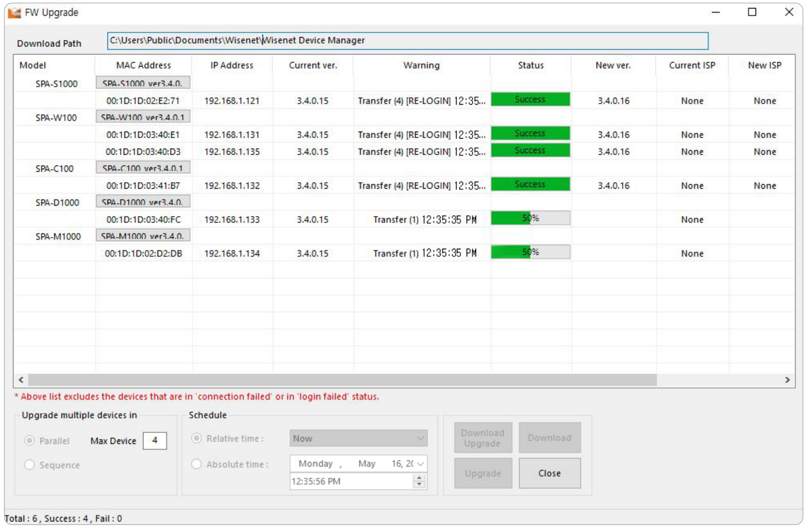
* Above list excludes the devices that are in 'connection failed' or in 'login failed' status.

Upgrade multiple devices in: ○ Parallel, Max Device 4, ○ Sequence

Schedule: ● Relative time : Now; ○ Absolute time : Monday , May 16, 2(12:35:56 PM

Total : 6 , Success : 0 , Fail : 0

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



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
SPA-S1000	SPA-S1000_ver3.4.0.							
	00:1D:1D:02:E2:71	192.168.1.121	3.4.0.15	Transfer (4) [RE-LOGIN] 12:35...	Success	3.4.0.16	None	None
SPA-W100	SPA-W100_ver3.4.0.1							
	00:1D:1D:03:40:E1	192.168.1.131	3.4.0.15	Transfer (4) [RE-LOGIN] 12:35...	Success	3.4.0.16	None	None
	00:1D:1D:03:40:D3	192.168.1.135	3.4.0.15	Transfer (4) [RE-LOGIN] 12:35...	Success	3.4.0.16	None	None
SPA-C100	SPA-C100_ver3.4.0.1							
	00:1D:1D:03:41:B7	192.168.1.132	3.4.0.15	Transfer (4) [RE-LOGIN] 12:35...	Success	3.4.0.16	None	None
SPA-D1000	SPA-D1000_ver3.4.0.							
	00:1D:1D:03:40:FC	192.168.1.133	3.4.0.15	Transfer (1) 12:35:35 PM	50%		None	
SPA-M1000	SPA-M1000_ver3.4.0.							
	00:1D:1D:02:D2:DB	192.168.1.134	3.4.0.15	Transfer (1) 12:35:35 PM	50%		None	

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

Upgrade multiple devices in: ○ Parallel, Max Device 4, ○ Sequence

Schedule: ● Relative time : Now; ○ Absolute time : Monday , May 16, 2(12:35:56 PM

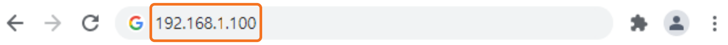
Total : 6 , Success : 4 , Fail : 0

- 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

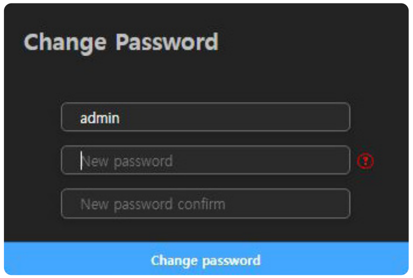
If you connect only one product to the switch hub, it is possible to set up the password even on the web page.

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



192.168.1.100

2. 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.

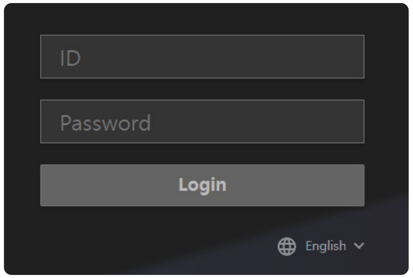


Change Password

admin

- 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.

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



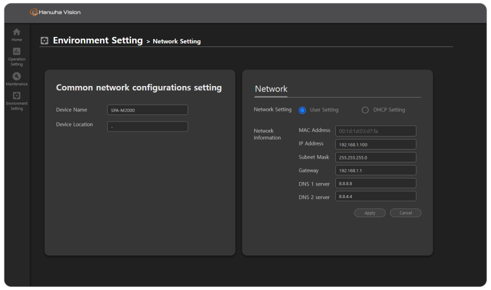
LOGGING IN

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 25)



Environment Setting > Network Setting

Common network configurations setting

Device Name: SPA-M2000

Device Location: -

Network

Network Setting: ● User Setting ○ DHCP Setting

Network Information

MAC Address: 00:1d:1d:03:d7:fa

IP Address: 192.168.1.100

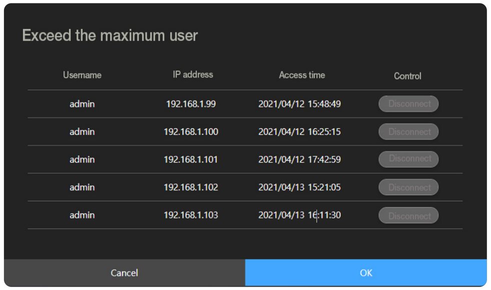
Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

DNS 1 server: 8.8.8.8

DNS 2 server: 8.8.4.4

- 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 23)
- 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.



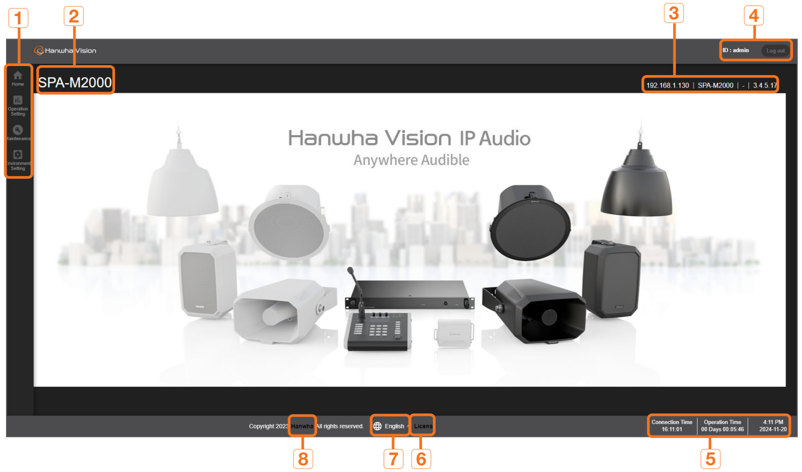
Exceed the maximum user

Username	IP address	Access time	Control
admin	192.168.1.99	2021/04/12 15:48:49	Disconnect
admin	192.168.1.100	2021/04/12 16:25:15	Disconnect
admin	192.168.1.101	2021/04/12 17:42:59	Disconnect
admin	192.168.1.102	2021/04/13 15:21:05	Disconnect
admin	192.168.1.103	2021/04/13 16:11:30	Disconnect

HOME SCREEN CONFIGURATION

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

Getting to Know the Home Screen



Name		Function Description
1	Home	Goes to the Home screen.
	Operation Setting	You can configure the SIP operation settings.
	Maintenance	Logs generated in the product can be checked.
	Environment Setting	You can set up the System Management, network, HTTPS Setting, IP Filtering Management, 802.1x setting, Certificate management and time information.
2	Product Model Name	Displays the device's model name.
3	Product Information	The IP address, device name, device location, and firmware version are displayed.
4	Connected Account/Login	Shows a connected account and its login status.
5	Time Information	The connection time to the web page menu, product cumulative operating time, and product time will be displayed.
6	License	The open source license notification is displayed.
7	Language	Shows the language options supported on the website. (Korean, English supported)
8	Go to the Official Website	If you click <**Hanwha**>, the screen will move to the Hanwha Vision Official Website. Before using the product, please check the latest firmware version on the Hanwha Vision website (https://www.HanwhaVision.com). Download and update it if it is necessary.

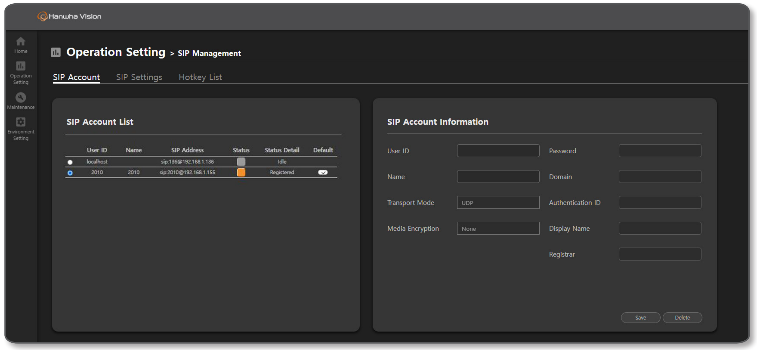
- The optimal monitor resolution is 1920x1080.

OPERATION SETTINGS

SIP Management

When it is connected to the VoIP phone which uses the standard SIP protocol and IP PBX server, the voice on the VoIP phone can be played on the speaker.
If you turn on the microphone by setting the <**DSP Setting**> ➞ <**Input Volume Setting**> of the speaker to <**CONDENSER MIC**>, 2-way Talk (Half Duplex) is supported between the VoIP phone and the speaker.
The SIP function has been verified in an IP PBX server (Asterisk) and VoIP phone (Grandstream, Yealink, Cisco) environment.
The SIP function has been verified in an IP PBX server (Grandstream) and VoIP phone (Grandstream) environment.

