

Panasonic®

Operating Instructions

Network Microphone

Model No. **WV-SMR10**



Before attempting to connect or operate this product, please read these instructions carefully and save this manual for future use.

Preface

About the user manuals

There are 3 sets of operating instructions as follows.

- Operating Instructions (this document): Explains how to perform the settings and how to operate this microphone.
- Important Information: Provides information about the cautions required for safely using and installing this microphone.
- Installation Guide: Explains how to install and connect devices.

Trademarks and registered trademarks

- Microsoft, Windows, Windows Vista, Internet Explorer, and ActiveX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.
- All other trademarks identified herein are the property of their respective owners.

Abbreviations

The following abbreviations are used in these operating instructions.

Microsoft® Windows® 8.1 is described as Windows 8.1.

Microsoft® Windows® 8 is described as Windows 8.

Microsoft® Windows® 7 is described as Windows 7.

Microsoft® Windows Vista® is described as Windows Vista.

Windows® Internet Explorer® 11, Windows® Internet Explorer® 10, Windows® Internet Explorer® 9, Windows® Internet Explorer® 8, and Windows® Internet Explorer® 7 are described as Internet Explorer.

Universal Plug and Play is described as UPnP™.

In this document, the Panasonic 360° network camera (WV-SF438, WV-SF448, WV-SF448E, and WV-SW458) is described as 360° camera.

Plugin software

It is necessary to install the plugin software “Network Microphone Plugin” (ActiveX®) to use the functions of the microphone. This software can be installed directly from the microphone or by selecting the [Install] button next to [Plug-in software] on the menu of the CD-ROM provided, and then following the on-screen instructions.

Furthermore, a network camera can be used with the microphone by registering it. It is necessary to install separate plugin software to display network camera images. For further information, refer to the operating instructions of the network camera to be used.



IMPORTANT

- The default setting of "Automatic installation of plug-in software" is "On". Follow the instructions on page 76 when the message is displayed on the information bar of the browser.
- When the "Live" page is displayed for the first time, the install wizard of the required plugin software will be displayed. Follow the instructions of the wizard.
- When the install wizard is displayed again even after completing the installation of the plugin software, restart the PC.

Table of Contents

- 1 Monitor sound on a PC6**
- 1.1 Display the “Live” page6
- 1.2 About the “Live” page9
- 1.3 Listen to audio11
- 2 Action at a malfunction notification12**
- 2.1 Action at a malfunction notification12
- 3 About the network security13**
- 3.1 Equipped security functions13
- 4 Display the setup menu from a PC14**
- 4.1 How to display the setup menu14
- 4.2 How to operate the setup menu15
- 4.3 About the setup menu window16
- 5 Configure the basic settings of the microphone [Basic]18**
- 5.1 Configure the basic settings [Basic]18
- 5.2 Configure the Internet settings [Internet]20
- 6 Configure the settings relating to audio [Audio]22**
- 7 Register a camera for the “Live” page [Camera reg.]24**
- 8 Configure the malfunction notification settings [Failure Notif.]26**
- 9 Configure the settings relating to the authentication [User mng.]28**
- 9.1 Configure the settings relating to the user authentication [User auth.]28
- 9.2 Configure the settings relating to the host authentication [Host auth.]29
- 9.3 Configure the settings relating to the priority stream [System]30
- 10 Configuring the network settings [Network]32**
- 10.1 Configure the network settings [Network]32**
- 10.2 Configure advanced network settings [Advanced]35**
- 10.2.1 Configure the settings relating to the NTP server35
- 10.2.2 Configure the UPnP settings37
- 10.2.3 Configure the HTTPS settings38
- 10.2.4 Configure the settings relating to DDNS39
- 10.2.5 Configure the settings relating to SNMP40
- 10.2.6 Configure the Diffserv settings41
- 10.3 How to configure HTTPS settings42**
- 10.3.1 Generation of the CRT key (SSL encryption key)43
- 10.3.2 Generation of the self-signed certificate (security certificate)44
- 10.3.3 Generation of CSR (Certificate Signing Request)46
- 10.3.4 Installation of the server certificate47
- 10.3.5 Configuration of the connection protocol48
- 10.4 Access the microphone using the HTTPS protocol49**
- 10.4.1 Install the security certificate49
- 10.5 How to configure the settings relating to DDNS55**
- 10.5.1 When using “Dynamic DNS Update”56
- 10.5.2 When using “Dynamic DNS Update(DHCP)”56

11 Maintenance of the microphone [Maintenance]	57
11.1 Check the system log [System log]	57
11.2 Upgrade the firmware [Upgrade]	57
11.3 Check the status [Status]	59
11.4 Reset the settings/Reboot the microphone [Default reset]	60
11.5 Settings data/backing up or restoring logs [Data]	60
12 Using the CD-ROM	62
12.1 About the CD launcher	62
12.2 Installing Panasonic “IP Setting Software”	63
12.3 Installing the manuals	64
12.4 Installing the plugin software	64
12.5 Configure the network settings of the microphone using the Panasonic “IP Setting Software”	65
13 About the displayed system log	68
14 Troubleshooting	70

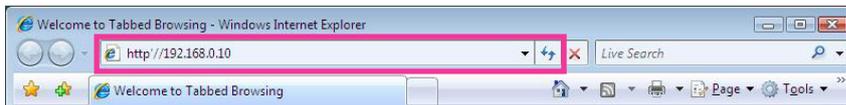
1 Monitor sound on a PC

The following are descriptions of how to monitor sound by accessing the network microphone from a PC, and how to display the screens of registered cameras.

1.1 Display the “Live” page

1. Start up the web browser.
2. Enter the IP address designated using the Panasonic “IP Setting Software” in the address box of the browser.
 - **Example when entering an IPv4 address:** http://URL registered using IPv4 address
http://192.168.0.10/
 - **Example when entering an IPv6 address:** http://[URL registered using IPv6 address]
http://[2001:db8::10]/

<Example of IPv4 access>



<Example of IPv6 access>



IMPORTANT

- When the HTTP port number is changed from “80”, enter “http://IP address of the microphone + : (colon) + port number” in the address box of the browser. (Example: http://192.168.0.11:8080)
- When the PC is in a local network, configure the proxy server setting of the web browser (under [Internet Options...] under [Tools] of the menu bar) to bypass the proxy server for the local address.

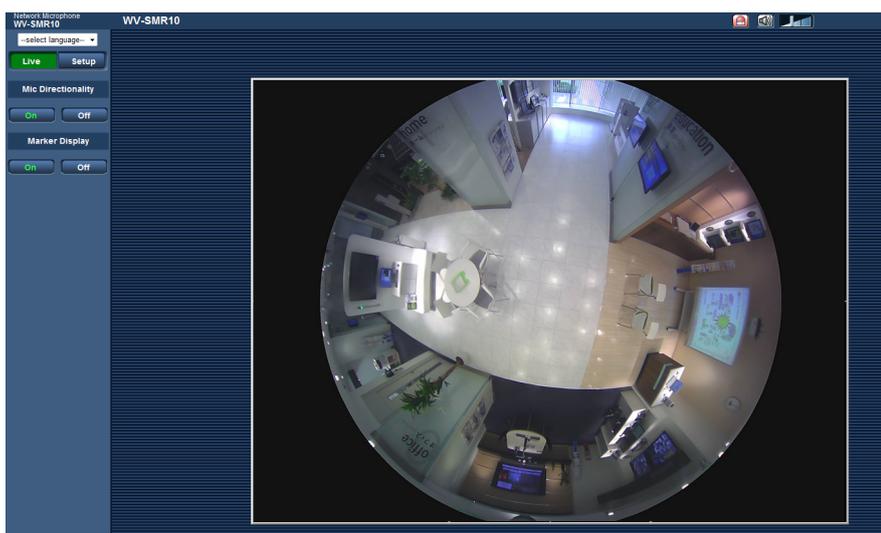
Note

- Refer to page 49 for further information about the case in which “HTTPS” is selected for “HTTPS” - “Connection” on the [Advanced] tab of the “Network” page (→page 32).
3. Press the [Enter] key on the keyboard.
 - The “Live” page of the microphone will be displayed. The layout of the “Live” page varies depending on whether a camera that displays images is registered or not. Refer to page 9 for further information about the “Live” page.

When a camera is not registered



When a camera is registered



When “On” is selected for “User auth.,” the authentication window will be displayed before displaying live images for the user name and password entries. The default user name and password are as follows.