SIP Account



SIP Account List

	User ID	Name	SIP Address	Status	Status Detail	Default
●	localhost		sip:136@192.168.1.136	🟫	Idle	
○	2010	2010	sip:2010@192.168.1.155	🟧	Registered	✓

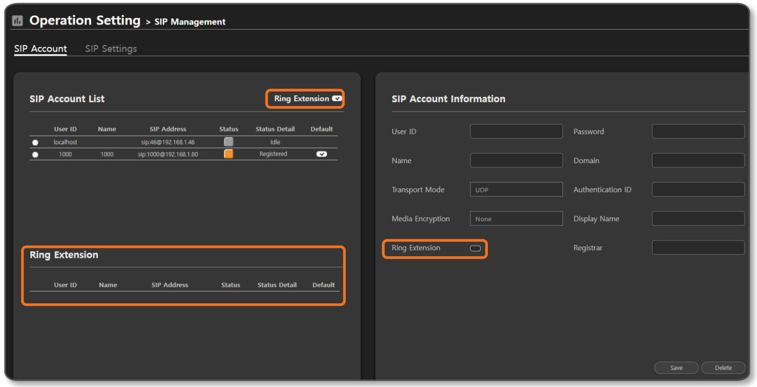
SIP Account Information

User ID		Password	
Name		Domain	
Transport Mode	UDP	Authentication ID	
Media Encryption	None	Display Name	
		Registrar	

1. Register the account and IP PBX information in <**SIP Account Information**>.
   - User ID: ID of SIP users (account in the IP PBX).
   - Name: Names that users enter for easy identification.
   - Transport Mode: UDP mode is provided using the VoIP packet transmission method.
   - Media Encryption: No encryption is used.
   - Password: Enter the password provided by IP PBX.
   - Domain: Enter the address of IP PBX.
   - Authentication ID: Enter the authentication ID provided by IP PBX. (It may not be used depending on the type of the IP PBX.)
   - Display name : It is the name which can be displayed on the receiver side. (It may not be used depending on the type of the IP PBX.)
   - Registrar: Enter the Registrar Server address. If the account is properly registered with Registrar, authentication is attempted regularly.
2. When you [save] <**SIP Account Information**>, the registered <**User ID**> information is displayed on the <**SIP Account List**>. On the <**SIP Account list**>, you can select and modify the account.
3. Set whether to use the account as the default account or not.
   When you check the account's [**Default**] on the <**SIP Account List**>, it will be sent from/received to that account.
   The account's [**Status**] is activated and [detailed information of the status] is also changed from Idle to Registered, and it is displayed as Online Devices in the IP PBX web page's Extensions menu.
   When you disable [**Default**], it is changed to Unregistered, and it is also displayed as Offline Devices in IP PBX.

4. If you dial <**User ID**> on your VoIP phone and speak, it will be received by and played on the speaker. The <**Status Detail**> of the <**User ID**> account will display as “Running, Conversation,” and if you hang up the phone, it will change to “Disconnected.” If you refresh the web screen, the status will be converted to “Registered” and maintained.
5. <**Local host**> is provided as a default, and it can be used in both <**speaker mode**> and <**Controller mode**> speakers.
   For <**Local host**>, playing audio is possible when the account linked with the IP PBX server is additionally registered or when there is only the VoIP phone without being linked to the IP PBX server. For example, if it is sent from the VoIP phone on the same network to <**sip:99@192.168.1.99**>, it is connected to the SIP of the local host.

SIP Ring Extension Settings



SIP Account List Ring Extension ☑

	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46	⬜	Idle	
○	1000	1000	sip:1000@192.168.1.80	🟧	Registered	☑

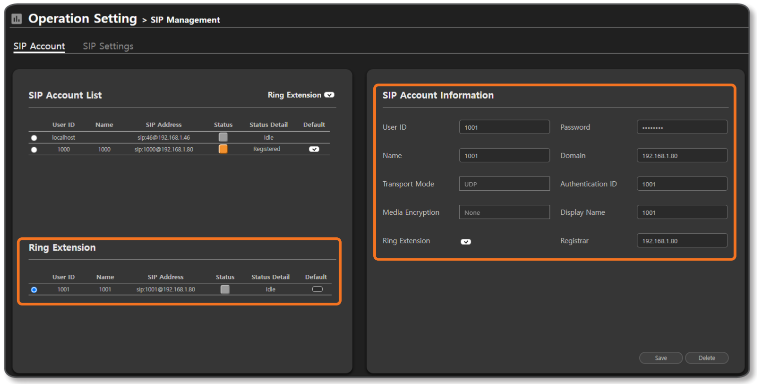
Ring Extension

	User ID	Name	SIP Address	Status	Status Detail	Default

SIP Account Information

User ID Password
Name Domain
Transport Mode UDP Authentication ID
Media Encryption None Display Name
Ring Extension ☐ Registrar

1. Selecting **<Ring Extension>** in the SIP account list will display the Ring Extension list and the **<Ring Extension>** item on the account registration screen on the right.



SIP Account List Ring Extension ☑

	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46	⬜	Idle	
○	1000	1000	sip:1000@192.168.1.80	🟧	Registered	☑

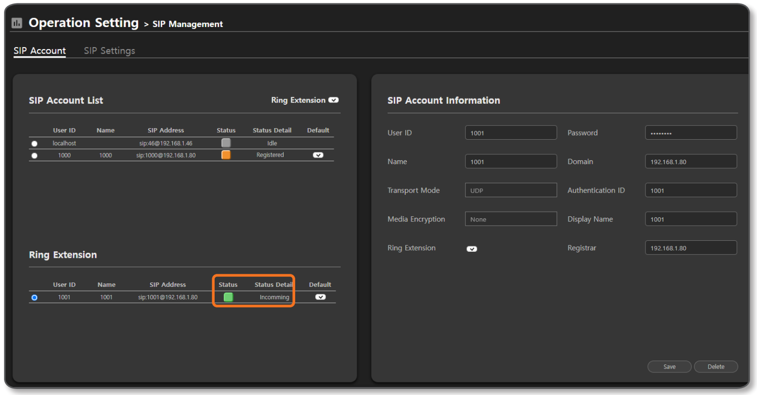
Ring Extension

	User ID	Name	SIP Address	Status	Status Detail	Default
●	1001	1001	sip:1001@192.168.1.80	⬜	Idle	☐

SIP Account Information

User ID 1001 Password ········
Name 1001 Domain 192.168.1.80
Transport Mode UDP Authentication ID 1001
Media Encryption None Display Name 1001
Ring Extension ☑ Registrar 192.168.1.80

2. Create an account to use as Ring Extension, then check the box for **<Ring Extension>**.
   In the Ring Extension list, check the box for **<Default>** and make sure that the status details are **<Registered>**.
   - To check other IP Phones ring simultaneously, you should use the same Ring Extension number with the number registered to other IP Phones.



SIP Account List Ring Extension ☑

	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46	⬜	Idle	
○	1000	1000	sip:1000@192.168.1.80	🟧	Registered	☑

Ring Extension

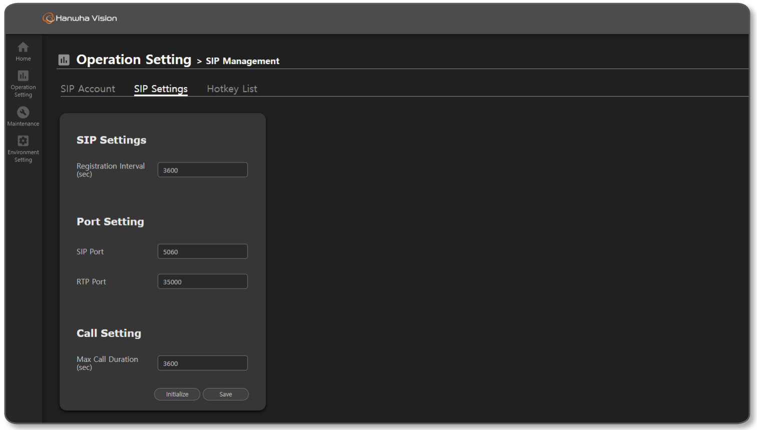
	User ID	Name	SIP Address	Status	Status Detail	Default
●	1001	1001	sip:1001@192.168.1.80	🟩	Incomming	☑

SIP Account Information

User ID 1001 Password ········
Name 1001 Domain 192.168.1.80
Transport Mode UDP Authentication ID 1001
Media Encryption None Display Name 1001
Ring Extension ☑ Registrar 192.168.1.80

3. When you call the number set as Ring Extension, other IP Phones registered with the same number as the IP Speaker will also ring simultaneously.
   - When you receive a call from an IP Phone, etc., the IP Speaker call will be disconnected automatically.

SIP Settings



SIP Settings

Registration Interval (sec): 3600

Port Setting

SIP Port: 5060

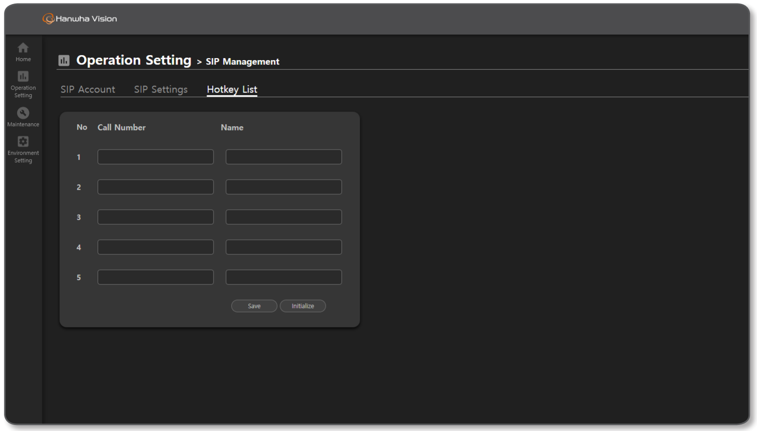
RTP Port: 35000

Call Setting

Max Call Duration (sec): 3600

1. Enter <**SIP Settings**> items.
   - Registration Interval: Enter the SIP registration period. (Default: 3600)
2. Enter <**Port Setting**> items.
   - SIP Port: Set up the port to operate SIP communication. (Default: 5060)
   - RTP Port: Set the RTP port. (Default: 35000)
3. Enter <**Call Setting**> items.
   - Max Call Duration: Set the waiting time when a call ends abnormally.
4. <**SIP Settings**> information can be initialized/saved.

SIP shortcut key settings



No	Call Number	Name
1		
2		
3		
4		
5		

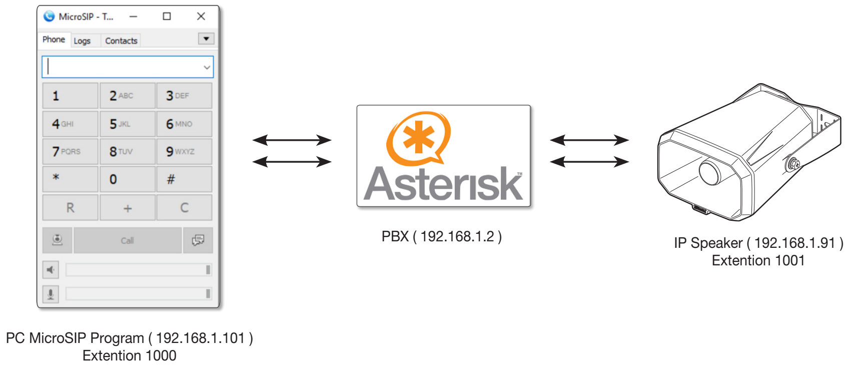
1. Enter the SIP address for each shortcut key.
   - ex) sip:2011@192.168.1.155
2. Enter the shortcut key name or short description.
3. If necessary, initialize or save the <**Hotkey List**>.

- The information may differ depending on the IP-PBX if linked to.
- In case of SIP Local Call (using the IP’s last digits), they must have been configured with LAN (dedicated network).
- The 1:N mapping is not supported for SIP Local Call (using the IP’s last digits) between the network microphones.

SIP TCP Function Settings and Testing

System Configuration Diagram

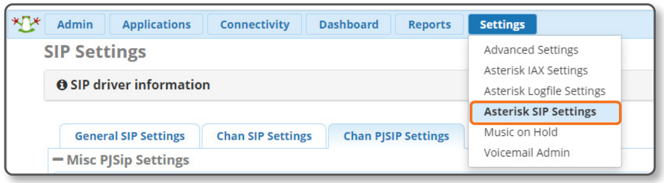
Extensions for PCs and test equipment should be registered in PBX.



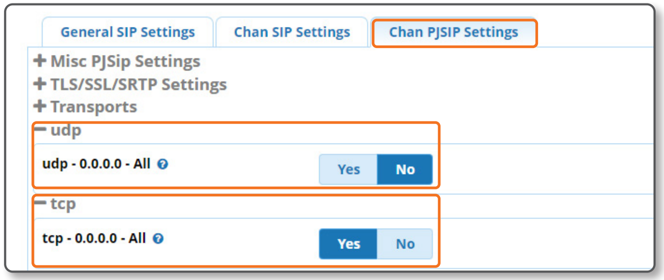
1. IP Speaker SIP TCP Function Settings and Asterisk PBX Settings

Asterisk PBX TCP Settings

- Click <**Settings**> ➞ <**Asterisk SIP Settings**>.

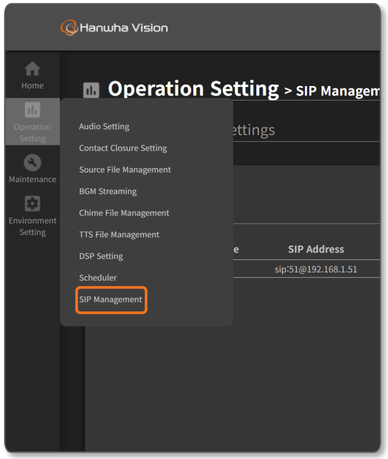


- After selecting <**Chan PJSIP Settings**> in the tab menu, set <**udp**> to <**No**> and <**tcp**> to <**Yes**>.
- To apply the changed settings, click the [**Submit**] button at the bottom right, then click the [**Apply Config**] button at the top right.

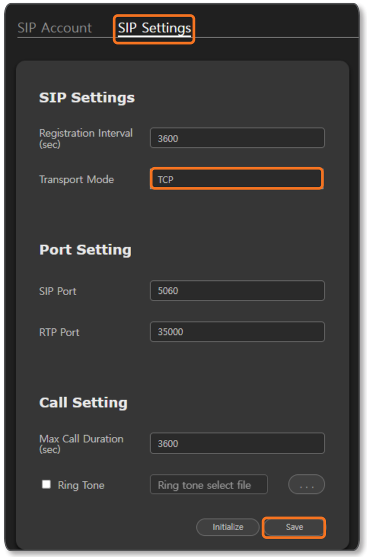


2. IP Speaker SIP TCP Settings

- Click <**Operate**> ➞ <**SIP Management**>.



- Click <**SIP Settings**>.
- Change the transmission mode to <**TCP**> and click the [**Save**] button.



SIP Settings

Registration Interval (sec): 3600

Transport Mode: TCP

Port Setting

SIP Port: 5060

RTP Port: 35000

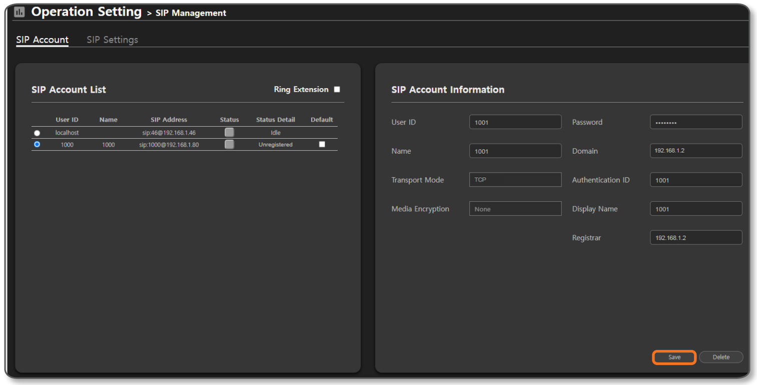
Call Setting

Max Call Duration (sec): 3600

□ Ring Tone: Ring tone select file

3. PBX SIP Account Registration and PBX Registration

- Click <**SIP Account**>.
- Enter the SIP account information, then click the [**Save**] button.



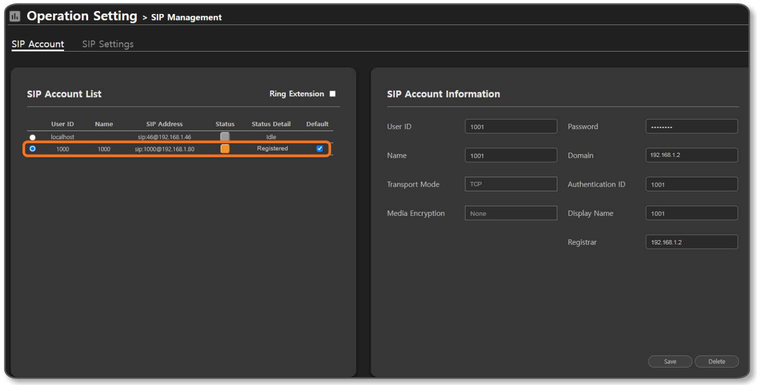
SIP Account List Ring Extension □

	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46		Idle	
●	1000	1000	sip:1000@192.168.1.80		Unregistered	□

SIP Account Information

User ID: 1001
Password: ········
Name: 1001
Domain: 192.168.1.2
Transport Mode: TCP
Authentication ID: 1001
Media Encryption: None
Display Name: 1001
Registrar: 192.168.1.2

- In the SIP account list, check the box for <**Default**> and make sure the status details are <**Registered**>. If successful, it will be displayed as shown below.



SIP Account List Ring Extension □

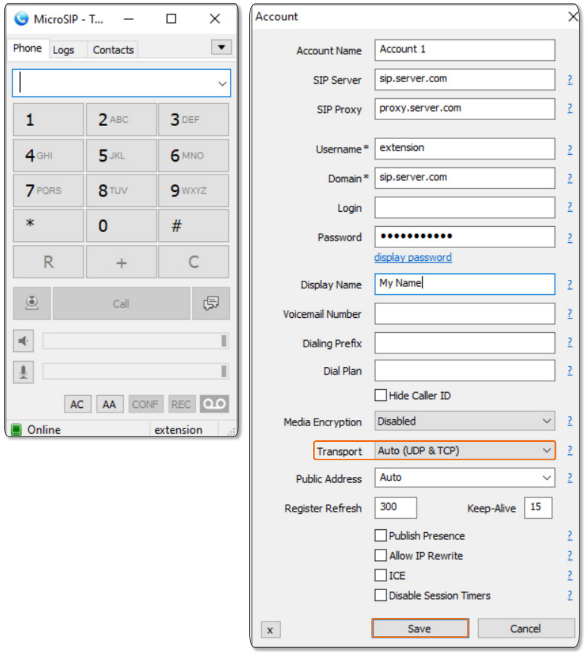
	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46		Idle	
●	1000	1000	sip:1000@192.168.1.80		Registered	☑

SIP Account Information

User ID: 1001
Password: ········
Name: 1001
Domain: 192.168.1.2
Transport Mode: TCP
Authentication ID: 1001
Media Encryption: None
Display Name: 1001
Registrar: 192.168.1.2

4. PC MicroSIP Program Account Information and PBX Registration

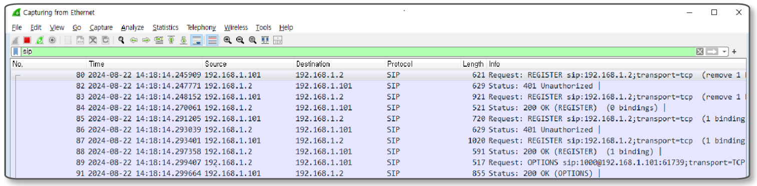
- After entering the account information in MicroSIP and setting the transport to <**TCP**>, click the [**Save**] button to attempt Registration with the PBX.