User name: admin

Password: 12345

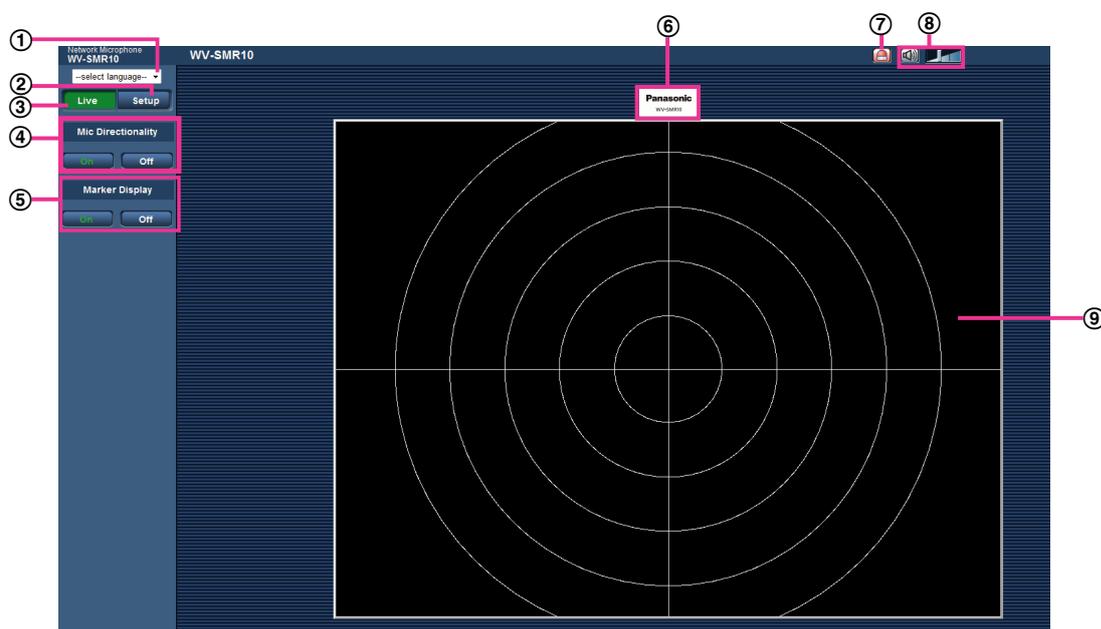
IMPORTANT

- To enhance the security, change the password for the user name “admin”. It is recommended to change this password periodically.
- When displaying live images, user name and password entry of the camera is required depending on the “User auth.” settings of the camera.
- Images from the camera may not display depending on the security settings of the browser. (→page 70)
- Audio from multiple “Live” pages cannot be monitored on one PC.

Note

- A maximum of 3 users can concurrently access the microphone and receive audio. If 3 users are concurrently accessing the microphone, the access limit message will be displayed for users who subsequently attempt to access the microphone. When “Multicast” is selected for “Transmission type” of audio, only the first user who is receiving “Live” images will be included in the maximum number. The second and subsequent users will not be included in the maximum number.

1.2 About the “Live” page



- ① **[select language] pull-down-menu**
The camera's display language can be selected. The default language can be set in the [Language] in the [Basic] settings. (→page 18)
- ② **[Setup] button**
Displays the setup menu. The button will turn green and the setup menu will be displayed.
- ③ **[Live] button**
Displays the “Live” page. The button will turn green and the “Live” page will be displayed.
- ④ **[Mic Directionality] button**
The directionality of the audio can be selected. The default setting when the “Live” page is displayed is “On” (audio with directionality), but because the directional position is not yet designated, the audio does not have actual directionality. Clicking on a position of the desired direction on the live image gives the audio directionality.
 - **[On] button:** The letters on the button will turn green and the audio of the images in the main area will have directionality.
 - **[Off] button:** The letters on the button will turn green and the audio of the images in the main area will not have directionality.
- ⑤ **[Marker Display] button**
Displays on images in the main area and switches between displaying and hiding the marker indicating the audio directionality position. The default setting when the “Live” page is displayed is “On” (display marker), but because the directional position is not yet designated, the marker is not actually displayed. Clicking on a position of the desired direction on the live image displays the marker.
 - **[On] button:** Marker is displayed.
 - **[Off] button:** Marker is hidden.
- ⑥ **Panasonic logo**
Indicates the position corresponding to the Panasonic logo printed on the microphone.
- ⑦ **Malfunction notification button**
This button will blink when a microphone malfunction is detected. When this button is clicked, the blinking will stop. Check the system log screen in the maintenance menu. (→page 12)
- ⑧ **Mic input button**
Turns on/off the audio output.

1 Monitor sound on a PC

When this button is clicked, the button will turn into the  button and audio from the microphone will not be heard on the PC.

Audio volume can be adjusted (Low/ Middle/ High) by moving the volume cursor .

Note

- The default setting when the “Live” page is displayed is audio output off (audio from the microphone cannot be heard on the PC). To hear audio, switch to audio output on using the mic input button.
- When switching audio output to on, be careful of loud volume and configure the output level of the audio output device.

⑨ Main area

Displays images from the camera.

Audio from a specified position can be selected by clicking the desired position in the main area on the “Live” page. (→page 24)

IMPORTANT

- When using a 360° camera installed in the center of the microphone, the microphone directionality that can be configured using camera images according to the type of the camera image is as follows.^{*1}

	Panorama	Quad PTZ	Single PTZ	Fisheye
Freely specify a direction using the image	✓	x	x	✓
Fix to the center of the image ^{*2}	x	✓	✓	x

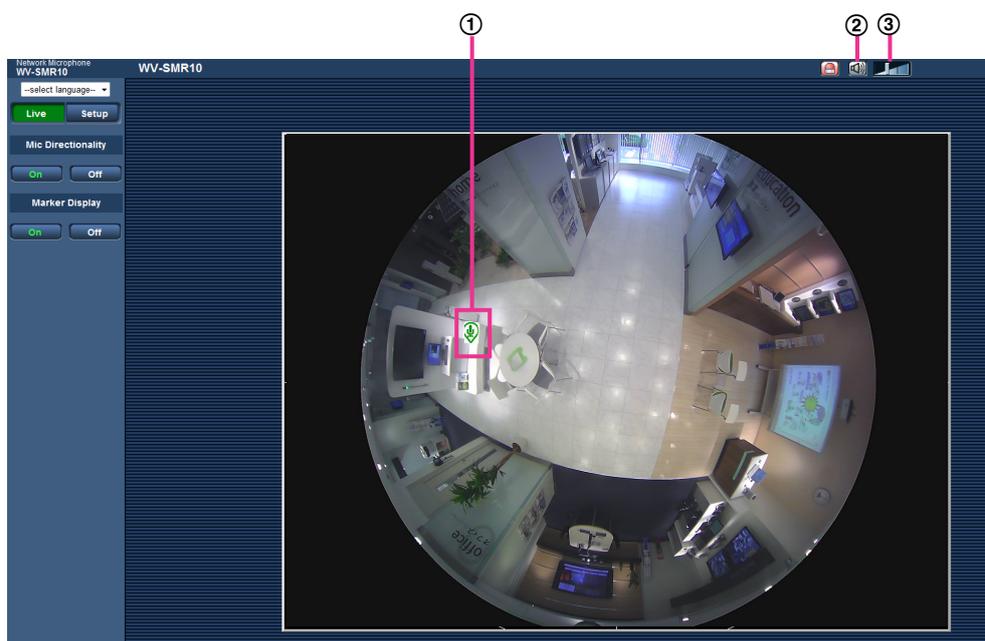
✓ = Operable

x = Inoperable

^{*1} Double panorama and quad stream mode of 360° cameras are not supported.

^{*2} Sound from the central direction of the displayed or selected image can be heard. When moving the direction of the image using panning or tilting operations of the 360° camera, sound from the central direction will not be heard. In that case, update the browser.

1.3 Listen to audio



To listen to audio from a specified position, display the “Live” page and perform the following procedure.

- ① When a desired position is clicked on the screen, the  icon is displayed on the sound collection position. Depending on the transmission image of the camera, audio from the specified position may not be heard. (→ Page 24)
- ② Click the  button to disable mute.
- ③ Adjust the audio volume by using the  icon.

2 Action at a malfunction notification

When an error is detected in the microphone element of the unit, a malfunction notification action will be performed in accordance with settings. When an error is detected in the microphone element, contact your dealer for assistance.