Account

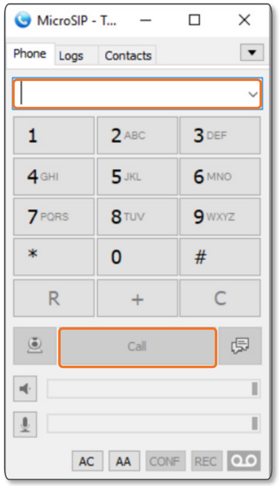
Account Name: Account 1
SIP Server: sip.server.com
SIP Proxy: proxy.server.com
Username*: extension
Domain*: sip.server.com
Login:
Password: ●●●●●●●●●●●
display password
Display Name: My Name
Voicemail Number:
Dialing Prefix:
Dial Plan:
□ Hide Caller ID
Media Encryption: Disabled
Transport: Auto (UDP & TCP)
Public Address: Auto
Register Refresh: 300 Keep-Alive: 15
□ Publish Presence
□ Allow IP Rewrite
□ ICE
□ Disable Session Timers

- You can check the SIP registration procedure by using the PC WireShark program to capture the packet.

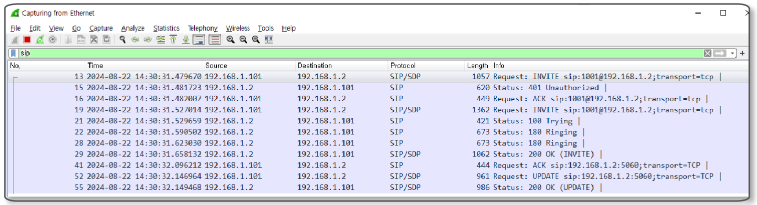

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip

```
No.    Time                        Source          Destination     Protocol   Length Info
    80 2024-08-22 14:18:14.245909 192.168.1.101   192.168.1.2     SIP          621 Request: REGISTER sip:192.168.1.2;transport=tcp  (remove 1
    82 2024-08-22 14:18:14.247771 192.168.1.2     192.168.1.101   SIP          629 Status: 401 Unauthorized |
    83 2024-08-22 14:18:14.248152 192.168.1.101   192.168.1.2     SIP          921 Request: REGISTER sip:192.168.1.2;transport=tcp  (remove 1
    84 2024-08-22 14:18:14.270061 192.168.1.2     192.168.1.101   SIP          521 Status: 200 OK (REGISTER)  (0 bindings) |
    85 2024-08-22 14:18:14.291205 192.168.1.101   192.168.1.2     SIP          720 Request: REGISTER sip:192.168.1.2;transport=tcp  (1 binding
    86 2024-08-22 14:18:14.293039 192.168.1.2     192.168.1.101   SIP          629 Status: 401 Unauthorized |
    87 2024-08-22 14:18:14.293401 192.168.1.101   192.168.1.2     SIP         1020 Request: REGISTER sip:192.168.1.2;transport=tcp  (1 binding
    88 2024-08-22 14:18:14.297358 192.168.1.2     192.168.1.101   SIP          591 Status: 200 OK (REGISTER)  (1 binding) |
    89 2024-08-22 14:18:14.299407 192.168.1.2     192.168.1.101   SIP          517 Request: OPTIONS sip:1000@192.168.1.101:61739;transport=TCP
    91 2024-08-22 14:18:14.299664 192.168.1.101   192.168.1.2     SIP          855 Status: 200 OK (OPTIONS) |
```

- Make a call from PC MicroSIP (192.168.1.101, Extension 1000) to IP Speaker (192.168.1.91, Extension 1001) to communicate.
- Enter the Extension 1001 number of the device you wish to call to in the prompt, then click the [**Call**] button.

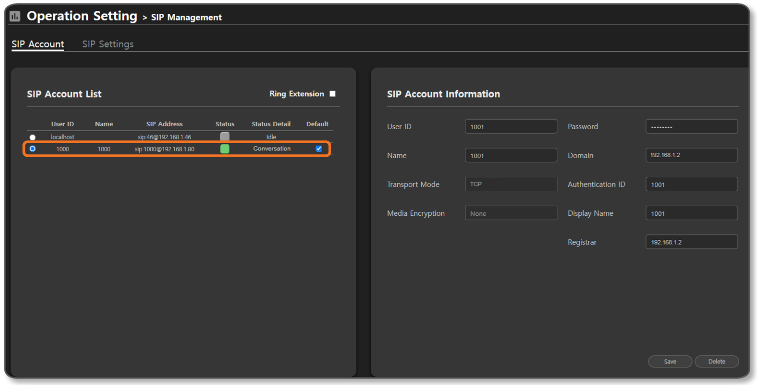


- You can check the SIP registration procedure by using the PC WireShark program to capture the packet.


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip

```
No.    Time                        Source          Destination     Protocol   Length Info
    13 2024-08-22 14:30:31.479670 192.168.1.101   192.168.1.2     SIP/SDP     1057 Request: INVITE sip:1001@192.168.1.2;transport=tcp |
    15 2024-08-22 14:30:31.481723 192.168.1.2     192.168.1.101   SIP          620 Status: 401 Unauthorized |
    16 2024-08-22 14:30:31.482007 192.168.1.101   192.168.1.2     SIP          449 Request: ACK sip:1001@192.168.1.2;transport=tcp |
    19 2024-08-22 14:30:31.527014 192.168.1.101   192.168.1.2     SIP/SDP     1362 Request: INVITE sip:1001@192.168.1.2;transport=tcp |
    21 2024-08-22 14:30:31.529659 192.168.1.2     192.168.1.101   SIP          421 Status: 100 Trying |
    22 2024-08-22 14:30:31.590502 192.168.1.2     192.168.1.101   SIP          673 Status: 180 Ringing |
    28 2024-08-22 14:30:31.623030 192.168.1.2     192.168.1.101   SIP          673 Status: 180 Ringing |
    29 2024-08-22 14:30:31.658132 192.168.1.2     192.168.1.101   SIP/SDP     1062 Status: 200 OK (INVITE) |
    41 2024-08-22 14:30:32.096212 192.168.1.101   192.168.1.2     SIP          444 Request: ACK sip:192.168.1.2:5060;transport=TCP |
    52 2024-08-22 14:30:32.146964 192.168.1.101   192.168.1.2     SIP/SDP      961 Request: UPDATE sip:192.168.1.2:5060;transport=TCP |
    55 2024-08-22 14:30:32.149468 192.168.1.2     192.168.1.101   SIP/SDP      986 Status: 200 OK (UPDATE) |
```

- If the call is successful, the status details of <**SIP Account List**> of the IP Speaker (192.168.1.91) will be displayed as <**Conversation**>.



SIP Account List

Ring Extension □

	User ID	Name	SIP Address	Status	Status Detail	Default
○	localhost		sip:46@192.168.1.46	⬜	Idle	
●	1000	1000	sip:1000@192.168.1.80	🟩	Conversation	☑

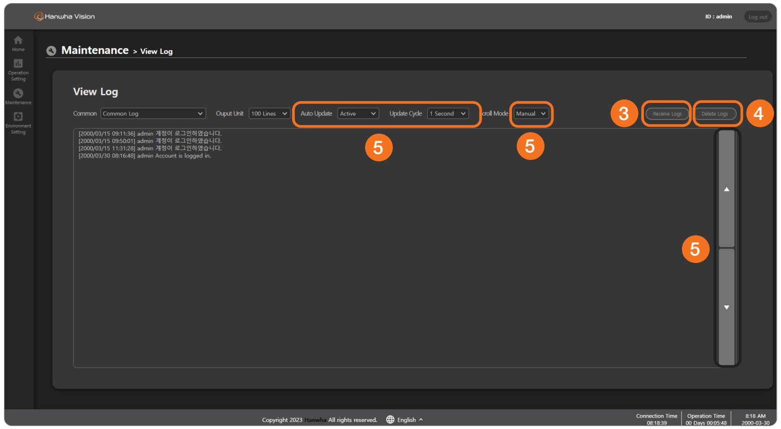
SIP Account Information

User ID: 1001
Password: ········
Name: 1001
Domain: 192.168.1.2
Transport Mode: TCP
Authentication ID: 1001
Media Encryption: None
Display Name: 1001
Registrar: 192.168.1.2

MAINTENANCE

View Log

Logs generated in the product can be checked.
The log items are different for each product, and they are recorded when the log operation occurs.



Common: Common Log
Ouput Unit: 100 Lines
Auto Update: Active
Update Cycle: 1 Second
croll Mode: Manual

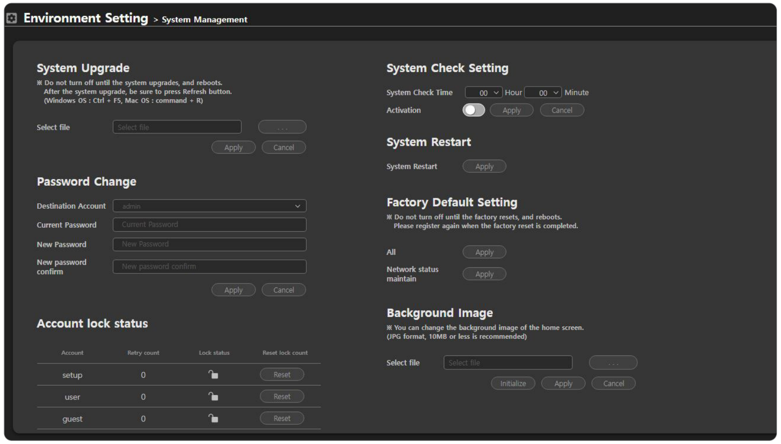
```
[2000/03/15 09:11:36] admin 계정이 로그인하였습니다.
[2000/03/15 09:50:01] admin 계정이 로그인하였습니다.
[2000/03/15 11:31:28] admin 계정이 로그인하였습니다.
[2000/03/30 08:16:48] admin Account is logged in.
```

Connection Time 08:18:39
Operation Time 00 Days 00:05:48
8:18 AM 2000-03-30

1. Click <**Maintenance**> ➞ <**View Log**> on the Home screen.
2. The action log history for the device is shown by item.
   The Log menu will appear on the 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, the file can be downloaded in the HTML format.
   Check HTML files using 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. The Output Unit, Auto Update, Update Cycle, and Scroll Mode can be set.
   If you activate <**Auto Update**>, logs will be displayed in accordance with the <**Update Cycle**> on the screen.
   - If you set <**Scroll Mode**> to automatic, the screen will be moved downward to show recent logs.
   - Press the [▲/▼] button to view the upper and lower logs.