2.1 Action at a malfunction notification

Display the malfunction notification button on the “Live” page

When an error is detected in the microphone element, the malfunction notification button is displayed on the “Live” page. (→page 9)

IMPORTANT

- When “Polling(30s)” is selected for “Alarm status update mode” (→page 20), the malfunction notification button will be refreshed in 30-second intervals. For this reason, it may take a maximum of 30 seconds until the malfunction notification button is displayed on the “Live” page after a malfunction in the microphone element has occurred.

Notify of malfunctions to the designated addresses (Panasonic alarm protocol notification)

This function is available only when a Panasonic device, such as the network disk recorder, is connected to the system. When “On” is selected for “Panasonic alarm protocol”, the connected Panasonic device will be notified that the microphone element of the unit is malfunctioning. The settings for Panasonic alarm protocol can be configured in the “Failure Notif.” page. (→page 26)

3 About the network security

3.1 Equipped security functions

The following security functions are featured in this microphone.

- ① Access restrictions by the host authentication and the user authentication
It is possible to restrict users from accessing the microphone by setting the host authentication and/or the user authentication to "On". (→page 28, page 29)
- ② Access restrictions by changing the HTTP port
It is possible to prevent illegal access such as port scanning, etc. by changing the HTTP port number. (→page 34)
- ③ Access encryption by the HTTPS function
It is possible to enhance the network security by encrypting the access to the microphone using the HTTPS function. (→page 42)

IMPORTANT

- Design and enhance security countermeasures to prevent leakage of information such as audio data, authentication information (user name and password), DDNS server information, etc. Perform the countermeasure such as access restriction (using the user authentication) or access encryption (using the HTTPS function).
- After the microphone is accessed by the administrator, make sure to close the browser for added security.
- Change the administrator password periodically for added security.

Note

- When user authentication (authentication error) has failed 8 times within 30 seconds using the same IP address (PC), access to the microphone will be denied for a while.

4 Display the setup menu from a PC

The settings of the microphone can be configured on the setup menu.

IMPORTANT

- The setup menu is only operable by users whose access level is “1. Administrator”. Refer to page 28 for information on how to configure the access level.

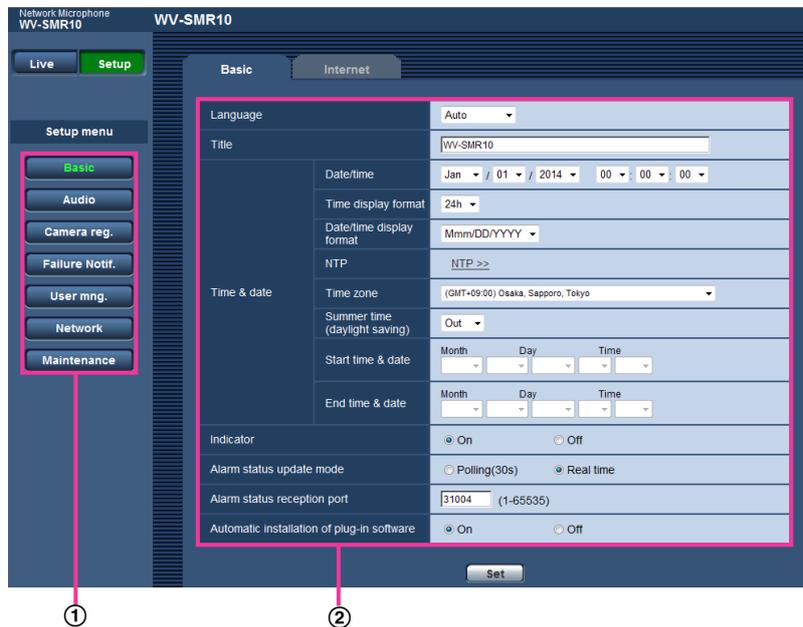
4.1 How to display the setup menu

1. Display the “Live” page. (→page 6)
2. Click the [Setup] button on the “Live” page.
→ The window with the user name and password entry fields will be displayed.



3. Click the [OK] button after entering the user name and the password.
The default user name and password are as follows.
User name: admin
Password: 12345
→ The setup menu will be displayed. Refer to page 16 for further information about this menu.

4.2 How to operate the setup menu



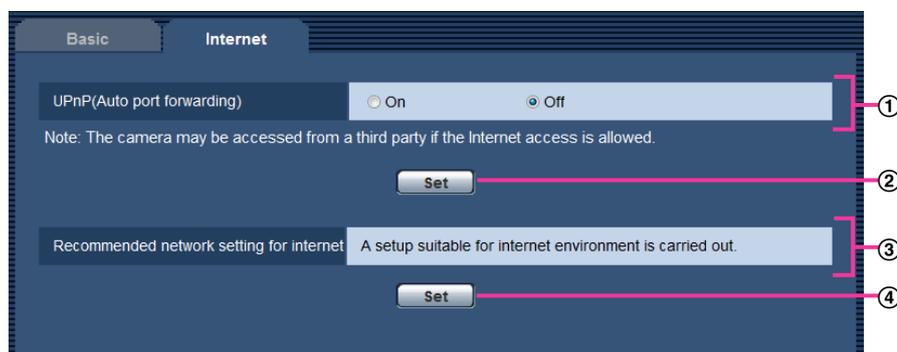
- ① Menu buttons
- ② Setup page

1. Click the desired button in the frame on the left of the window to display the respective setup menu. When there are tabs at the top of the “Setup” page displayed in the frame on the right of the window, click the desired tab to display and configure the setting items relating to the name of the tab.
2. Complete each setting item displayed in the frame on the right of the window.
3. After completing each setting item, click the [Set] button to apply them.

IMPORTANT

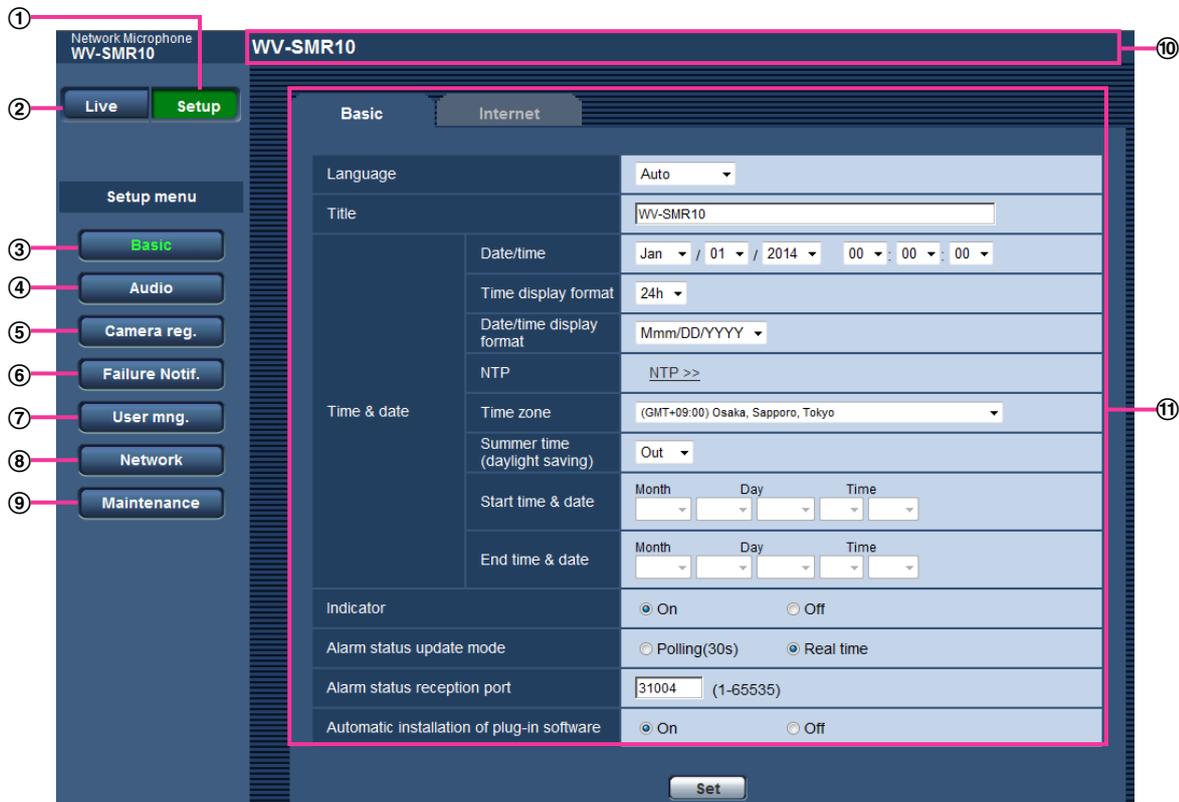
- When there are two or more [Set] and [Execute] buttons on the page, click the button respective to the edited setting item.