SYSTEM MANAGEMENT

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



※ Do not turn off until the system upgrades, and reboots.
After the system upgrade, be sure to press Refresh button.
(Windows OS : Ctrl + F5, Mac OS : command + R)

Destination Account: admin

Account	Retry count	Lock status	Reset lock count
setup	0	🔓	Reset
user	0	🔓	Reset
guest	0	🔓	Reset

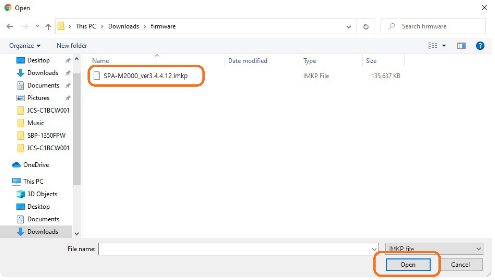
System Check Time: 00 Hour 00 Minute
Activation: ○

※ Do not turn off until the factory resets, and reboots.
Please register again when the factory reset is completed.

※ You can change the background image of the home screen.
(JPG format, 10MB or less is recommended)

Upgrading the System

1. Click <**Environment Setting**> ➞ <**System Management**> on the Home screen.
2. Click the [. . .] button in <**System Upgrade**>.
3. 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]**.



Name	Date modified	Type	Size
SPA-M2000_ver3.4.4.12.imkp		IMKP File	135,637 KB

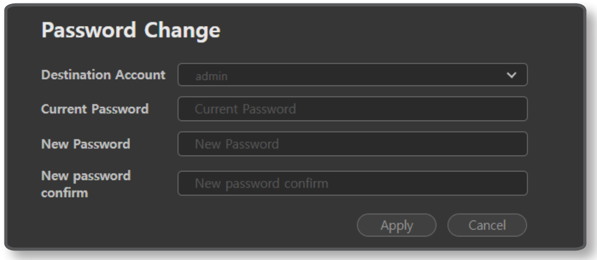
4. Click **[Apply]** to start System Upgrade. Click **<OK>** when the "**System Restart**" window appears after up to five minutes.

- 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.

5. 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.



Password Change

Destination Account: admin

Current Password: Current Password

New Password: New Password

New password confirm: New password confirm

1. On the Home screen, click **<Environment Setting> ➞ <System Management>**.
2. By clicking <**Destination Account**> from <**Change Password**>, select the account you want to change and set the password.
3. Click the [**Apply**] button after entering a new password in the two input fields.
4. 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.
5. The password of the setup, user, and guest accounts can be set, changed, or reset from the admin account if they are forgotten.

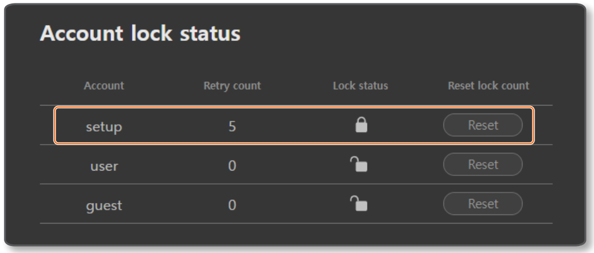
Viewing the supported menu by account

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**: The system management, network settings, time settings, and log history can be viewed.
- **setup**: The SIP settings and log history can be viewed.
- **user**: The log history can be viewed.
- **guest**: The product information can be checked 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.



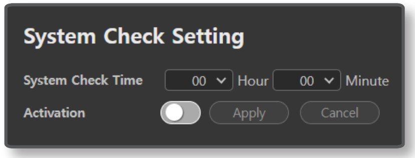
Account lock status

Account	Retry count	Lock status	Reset lock count
setup	5	🔒	Reset
user	0	🔓	Reset
guest	0	🔓	Reset

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.

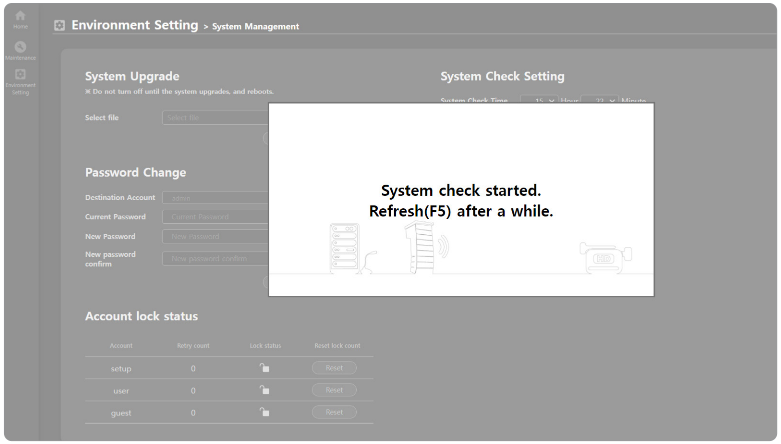


System Check Setting

System Check Time 00 Hour 00 Minute

Activation

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 **<Activation>**.
4. The system will be checked and be rebooted at the set time➞ it will take approximately 5 minutes.



Environment Setting > System Management

System Upgrade

※ Do not turn off until the system upgrades, and reboots.

Select file

System Check Setting

System Check Time 15 Hour 22 Minute

Password Change

Destination Account admin

Current Password

New Password

New password confirm

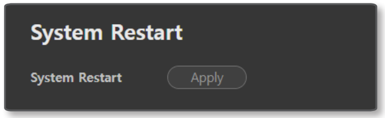
System check started.
Refresh(F5) after a while.

Account lock status

Account	Retry count	Lock status	Reset lock count
setup	0		Reset
user	0		Reset
guest	0		Reset

Restarting System

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



System Restart

System Restart

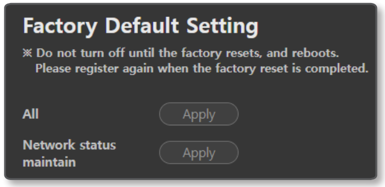
1. On the Home screen, click **<Environment Setting>** ➞ **<System Management>**.
2. Click the **[Apply]** button in **<System Restart>**.
3. Click **<OK>** when the system restarting window appears.
   It will take approximately 5 minutes to reboot the system.

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.

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.



Factory Default Setting

※ Do not turn off until the factory resets, and reboots.
Please register again when the factory reset is completed.

All

Network status maintain

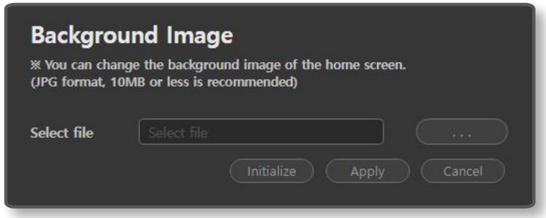
3. Click **<OK>** when the factory default window appears. Product initialization starts.
4. Click **<OK>** when the system start window appears on the web browser.

- **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.



Background Image

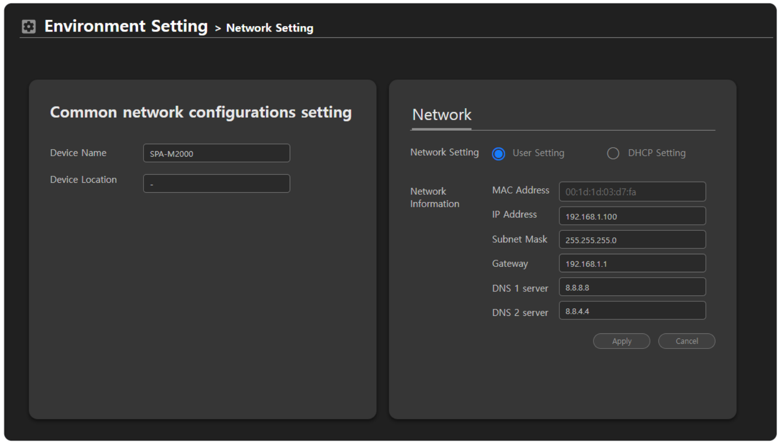
※ You can change the background image of the home screen.
(JPG format, 10MB or less is recommended)

Select file: Select file

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>**.



Environment Setting > Network Setting

Common network configurations setting

Device Name: SPA-M2000
Device Location: -

Network

Network Setting: ● User Setting ○ DHCP Setting

Network Information
MAC Address: 00:1d:1d:03:d7:fa
IP Address: 192.168.1.100
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS 1 server: 8.8.8.8
DNS 2 server: 8.8.4.4

- 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.

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

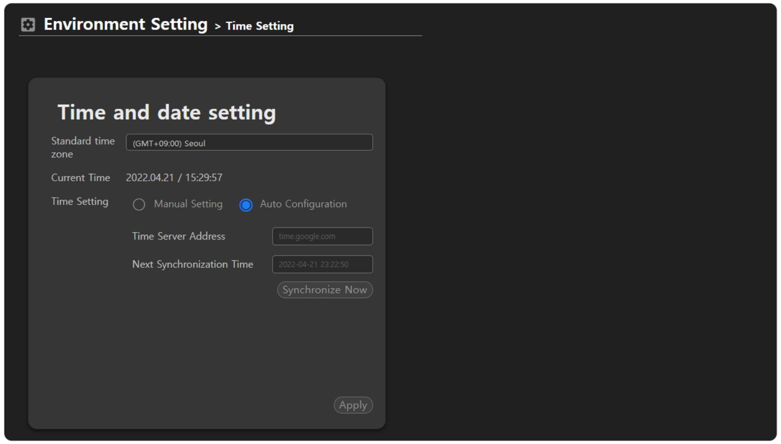
- The IP, subnet mask, gateway, DNS 1 and DNS 2 server addresses for the product will be allocated automatically from the DHCP server by selecting <**DHCP Setting**> in <**Network Setting**>.
- Click [**Apply**] to apply the set network information to the product.
- Click [**Cancel**] to return to the 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>**.



Environment Setting > Time Setting

Time and date setting

Standard time zone: (GMT+09:00) Seoul

Current Time: 2022.04.21 / 15:29:57

Time Setting: ○ Manual Setting ● Auto Configuration

Time Server Address: time.google.com

Next Synchronization Time: 2022-04-21 23:22:50

- 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 <**User 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 Settings**> 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 [**Synchronization Now**] to synchronize the time to the time server.

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

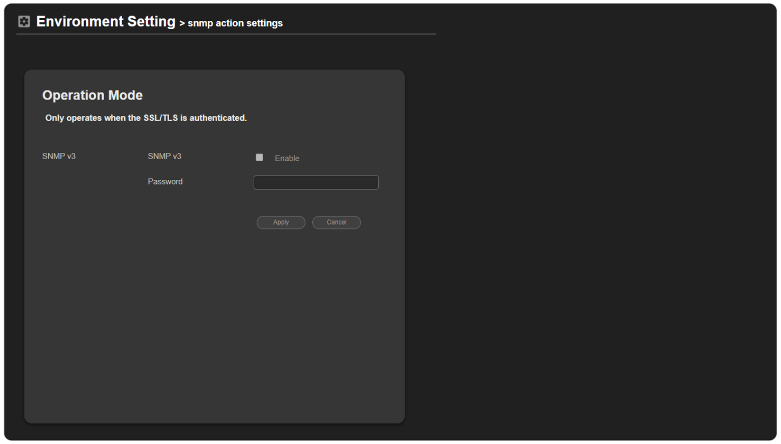
- If the product is used in a local network environment without an external Internet connection, the time information may become incorrect due to the product’s accumulated time errors. To accurately schedule the broadcasting time, we recommend installing a separate time server device using GPS signals 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>**.



Environment Setting > snmp action settings

Operation Mode

Only operates when the SSL/TLS is authenticated.

SNMP v3 — SNMP v3: □ Enable

Password:

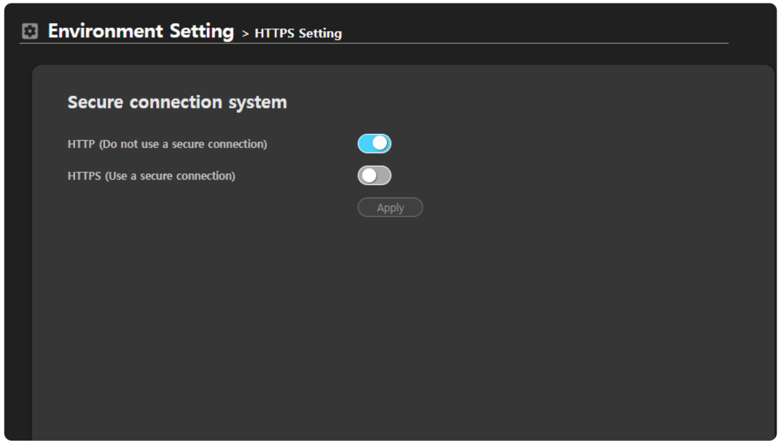
- Use SNMP v3: SNMP v3 is used.
  - Password : Set the initial user password for SNMP v3.
    The initial password is insecure, so we recommend that you change it to a new password.
    The password must be between 8 and 16 characters long, and some special characters (\, |, <, >, ‘, “, /, ?) are not 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>**.



Environment Setting > HTTPS Setting

Secure connection system

HTTP (Do not use a secure connection) ●

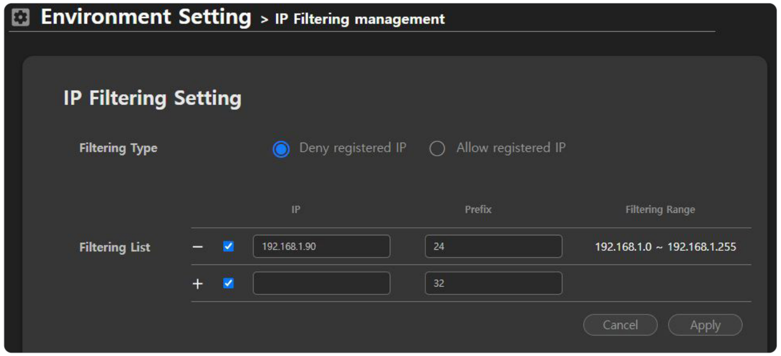
HTTPS (Use a secure connection) ○

- Secure connection system: Select a secure connection method according to the operation environment, considering the security level. HTTPS (HyperText Transfer Protocol over Secure Socket Layer) exchanges data through encryption and decryption for page requests from users in the SSL sublayer below the hypertext transfer protocol layer. Therefore, it may be more secure than the HTTP mode.
  - ▪ HTTP (Do not use a secure connection): Select when you want to transmit data over HTTP without encryption.
  - ▪ HTTPS (Use a secure connection): Select when you want 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>**.



Environment Setting > IP Filtering management

IP Filtering Setting

Filtering Type: ● Deny registered IP ○ Allow registered IP

Filtering List

		IP	Prefix	Filtering Range
–	☑	192.168.1.90	24	192.168.1.0 ~ 192.168.1.255
+	☑		32	

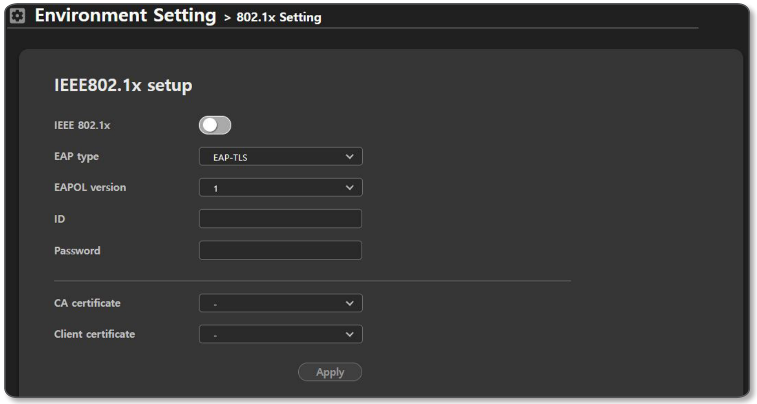
- Filtering Type
  - Deny registered IP: Denies access for a registered IP.
  - Allow registered IP: Allows access for a registered IP
- Filtering List : Enter the IP and Prefix information. The filtering range for the entered information will be displayed.
  - IP address : Displays the registered IP 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>**.



Environment Setting > 802.1x Setting

IEEE802.1x setup

IEEE 802.1x

EAP type: EAP-TLS

EAPOL version: 1

ID

Password

CA certificate: -

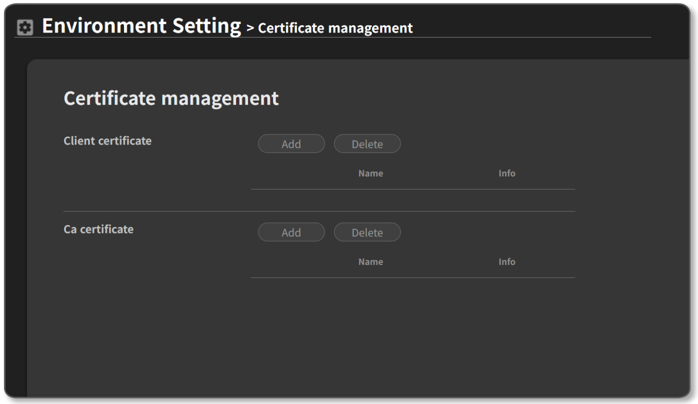
Client certificate: -

- 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**>**.



Environment Setting > Certificate management

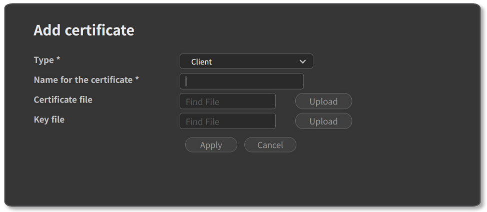
Certificate management

Client certificate

Ca certificate

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.
i Clicking the button shows the certificate information.



Add certificate

Type *: Client

Name for the certificate *

Certificate file: Find File

Key file: Find File

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.

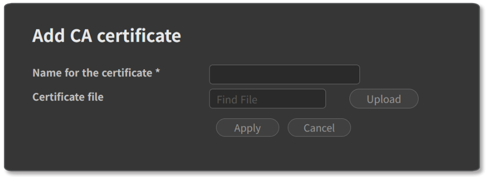
3. To create a certificate, select **<Self-signed>** among **<Type>** options in the **[Add certificate]** dialog and set each item.
4. In the <**Add certificate**> dialog, click the <**OK**> button to save the entered information in the list.

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). i Clicking the button shows the certificate information.



Adding a CA certificate

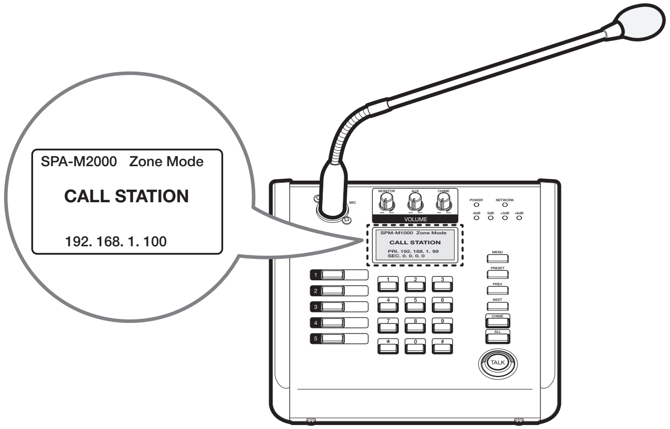
1. Click the [**Add**] button.
2. In the <**Add CA certificate**> dialog:
   - Certificate name: Enter the certificate name.
   - Certificate file: Click [**Upload**] and select the certificate file.
3. In the <**Add CA certificate**> dialog, click the [**OK**] button to save the entered information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

Deleting a CA certificate

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

using the microphone

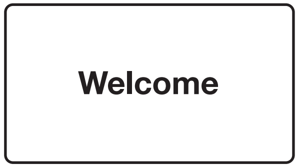
When using the microphone, you can check the input number and current status through the status indicator of the product.