<Example>



When completing the setting items in field ①, click the [Set] button ②. The edited settings in field ① will not be applied unless the [Set] button ② below field ① is clicked. In the same manner as above, click the [Set] button ④ when completing the setting items in field ③.

4.3 About the setup menu window



- ① **[Setup] button**
Displays the “Setup” page.
- ② **[Live] button**
Displays the “Live” page.
- ③ **[Basic] button**
Displays the “Basic” page. The basic settings such as time and date and microphone title can be configured on the “Basic” page. (→page 18)
- ④ **[Audio] button**
Displays the “Audio setup” page. The settings relating to microphone sensitivity and audio transmission type can be configured on the “Audio setup” page. (→page 22)
- ⑤ **[Camera reg.] button**
Displays the “Camera reg.” page. The camera images to be displayed on the “Live” page of the unit can be specified on the “Camera reg.” page. (→page 24)
- ⑥ **[Failure Notif.] button**
Displays the “Failure Notif.” page. The settings relating to the notification destination when an error occurs in the microphone element can be configured on the “Failure Notif.” page. (→page 26)
- ⑦ **[User mng.] button**
Displays the “User mng.” page. The settings relating to authentications and restrictions for users and PCs accessing the microphone can be configured on the “User mng.” page. (→page 28)
- ⑧ **[Network] button**
Displays the “Network” page. The network settings and the settings relating to the NTP server, UPnP, HTTPS, DDNS (Dynamic DNS), SNMP (Simple Network Management Protocol), and Diffserv can be configured on the “Network” page. (→page 32)

- ⑨ **[Maintenance] button**
Displays the “Maintenance” page. System log check, firmware upgrade, status check and initialization of the setup menu can be carried out on the “Maintenance” page. (→page 57)
- ⑩ **Microphone title**
The title of the microphone whose settings are currently being configured will be displayed.
- ⑪ **Setup page**
Pages of each setup menu will be displayed. There are tabs for some setup menus.

5 Configure the basic settings of the microphone [Basic]

The basic settings such as microphone title, time and date, and network settings for the Internet can be configured on the “Basic” page. The “Basic” page has the [Basic] tab and the [Internet] tab.

5.1 Configure the basic settings [Basic]

Click the [Basic] tab on the “Basic” page. (→page 14, page 15)

The settings such as the microphone title, time and date, etc. can be configured on this page.

Basic		Internet	
Language	Auto		
Title	WV-SMR10		
Time & date	Date/time	Jan	/ 01 / 2014 00 : 00 : 00
	Time display format	24h	
	Date/time display format	Mmm/DD/YYYY	
	NTP	NTP >>	
	Time zone	(GMT+09:00) Osaka, Sapporo, Tokyo	
	Summer time (daylight saving)	Out	
	Start time & date	Month	Day
End time & date	Month	Day	Time
Indicator	<input checked="" type="radio"/> On <input type="radio"/> Off		
Alarm status update mode	<input type="radio"/> Polling(30s) <input checked="" type="radio"/> Real time		
Alarm status reception port	31004 (1-65535)		
Automatic installation of plug-in software	<input checked="" type="radio"/> On <input type="radio"/> Off		
Set			

[Language]

Select the language to initially display when the microphone is accessed from the following. Auto/English/Japanese/Italian/French/German/Spanish/Chinese/Russian/Portuguese

- **Auto:** The language used by the browser is automatically selected. If the language used by the browser is not supported by the microphone, English is selected.
- **Default:** Auto

The language displayed on the “Live” page can also be changed. (→page 9)

[Title]

Enter the title of the microphone. Click the [Set] button after entering the title of the microphone. The entered title will be displayed in the “Title” field.

- **Available number of characters:** 0 - 20 characters
- **Unavailable characters:** " &
- **Default:** The model No. is displayed.

[Date/time]

Enter the current time and date. When “12h” is selected for “Time display format”, “AM” or “PM” can be selected.

- **Available range:** Jan/01/2013 00:00:00 - Dec/31/2035 23:59:59

IMPORTANT

- Use an NTP server when the more accurate time & date setting is required for the system operation. (→page 35)

[Time display format]

Select the time display format from “24h” or “12h”. Enter the current hour reflecting this setting when entering the current time and date for “Date/time”.

- **Default:** 24h

[Date/time display format]

Select a date/time display format. When “2014/04/01 13:10:00” is set for “Date/time” after selecting “24h” for “Date/time display format”, time & date will be respectively displayed as follows.

- **DD/MM/YYYY:** 01/04/2014 13:10:00
- **MM/DD/YYYY:** 04/01/2014 13:10:00
- **DD/Mmm/YYYY:** 01/Apr/2014 13:10:00
- **YYYY/MM/DD:** 2014/04/01 13:10:00
- **Mmm/DD/YYYY:** Apr/01/2014 13:10:00
- **Default:** Mmm/DD/YYYY

[NTP]

When [NTP >>] is clicked, the [Advanced] tab of the “Network” page will be displayed. (→page 35)

[Time zone]

Select a time zone corresponding to the location where the microphone is in use.

- **Default:** (GMT +09:00) Osaka, Sapporo, Tokyo

[Summer time (daylight saving)]

Select “In”, “Out” or “Auto” to determine whether or not to apply daylight saving time. Configure this setting if the summer time (daylight saving time) is applied in the location where the microphone is in use.

- **In:** Applies summer time. An asterisk (*) will be displayed on the left side of the displayed time and date.
- **Out:** Does not apply summer time.
- **Auto:** Applies summer time in accordance with the settings for “Start time & date” and “End time & date” (month, week, day of the week, and time).
- **Default:** Out

[Start time & date] [End time & date]

When “Auto” is selected for “Summer time (daylight saving)”, select the time & date for the start time and the end time (month, week, day of the week, and time).

[Indicator]

Determine whether or not to use the following indicators. Select “On” to use the following indicators to check the operational status by lighting them. Select “Off” to turn off the indicators at all times.

- Link indicator (LINK)
- Access indicator (ACT)
- **Default:** On

Note

- **Link indicator (LINK) (orange):** This indicator will light when communication with the connected device is available.
- **Access indicator (ACT) (green):** This indicator will blink when accessing a network.

5 Configure the basic settings of the microphone [Basic]

[Alarm status update mode]

Select an interval of the microphone status notification from the following.

When the status of the microphone changes, the malfunction notification button will be displayed to notify of the microphone status.

- **Polling(30s):** Updates the status every 30 seconds and provides notification of the microphone status.
- **Real time:** Provides notification of the microphone status when the status has changed.
- **Default:** Real time

Note

- Depending on the network environment, notification may not be provided in real time.
- When multiple microphones are using the same “Alarm status reception port”, even if “Real time” is selected for “Alarm status update mode”, status notification is not provided in real time. In this case, change the “Alarm status reception port” settings.

[Alarm status reception port]

When selecting “Real time” for “Alarm status update mode”, designate a port number to which the status change notification is to be sent.

- **Available port number:** 1 - 65535
- **Default:** 31004

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[Automatic installation of plug-in software]

Determine whether or not to install the plugin software from this microphone.

- **On:** Installs the plugin software from the microphone automatically.
- **Off:** The plugin software cannot be installed from the microphone.
- **Default:** On

IMPORTANT

- Audio cannot be monitored when the plugin software “Network Microphone Plugin” (ActiveX) is not installed on the PC.

5.2 Configure the Internet settings [Internet]

Click the [Internet] tab of the “Basic” page. (→page 14, page 15)

The settings relating to UPnP (Auto port forwarding) and network settings for the Internet can be configured on this page.



[UPnP (Auto port forwarding)]

Select “On” or “Off” to determine whether or not to use the port forwarding function of the router.

To use the auto port forwarding function, the router in use must support UPnP and the UPnP must be enabled.