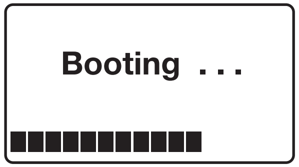


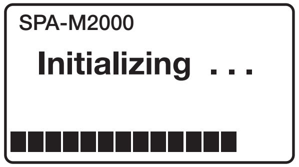
POWER ON

Initial Screen

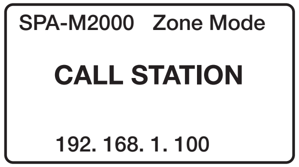
1. When the product is powered on, a **<Welcome>** message will be displayed on the status indicator.
2. After about 5 seconds, the **<Booting ...>** message will be displayed, and then the **<Initializing ...>** message will appear.
3. When the product is booted up, the status indicator will be displayed as a standby screen.


Welcome


Booting . . .


SPA-M2000

Initializing . . .

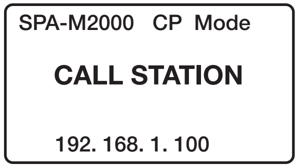

SPA-M2000 Zone Mode

CALL STATION

192. 168. 1. 100

Standby Screen

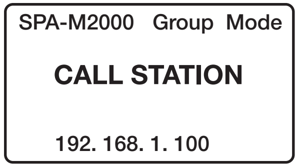
By pressing the **<MENU>** button on the main body of the product, it will be divided into 4 modes according to the **<3. Talk Protocol>** setting in the **<Talk type>** menu as follows. You can switch each mode with the **[PRESET]** button on the product body.


SPA-M2000 CP Mode

CALL STATION

192. 168. 1. 100

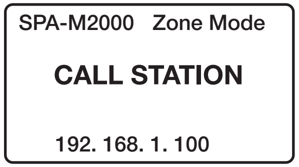
If <Talk Protocol> is in the Isls-CP


SPA-M2000 Group Mode

CALL STATION

192. 168. 1. 100

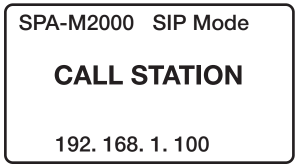
If <Talk Protocol> is in the Isls-Group


SPA-M2000 Zone Mode

CALL STATION

192. 168. 1. 100

If <Talk Protocol> is in the Isls-Zone

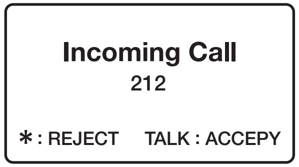

SPA-M2000 SIP Mode

CALL STATION

192. 168. 1. 100

If <Talk Protocol> is in the SIP

- If there is no button input for about 30 seconds on the standby screen, it will enter sleep mode and the status indicator will turn off.
  Press any button to switch from sleep mode to the standby screen.
- When receiving a SIP call on the standby screen, you can hear the other party's voice through the speaker of the main body.

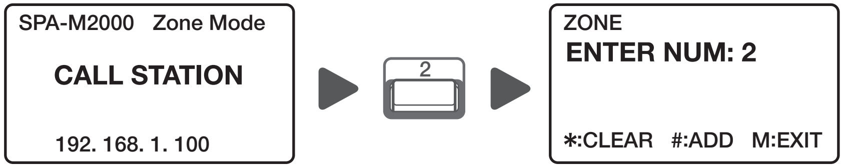

Incoming Call

212

∗ : REJECT TALK : ACCEPY

BROADCASTING

1. If you press any number button while on the standby screen, the broadcasting mode (Zone, Group, CP, SIP) set in **<Talk Protocol>** and the entered number will be displayed on the screen.

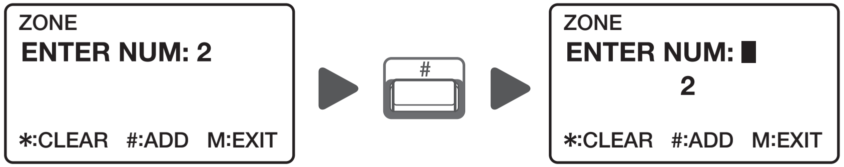


SPA-M2000 Zone Mode
CALL STATION
192. 168. 1. 100

ZONE
ENTER NUM: 2
∗:CLEAR #:ADD M:EXIT

- The number specified in the zone registration and group setting menus of the controller device will be selected for Zone and Group mode.
  The VP number specified in the Event & Preset menu of the controller device will be selected for CP mode.
- While on the Number input screen, press the **[MENU]** button on the product body to end number input and switch to the standby screen.
- An incorrectly entered number can be deleted by pressing the **[∗]** button. (Role of Backspace)

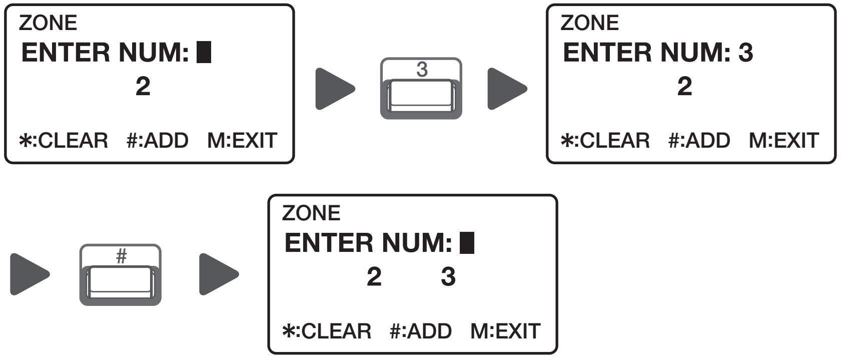
2. Press the **[#]** button to register the entered number.



ZONE
ENTER NUM: 2
∗:CLEAR #:ADD M:EXIT

ZONE
ENTER NUM: ▮
2
∗:CLEAR #:ADD M:EXIT

3. If there are more numbers to broadcast, press the appropriate Number button and then press the **[#]** button.



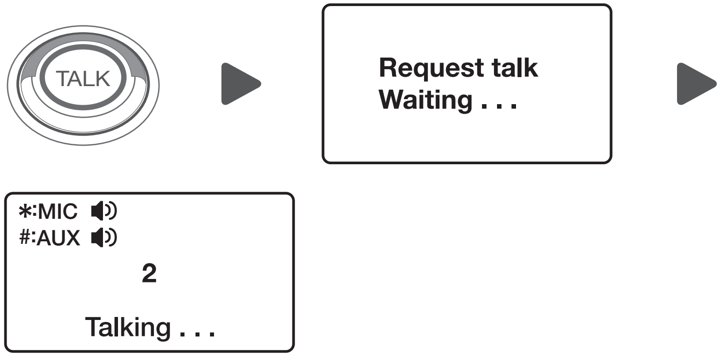
ZONE
ENTER NUM: ▮
2
∗:CLEAR #:ADD M:EXIT

ZONE
ENTER NUM: 3
2
∗:CLEAR #:ADD M:EXIT

ZONE
ENTER NUM: ▮
2 3
∗:CLEAR #:ADD M:EXIT

- To cancel a registered number, press the button of the number and then press the **[∗]** button to delete the number.
- For SIP, only one number can be registered.

4. When the number registration is complete, press the **[TALK]** button on the product body.



Request talk
Waiting . . .

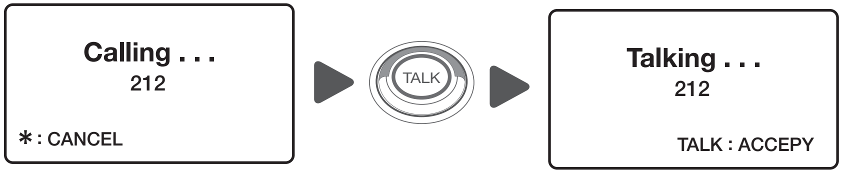
∗:MIC 🔊
#:AUX 🔊
2
Talking . . .

5. When the **<Talking...>** screen is displayed, start broadcasting with the microphone.

- If the product is not registered as an RM source in the controller device of the network audio system, the **<Request talk>** screen will display for about 10 seconds and then switch back to the standby screen.
- If the product is registered as a device and RM source and Event & Preset, Zone, and Group are normally set and operated in the controller device, the screen will switch to **<Talking...>**.

- Press the **[∗]** button on the **<Talking...>** screen to mute the microphone volume, and press the **[#]** button to mute the external audio source (AUX) volume. You cannot mute the volume of the microphone and AUX at the same time.
- The way the **[TALK]** button is used depends on the product's **<Talk type>** settings. Refer to "**Talk Type Settings**" for details. (Page 34)

6. If you press the [**CHIME**] button in the <**Talking...**> state, the chime which is set in [**Start Chime Set**] will appear. If you press it once more, the chime which is set in [**End Chime Set**] will appear.
7. If <**Talk Protocol**> is in SIP mode, enter the last 3 octets of the target device's IP address and then press the [**Talk**] button.



Calling . . .
212
∗ : CANCEL

Talking . . .
212
TALK : ACCEPY

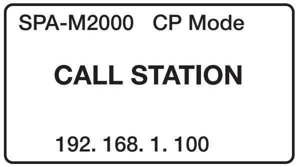
8. When a SIP call is connected, it switches to the call screen. Listen to the other party's voice through the speaker of the main body.

- In case of SIP Local Call (using the IP's last digits), they must have been configured with LAN (dedicated network).
- The 1:N mapping is not supported for SIP Local Call (using the IP's last digits) between the remote microphones.

USING CP EVENT BUTTON

If the microphone event is set as <**CP**> in the <**All Event & Preset List**> of the controller mode speaker or audio server, you can generate the event by pressing the CP event button (5 key) on the left side of the microphone.

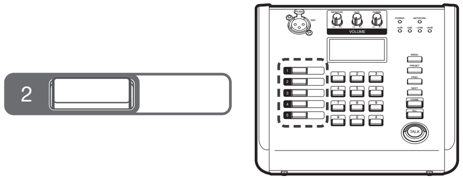
1. Press the desired CP event button on the standby screen.

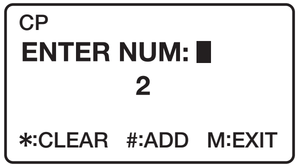


SPA-M2000 CP Mode

CALL STATION

192. 168. 1. 100





CP

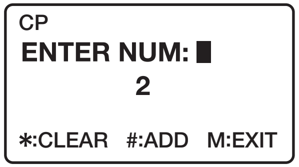
ENTER NUM: ▮

2

∗:CLEAR #:ADD M:EXIT

- While on the Number input screen, press the **[MENU]** button on the product body to end number input and switch to the standby screen.

2. If there are more event numbers to add, press the corresponding CP event button.

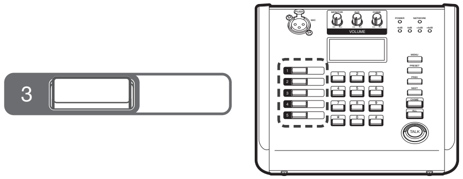


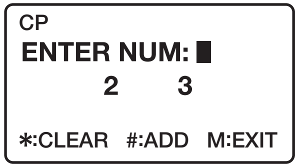
CP

ENTER NUM: ▮

2

∗:CLEAR #:ADD M:EXIT





CP

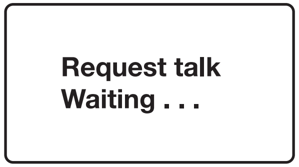
ENTER NUM: ▮

2 3

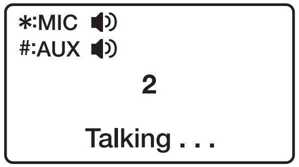
∗:CLEAR #:ADD M:EXIT

- To cancel the registered CP event number, press the button once more to delete the number.

3. When the registration of the CP event number is completed, press the **[TALK]** button on the product body.



Request talk
Waiting . . .



∗:MIC 🔊
#:AUX 🔊

2

Talking . . .

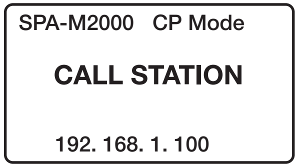
4. When the **<Talking...>**screen is displayed, the set event of the entered CP number will occur.

USING VP EVENT BUTTON

If the microphone event is set as <**VP**> in the <**All Event & Preset List**> of the controller mode speaker or audio server, you can generate the event by pressing the number button (10 key) in the middle of the microphone.

The microphone event can be set up as either <**CP**> or <**VP**>.

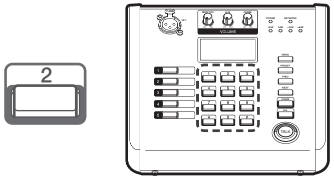
1. Press the desired VP event button on the standby screen.

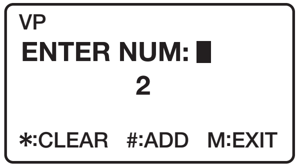


SPA-M2000 CP Mode

CALL STATION

192. 168. 1. 100





VP

ENTER NUM: ▮

2

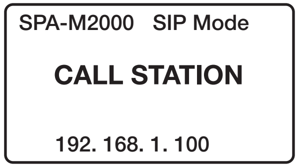
∗:CLEAR #:ADD M:EXIT

2. If there are more event numbers to add, click the corresponding VP event button.
3. When the registration of the VP event number is completed, press the [**TALK**] button on the product body.
4. When the <**Talking...**>screen is displayed, the set event of the entered VP number occurs.

USING THE SIP SHORTCUT KEYS

You can call a device registered as a SIP shortcut key by pressing the button (5 key) on the left of the microphone.

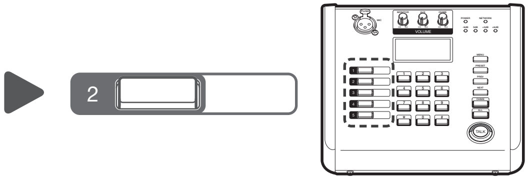
1. Press the desired SIP shortcut key on the standby screen.

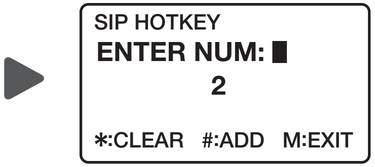


SPA-M2000 SIP Mode

CALL STATION

192. 168. 1. 100





SIP HOTKEY

ENTER NUM: █

2

∗:CLEAR #:ADD M:EXIT

2. When the number registration is complete, press the [TALK] button on the product body.
3. When <**Calling...**> appears, calling to the entered number begins.

USING MENU

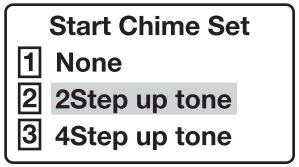
If you press the **[MENU]** button on the product body, you can change the **<Chime>** and **<Talk type>** settings, or you can check the network information and firmware version.

Each time the **[MENU]** button is pressed, **<Start Chime Set>➞<End Chime Set>➞<Talk type>➞** Network Information ➞ the Firmware Information screen will switch sequentially.

Chime Settings

You can set the type of chime that indicates the start and end of a microphone broadcast.

1. Press the **[MENU]** button on the product body.
2. After selecting the **<Start Chime Set>** setting screen, press buttons 1-3 to select the desired chime output method.



Start Chime Set

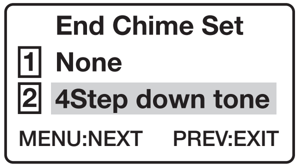
1 None

2 2Step up tone

3 4Step up tone

- Before starting the microphone broadcast on the **<Talking>** screen, if you press the **[CHIME]** button, you will hear the chime you set at **<Start Chime Set>**.

3. Press the **[MENU]** button once more.
4. Press button 1 or 2 on the **<End Chime Set>** setting screen to select the desired chime output method.



End Chime Set

1 None

2 4Step down tone

MENU:NEXT PREV:EXIT

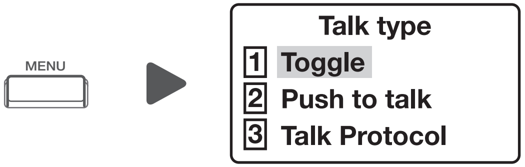
- Before ending the microphone broadcast on the **<Talking>** screen, if you press the **[CHIME]** button, you will hear the chime you set at **<End Chime Set>**.

5. Press the **[PREV]** button to exit the chime settings.

Talk Type Settings

You can set the **[TALK]**button usage method when making a microphone broadcast.

1. Press the **[MENU]** button on the product body.
2. After selecting the **<Talk type>** setting screen, press buttons 1 or 2 to select the desired method.
   - **<Toggle>**: If you press the **[TALK]** button, the **<Request talk Waiting>** screen will appear, and after a while, the screen will switch to the **<Talking>** screen and microphone broadcasting will be available.
   - **<Push to talk>**: If the **<Request talk Waiting>** screen appears while pressing the **[TALK]** button, **<Talking>** screen will appear after a while. Then, microphone broadcasting will be available.



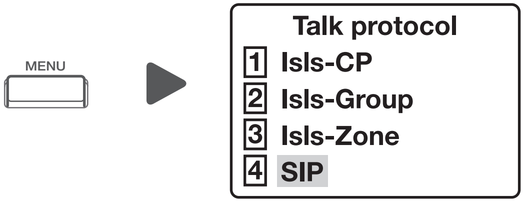
Talk type
1 Toggle
2 Push to talk
3 Talk Protocol

3. Press the **[PREV]** button to exit the **<Talk type>**settings.

Talk Protocol Settings

You can set the communication protocol method with the controller device the product is registered with.

1. Press the **[MENU]** button on the product body.
2. After selecting the **<Talk type>** setting screen, press button 3 to select **<Talk Protocol>**.
3. Select the desired protocol method.
   - **<Isls-CP>**: It operates in CP Mode. If you enter the CP event button (5key) or 10key button on the microphone body and press the [**TALK**] button, the VP event set in the <**Event & Preset**> menu of the controller device will occur.
   - **<Isls-Group>**: It operates in Group Mode. If you press the 10 key button on the microphone body and press the **[TALK]** button, it will broadcast to the group set in the **<Group Settings>** menu of the controller device.
   - **<Isls-Zone>**: It operates in Zone Mode, and if you input the 10 key button on the microphone body and press the **[TALK]** button, it will broadcast to the zone set in the **<Zone registration>** menu of the controller device.
   - **<SIP>**: It operates in SIP Mode, and if you enter the CP event button (5key) or 10key button on the microphone body and then press the [**TALK**] button, the SIP call begins.



Talk protocol
1 Isls-CP
2 Isls-Group
3 Isls-Zone
4 SIP

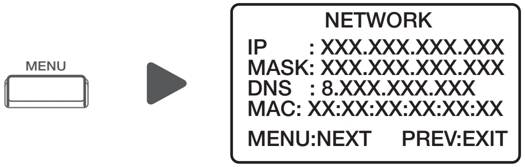
4. Press the **[PREV]**button to exit the **<Talk Protocol>**settings.

- On the standby screen, press the **[PRESET]** button on the microphone body to switch the **<Talk Protocol>**method.

Checking Network Information

You can check the network information set in the product.

1. Press the **[MENU]** button on the product body.
2. The **<NETWORK>** information screen will be displayed.



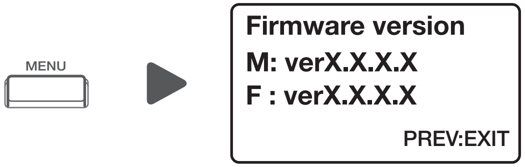
```
NETWORK
IP     : XXX.XXX.XXX.XXX
MASK: XXX.XXX.XXX.XXX
DNS  : 8.XXX.XXX.XXX
MAC: XX:XX:XX:XX:XX:XX
MENU:NEXT    PREV:EXIT
```

3. Press the **[PREV]** button to close the Network information screen.

Checking Firmware Version Information

You can check the current firmware version of the product.

1. Press the **[MENU]** button on the product body.
2. The **<Firmware version>** information screen will be displayed.



```
Firmware version
M: verX.X.X.X
F : verX.X.X.X
              PREV:EXIT
```

- **(M : Main board firmware version, F : Front board firmware version)**

3. Press the **[PREV]** button to close the Firmware information screen.

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.

eco
RoHS compliant

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.

Hanwha
Vision