- **Default:** Off

Note

- Due to auto port forwarding, the port number may sometimes be changed. When the number is changed, it is necessary to change the port numbers registered in the PC and recorders, etc.
- The UPnP function is available when the microphone is connected to the IPv4 network. IPv6 is not supported.
- To check if auto port forwarding is properly configured, click the [Status] tab on the “Maintenance” page, and check that “Enable” is displayed for “Status” of “UPnP”. (→page 59)
When “Enable” is not displayed, refer to “Cannot access the microphone via the Internet.” in 14 Troubleshooting.
- When the “UPnP (Auto port forwarding)” setting is changed, the “Auto port forwarding” setting under “UPnP” on the [Advanced] tab of the “Network” page also changes to the same setting.

[Recommended network setting for internet]

The recommended settings for connecting to the Internet are performed here.

By clicking the [Set] button, a dialog displaying how the following settings will change is displayed.

Click the [OK] button after checking the settings to change the settings to the displayed values.

- [Audio] tab on the “Audio” page
[Internet mode (over HTTP)]: On

6 Configure the settings relating to audio [Audio]

The settings relating to microphone sensitivity and audio transmission type can be configured on the “Audio setup” page. (→page 14, page 15)

Audio setup	
Microphone sensitivity	3 Default

Transmission setup	
Internet mode (over HTTP)	<input type="radio"/> On <input checked="" type="radio"/> Off
Transmission type	Unicast port (AUTO)
Unicast port	32024 (1024-50000)
Multicast address	239.192.0.20
Multicast port	37004 (1024-50000)
Multicast TTL/HOPLimit	16 (1-254)

[Microphone sensitivity]

Configure the sensitivity of the microphone according to the installation environment.

- **Available microphone sensitivity:** 0 High sensitivity – 5 Low sensitivity
- **Default:** 3 Default

[Internet mode (over HTTP)]

Select “On” when transmitting audio via the Internet.

- **On:** Audio will be transmitted using the HTTP port. Refer to page 34 for further information about the HTTP port number settings.
- **Off:** Audio will be transmitted using the UDP port.
- **Default:** Off

Note

- When “On” is selected, only “Unicast port (AUTO)” will be available for “Transmission type”.
- When “On” is selected, only IPv4 access is available.
- When audio cannot be heard even after increasing the volume on the “Live” page, select a higher sensitivity.
- When the audio heard on the “Live” page is too loud, distorted, or contains noise, select a lower sensitivity.

[Transmission type]

Select the transmission type of audio from the following.

- **Unicast port (AUTO):** Up to 3 users can access a single microphone concurrently. “Unicast port” will automatically be selected when transmitting audio from the microphone. When it is unnecessary to fix the port number for audio transmission such as when using in a particular LAN environment, it is recommended to select “Unicast port (AUTO)”.

- **Unicast port (MANUAL):** Up to 3 users can access a single microphone concurrently. It is necessary to select “Unicast port” manually to transmit audio from the microphone.
It is possible to fix the port number of the router used for audio transmission via the Internet by setting “Unicast port (MANUAL)” (→page 32). Refer to the operating instructions of the router in use.
- **Multicast:** Unlimited number of users can access a single microphone concurrently. Complete the entry field of “Multicast address”, “Multicast port” and “Multicast TTL/HOPLimit” when transmitting audio with multicast. Refer to page 6 for further information about the maximum concurrent access number.
- **Default:** Unicast port (AUTO)

[Unicast port]¹

Enter the unicast port number (used to transmit audio from the microphone).

- **Available port number:** 1024 - 50000 (Only even numbers are available.)
- **Default:** 32024

[Multicast address]²

Enter the multicast IP address. Audio will be transmitted to the designated IP address.

- **Available IPv4 address:** 224.0.0.0 - 239.255.255.255
- **Available IPv6 address:** Multicast address starting with “FF”
- **Default:** 239.192.0.20

Note

- Enter a multicast IP address after checking available multicast addresses.

[Multicast port]²

Enter the multicast port number.

- **Available port number:** 1024 - 50000 (Only even numbers are available.)
- **Default:** 37004

[Multicast TTL/HOPLimit]²

Enter a value for “Multicast TTL/HOPLimit”.

- **Available value:** 1-254
- **Default:** 16

IMPORTANT

- When transmitting audio via a network, the transmitted audio sometimes may not be heard depending on the settings of a proxy server or a firewall. In this case, refer to the network administrator.
- When two or more network interface cards are installed on the PC in use, the network interface card(s) not used for receiving audio should be invalidated when receiving audio using the multicast port.

¹ It is necessary to designate the unicast port number when “Unicast port (MANUAL)” is selected for “Transmission type”.

² It is necessary to designate the multicast IP address when “Multicast” is selected for “Transmission type”.

7 Register a camera for the “Live” page [Camera reg.]

The camera images to be displayed on the “Live” page of the unit can be specified on the “Camera reg.” page. (→page 14, page 15)

Camera registration setting		Delete
Camera image format	<input checked="" type="radio"/> JPEG <input type="radio"/> H.264	Stream ▼
IP address	Example of entry: http://192.168.0.10	
Port number	80 (1-65535)	

Set

[Camera image format]

Select from JPEG or H.264 for the camera image to be displayed. When H.264 is selected, select the stream number using “Stream”.

[IP address]

Enter the IP address of the camera to be registered.

Note

- Specify the IPv4 address of the camera.
- When the setting on the camera side is an HTTPS connection, enter the IP address in the “https://IP address” format.
- When only the IP address is configured, the camera is accessed via HTTPS or HTTP and the camera image is displayed depending on the connection setting (→page 48).

[Port number]

Enter the connection port number of the camera to be registered.

[Set] button

Register the setting details on this page.

[Delete] button

Delete the currently displayed registration.

Note

- The unit supports the following Panasonic 360° camera images.
 - Fisheye images
 - Panorama images
 - Quad PTZ images
 - Single PTZ images
- When an unsupported camera or image is specified, sound that has directionality cannot be heard. Check the following.
 - The registered camera is a 360° camera
 - The image of the 360° camera is a fisheye, panorama, quad PTZ, or single PTZ image

- The registered 360° camera is updated to the latest firmware (→page 10)
Refer to our website (<http://security.panasonic.com/pss/security/support/info.html>) for further information about the firmware of supported 360° cameras.
- The image capture size when “JPEG” is selected for “Camera image format” is as follows.
 - 1280 x 960 (fisheye, quad PTZ, or single PTZ image)
 - 1920 x 1080 (panorama image)However, when the image capture mode selected for the camera does not support the image capture sizes above, the images displayed may be zoomed in and blurry.

8 Configure the malfunction notification settings [Failure Notif.]

The settings relating to the notification destination when an error occurs in the microphone element can be configured on the “Failure Notif.” page. (→page 14, page 15)

Panasonic alarm protocol notification	
Panasonic alarm protocol	<input type="radio"/> On <input checked="" type="radio"/> Off
Destination port	1818 (1-65535)
Retry times	2

Destination of notification	Destination server address
Address 1	<input type="text"/> <input type="button" value="Delete"/>
Address 2	<input type="text"/> <input type="button" value="Delete"/>
Address 3	<input type="text"/> <input type="button" value="Delete"/>
Address 4	<input type="text"/> <input type="button" value="Delete"/>

Panasonic alarm protocol notification

[Panasonic alarm protocol]

Select “On” or “Off” to determine whether or not to provide notification by Panasonic alarm protocol when an error occurs in the microphone element.

- **Default:** Off

Note

- When “On” is selected, notification of the alarm occurrence will be provided to the registered destination server addresses in order (to IP address 1 first, to IP address 4 last).

[Destination port]

Select a destination port for the Panasonic alarm protocol from the following.

- **Available range:** 1 - 65535
- **Default:** 1818

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 995, 10669, 10670

[Retry times]

Select a retry time for the Panasonic alarm protocol.

- **Available range:** 0-30
- **Default:** 2

Destination of notification

[Address 1] - [Address 4]

Enter the destination IP address or host name of the Panasonic alarm protocol. Up to 4 destination server addresses can be registered.

To delete the registered destination server address, click the [Delete] button respective to the desired destination server address.

IMPORTANT

- When entering the host name of the “Destination server address”, the DNS settings on the [Network] tab of the “Network” page must be configured. (→page 32)
- Confirm that the destination IP addresses are registered correctly. When a registered destination does not exist, notifications may be delayed or not be received.

9 Configure the settings relating to the authentication [User mng.]

The settings relating to authentications and restrictions for users and PCs accessing the microphone with a PC can be configured on the “User mng.” page.

The “User mng.” page has 3 tabs; the [User auth.] tab, the [Host auth.] tab, and the [System] tab.

9.1 Configure the settings relating to the user authentication [User auth.]

Click the [User auth.] tab on the “User mng.” page. (→page 14, page 15)

The settings relating to the authentication of users who can access this microphone from the PC can be configured on this page. Up to 24 users can be registered.

Note

- When user authentication has failed (authentication error) 8 times within 30 seconds using the same IP address (PC), access to the microphone will be denied for a while.

The screenshot shows the 'User auth.' configuration page. At the top, there are three tabs: 'User auth.', 'Host auth.', and 'System'. The 'User auth.' tab is selected. Below the tabs, there are several configuration sections. The first section has 'User auth.' with two radio buttons: 'On' and 'Off', with 'Off' selected. Below this is the 'Authentication' section with a dropdown menu showing 'Digest or Basic'. A 'Set' button is located below the dropdown. The second section contains three text input fields: 'User name', 'Password', and 'Retype password'. The third section has 'Access level' with two radio buttons: '1. Administrator' and '2. Live only', with '2. Live only' selected. A 'Set' button is below this section. The final section is 'User check' with a dropdown menu showing 'admin[1]' and a 'Delete' button.

[User auth.]

Select “On” or “Off” to determine whether or not to authenticate the users.

- **Default:** Off

[Authentication]

Set the user authentication method.

Digest or Basic: Uses Digest or Basic authentication.

Digest: Uses Digest authentication.

Basic: Uses Basic authentication.

- **Default:** Digest or Basic

Note

- When the [Authentication] setting has been changed, close the web browser, and then access the microphone again.
- For other devices such as network disk recorders, unless otherwise stated, Digest authentication is not supported. (As of August, 2014)
- Digest authentication is the safer authentication method when compared to Basic authentication. When using the microphone via the Internet, operation under Digest authentication is recommended.

[User name]

Enter a user name.

- **Available number of characters:** 1 - 32 characters
- **Unavailable characters:** " & ; ; \
- **Default:** None (blank)

[Password] [Retype password]

Enter a password.

- **Available number of characters:** 4 - 32 characters
- **Unavailable characters:** " &
- **Default:** None (blank)

Note

- When the user name already in use is entered and the [Set] button is clicked, the respective user information will be overwritten.

[Access level]

Select the access level of the user from the following.

- **1. Administrator:** Allowed all available operations of the microphone.
- **2. Live only:** Display of live images and "Live" page functions are available.
- **Default:** 2. Live only

[User check]

From the pull-down menu of "User check", the registered user can be selected and the selected user's information can be checked.

The registered user will be displayed with the access level.

(Example: admin [1])

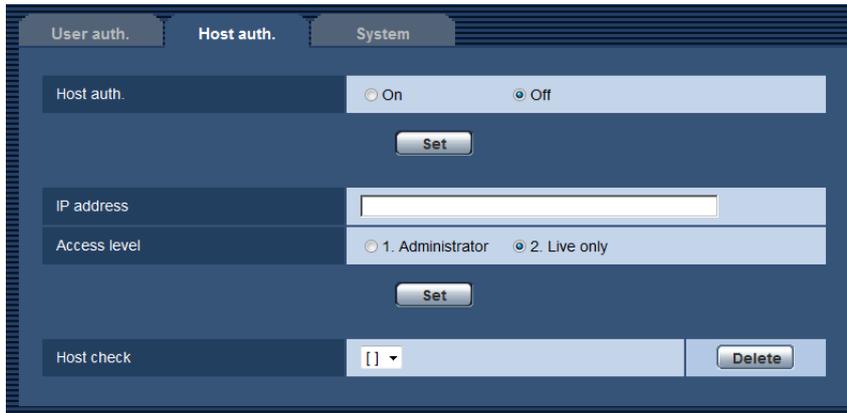
To delete the registered user, click the [Delete] button after selecting the user to be deleted.

9.2 Configure the settings relating to the host authentication [Host auth.]

Click the [Host auth.] tab on the "User mng." page. (→page 14, page 15)

9 Configure the settings relating to the authentication [User mng.]

The restriction settings of PCs (IP address) from accessing the microphone can be configured on this page.



[Host auth.]

Select “On” or “Off” to determine whether or not to authenticate the host.

- **Default:** Off

[IP address]

Enter the IP address of the PC to be allowed to access the microphone. Host name cannot be entered for the IP address.

Note

- When “IP address/subnet mask” is entered, it is possible to restrict PCs in each subnet. For example, when “192.168.0.1/24” is entered and “2. Live only” is selected for the access level, the PCs whose IP address is between “192.168.0.1” - “192.168.0.254” can access the microphone with the access level “2. Live only”.
- When the IP address already in use is entered and the [Set] button is clicked, the respective host information will be overwritten.

[Access level]

Select the access level of the host from the following.

1. Administrator/ 2. Live only

Refer to page 28 for further information about the access level.

- **Default:** 2. Live only

[Host check]

From the pull-down menu of “Host check”, the registered host can be selected and the selected host’s IP address can be checked.

The registered IP address will be displayed with the access level.

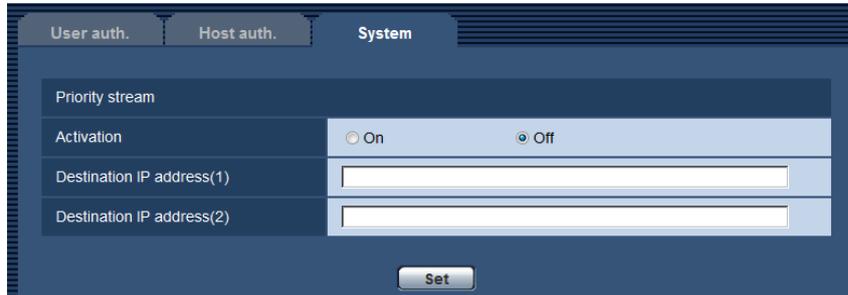
(Example: 192.168.0.21 [1])

To delete the registered host, click the [Delete] button after selecting the IP address to be deleted.

9.3 Configure the settings relating to the priority stream [System]

Click the [System] tab on the “User mng.” page. (→page 14, page 15)

Priority stream destinations (IP addresses) can be configured here.



The screenshot shows a web interface with three tabs: 'User auth.', 'Host auth.', and 'System'. The 'System' tab is active. Under the 'Priority stream' section, there are three rows: 'Activation' with radio buttons for 'On' and 'Off' (where 'Off' is selected), 'Destination IP address(1)' with an empty text input field, and 'Destination IP address(2)' with an empty text input field. A 'Set' button is located at the bottom of the form.

Priority stream

[Activation]

Select "On" or "Off" to determine whether or not to use the priority stream.

- **Default:** Off

[Destination IP address(1)]

Enter the first destination IP address.

[Destination IP address(2)]

Enter the second destination IP address.

Note

- When "On" is selected for "Activation" of "Priority stream", the number of users who can access the microphone may be limited.
- If multiple connections are performed from the IP address entered in the destination IP address, only Stream 1 is prioritized.

10 Configuring the network settings [Network]

The network settings can be configured on the “Network” page.
The “Network” page has the [Network] tab, and the [Advanced] tab.

10.1 Configure the network settings [Network]

Click the [Network] tab on the “Network” page. (→page 14, page 15)
The following information is required to configure the network settings. Contact the network administrator or your Internet service provider.

- IP address
- Subnet mask
- Default gateway (when using the gateway server/router)
- HTTP port
- Primary DNS address, Secondary DNS address (when using DNS)

Network	
Advanced	
IPv4 network	
Network Settings	Auto(Advanced) ▾
IP address(IPv4)	192 . 168 . 0 . 10
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 0 . 1
DNS	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Primary server address	0 . 0 . 0 . 0
Secondary server address	0 . 0 . 0 . 0
IPv6 network	
Manual	<input type="radio"/> On <input checked="" type="radio"/> Off
IP address(IPv6)	
Default gateway	
DHCPv6	<input type="radio"/> On <input checked="" type="radio"/> Off
Primary DNS server address	
Secondary DNS server address	
Common	
HTTP port	80 (1-65535)
Line speed	Auto ▾
Easy IP Setup accommodate period	<input checked="" type="radio"/> 20min <input type="radio"/> Unlimited
<input type="button" value="Set"/>	

IPv4 network

[Network Settings]

Select the method of how to configure the IP address from the following.

- **Static:** The IP address is configured by entering manually on “IP address(IPv4)”.
- **DHCP:** The IP address is configured using the DHCP function.
- **Auto(AutoIP):** The IP address is configured using the DHCP function. When the DHCP server is not found, the IP address is automatically configured.
- **Auto(Advanced):** Using the DHCP function, network address information is referred to, and an unused IP address is configured to the microphone as a static IP address. The configured IP address is automatically determined within the subnet mask range by the microphone. When the DHCP server is not found, the IP address is set to 192.168.0.10.
- **Default:** Auto(Advanced)

Note

- When “Auto(AutoIP)” is selected and the IP address cannot be obtained from the DHCP server, an IP address not used in the same network will be searched within 169.254.1.0 - 169.254.254.255.

[IP address(IPv4)]

When not using the DHCP function, enter the IP address of the microphone. Do not enter an IP address already in use (for the PCs and the other network cameras).

- **Default:** 192.168.0.10

Note

- Multiple IP addresses are unavailable even when using the DHCP function. Refer to the network administrator for further information about the settings of the DHCP server.

[Subnet mask]

When not using the DHCP function, enter the subnet mask of the microphone.

- **Default:** 255.255.255.0

[Default gateway]

When not using the DHCP function, enter the default gateway of the microphone.

- **Default:** 192.168.0.1

Note

- Multiple IP addresses for the default gateway are unavailable even when using the DHCP function. Refer to the network administrator for further information about the settings of the DHCP server.

[DNS]

Determine how to set the address of the DNS server by selecting “Auto” (obtain the address automatically) or “Manual” (enter the address of the DNS server). When “Manual” is selected, it is necessary to configure the settings for the DNS.

When using the DHCP function, it is possible to obtain the DNS address automatically by selecting “Auto”. Refer to the network administrator for further information about the settings.

- **Default:** Auto

[Primary server address], [Secondary server address]

When “Manual” is selected for “DNS”, enter the IP address of the DNS server. Refer to the network administrator about the IP address of the DNS server.

IPv6 network**[Manual]**

Select “On” or “Off” to determine whether or not to manually configure the IP address for IPv6 network (IPv6 address).

- **On:** Enter an IPv6 address manually.

10 Configuring the network settings [Network]

- **Off:** Manual entry of an IPv6 address will become unavailable.
- **Default:** Off

[IP address(IPv6)]

When “On” is selected for “Manual”, manual entry of the IPv6 address is required. Do not enter an address already in use.

Note

- When connecting to the manually configured IPv6 address beyond the router, use an IPv6 compatible router and turn on the automatic IPv6 address assignment function. In this case, it is necessary to configure an IPv6 address including prefix information provided from the IPv6 compatible router. Refer to the manuals provided with the router for further information.

[Default gateway]

When “On” is selected for “Manual” of IPv6 network, enter the default gateway of IPv6 network of the microphone.

- **Default:** None (blank)

[DHCPv6]

Select “On” or “Off” to determine whether or not to use the IPv6 DHCP function.

Configure the DHCP server not to assign the same IP addresses used for the other network cameras and PCs whose IP addresses are unique. Refer to the network administrator for further information about the settings of the server.

- **Default:** Off

[Primary DNS server address], [Secondary DNS server address]

Enter the IPv6 address of the DNS server. Refer to the network administrator about the IPv6 address of the DNS server.

Common

[HTTP port]

Assign the port numbers independently.

- **Available port number:** 1 - 65535
- **Default:** 80

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 110, 123, 161, 162, 443, 554, 995, 10669, 10670, 59000 - 61000

[Line speed]

Select the line speed for data transmission from the following. It is recommended to use with the default “Auto”.

- **Auto:** Line speed will be applied automatically.
- **100M-Full:** 100 Mbps full-duplex
- **100M-Half:** 100 Mbps half-duplex
- **10M-Full:** 10 Mbps full-duplex
- **10M-Half:** 10 Mbps half-duplex
- **Default:** Auto

[Easy IP Setup accommodate period]

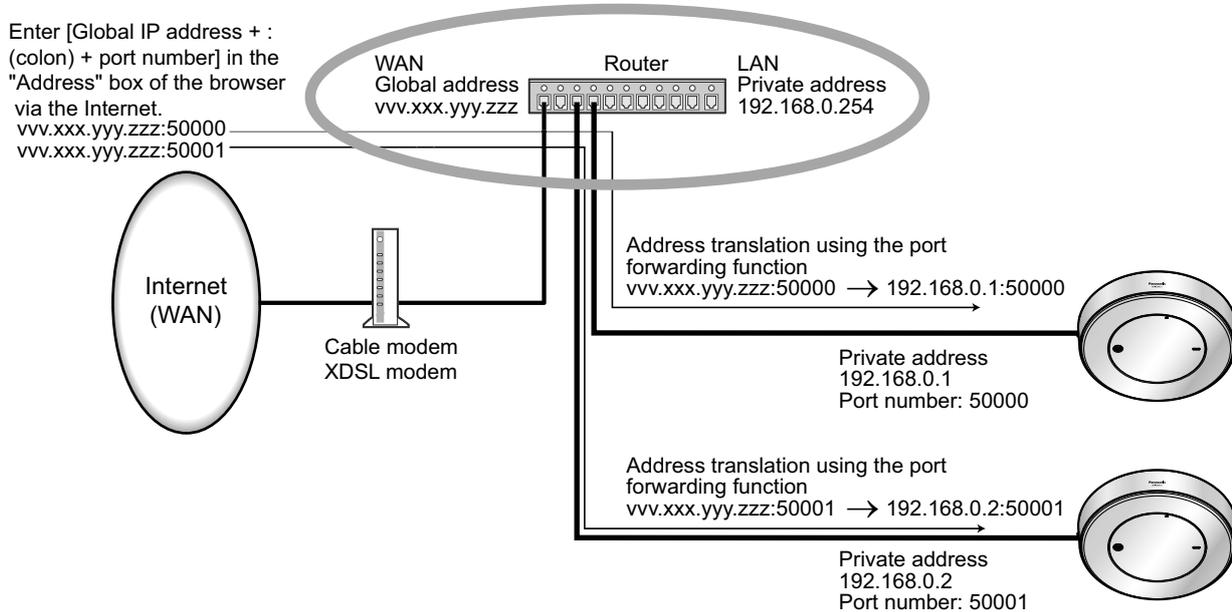
Select “20min” or “Unlimited” to determine how long the network setting operation using the Panasonic “IP Setting Software” can be allowed.

- **20min:** The network setting operation using the Panasonic “IP Setting Software” are allowed for 20 minutes since the microphone starts up.

- **Unlimited:** The network setting operation using the Panasonic “IP Setting Software” are allowed without time limitation.
- **Default:** 20min

Note

- The list display of camera related devices using the Panasonic “IP Setting Software” is allowed without time limitation, and live images of the unit can be opened using the [Open the device window] button.
- Refer to the network administrator for the addresses of each server.
- The port forwarding function changes a global IP address to a private IP address, and “Static IP masquerade” and “Network Address Translation (NAT)” have this function. This function is to be set in a router.
- To access the microphone via the Internet by connecting the microphone to a router, it is necessary to assign a respective HTTP port number for each microphone and address translation by using the port forwarding function of the router. For further information, refer to the operating instructions of the router in use.



10.2 Configure advanced network settings [Advanced]

Click the [Advanced] tab on the “Network” page. (→page 14, page 15)

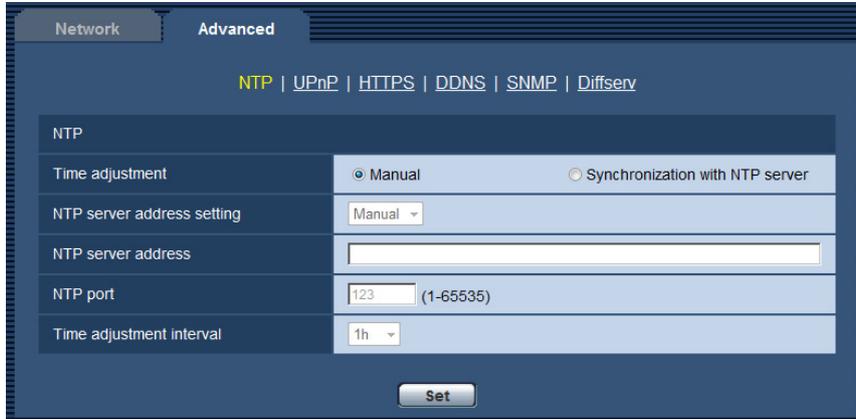
The settings related to NTP, UPnP, HTTPS, DDNS, SNMP, and Diffserv can be configured in this section. You can move to the setting page of a setting item by clicking the corresponding link for that setting item.

10.2.1 Configure the settings relating to the NTP server

The settings relating to the NTP server such as the NTP server address, port number, etc. can be configured on this page.

IMPORTANT

- Use an NTP server when the more accurate time & date setting is required for the system operation.



[Time adjustment]

Select the time adjustment method from the following. Time adjusted by the selected method will be used as the standard time of the microphone.

- **Manual:** Time set on the [Basic] tab on the “Basic” page will be used as the standard time of the microphone.
- **Synchronization with NTP server:** Time automatically adjusted by synchronizing with the NTP server will be used as the standard time of the microphone.
- **Default:** Manual

[NTP server address setting]

When “Synchronization with NTP server” is selected for “Time adjustment”, select the method of how to obtain the NTP server address from the following.

- **Auto:** Obtains the NTP server address from the DHCP server.
- **Manual:** The NTP server address will be entered manually on “NTP server address”.
- **Default:** Manual

IMPORTANT

- When obtaining the NTP server address from the DHCP server, it is necessary to select “DHCP”, “Auto(AutoIP)”, or “Auto(Advanced)” for “Network Settings” on the [Network] tab of the “Network” page. (→page 32)

[NTP server address]

When “Manual” is selected for “NTP server address setting”, enter the IP address or the host name of the NTP server.

- **Available number of characters:** 1 - 128 characters
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

IMPORTANT

- When entering the host name for “NTP server address”, it is necessary to configure the DNS settings on the [Network] tab of the “Network” page. (→page 32)

[NTP port]

Enter a port number of the NTP server.

- **Available port number:** 1 - 65535
- **Default:** 123

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 161, 162, 443, 995, 10669, 10670

[Time adjustment interval]

Select an interval (1 - 24 hours: in 1 hour intervals) of synchronization with the NTP server.

- **Default:** 1h

10.2.2 Configure the UPnP settings

This microphone supports UPnP (Universal Plug and Play). By using the UPnP function, it becomes possible to configure the following automatically.

- Configuration of the port forwarding function of the router. (However, a router supporting UPnP is required.) This configuration is useful when accessing the microphone via the Internet.
- Automatic refreshment of the shortcut to the microphone that is created on the [Network] folder of the PC even when the IP address of the microphone changes.



[Auto port forwarding]

Select “On” or “Off” to determine whether or not to use the port forwarding function of the router.

To use the port forwarding function, the router in use must support UPnP and the UPnP must be enabled.

- **Default:** Off

Note

- Due to port forwarding, the port number may sometimes be changed. When the number is changed, it is necessary to change the port numbers registered in the PC and recorders, etc.
- The UPnP function is available when the microphone is connected to the IPv4 network. IPv6 is not supported.
- To check if auto port forwarding is properly configured, click the [Status] tab on the “Maintenance” page, and check that “Enable” is displayed for “Status” of “UPnP”. (→page 59)
When “Enable” is not displayed, refer to “Cannot access the microphone via the Internet.” in the “14 Troubleshooting” section. (→page 70)

[Short-cut to the microphone]

Select whether or not to create the shortcut to the microphone on the [Network] folder of the PC. When creating the shortcut, select “On”.

To use the Short-cut to the microphone function, enable the UPnP function on the PC in advance.

- **Default:** Off

Note

- To display the shortcut to the microphone on the [Network] folder of the PC, it is necessary to add the Windows component. Refer to the following to enable the UPnP function.

For Windows Vista

[Start] → [Control Panel] → [Network and Internet] → [Network and Sharing Center] → expand the section of [Network discovery] of [Sharing and Discovery] → select [Turn on network discovery] → click [Apply] → Complete

For Windows 7

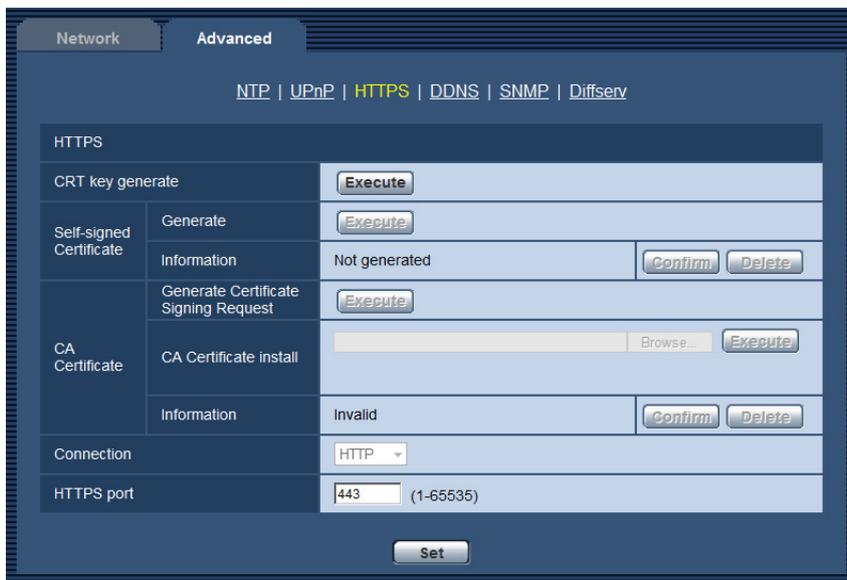
[Start] → [Control Panel] → [Network and Internet] → [Network and Sharing Center] → select [Turn on network discovery] of [Network discovery] of [Change advanced sharing settings] → click [Save changes] → Complete

For Windows 8.1 and Windows 8

[Start] → select [Apps] → [Control Panel] → [Network and Internet] → [Network and Sharing Center] → select [Turn on network discovery] of [Network discovery] of [Change advanced sharing settings] → click [Save changes] → Complete

10.2.3 Configure the HTTPS settings

It is possible to enhance the network security by encrypting the access to microphones using the HTTPS function. Refer to page 42 for information on how to configure the HTTPS settings.



[CRT key generate]

CRT key (SSL encryption key) used for the HTTPS protocol is generated. To generate the CRT key, click the [Execute] button to display the "CRT key generate" dialog box.

[Self-signed Certificate - Generate]

The microphone itself generates the security certificate used for the HTTPS protocol (self-signed certificate). To generate the self-signed certificate, click the [Execute] button to display the "Self-signed Certificate - Generate" dialog box.

[Self-signed Certificate - Information]

Displays the information of the self-signed certificate.

When the [Confirm] button is clicked, the registered information of the self-signed certificate will be displayed in the "Self-signed Certificate - Confirm" dialog box.

When the [Delete] button is clicked, the generated self-signed certificate will be deleted.

[CA Certificate - Generate Certificate Signing Request]

When using the security certificate issued by CA (Certificate Authority) as the security certificate used for the HTTPS protocol, the CSR (Certificate Signing Request) will be generated.

To generate the CSR, click the [Execute] button to display the “CA Certificate - Generate Certificate Signing Request” dialog window.

[CA Certificate - CA Certificate install]

Installs the server certificate (security certificate) issued by CA (Certificate Authority) and displays the information of the installed server certificate.

To install the server certificate, click the [Browse...] button to display the [Open] dialog box, and select the file of the server certificate issued by CA, and click the [Execute] button.

If the server certificate is already installed, the file name of the installed server certificate will be displayed.

[CA Certificate - Information]

Displays the information of the server certificate.

When the [Confirm] button is clicked, the registered information of the installed server certificate will be displayed in the “CA Certificate - Confirm” dialog box. If the server certificate is not installed, the content of the generated CSR file will be displayed.

When the [Delete] button is clicked, the installed server certificate will be deleted.

IMPORTANT

- Before deleting the valid server certificate (security certificate), confirm that there is a backup file on the PC or another media. The backup file will be required when installing the server certificate again.

[Connection]

Select the protocol used to connect the microphone.

- **HTTP:** Only the HTTP connection is available.
- **HTTPS:** Only the HTTPS connection is available.
- **Default:** HTTP

[HTTPS port]

Designate the HTTPS port number to be used.

- **Available port number:** 1 - 65535
- **Default:** 443

The following port numbers are unavailable since they are already in use.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 554, 995, 10669, 10670, 59000-61000

Note

- After the connection setting is changed, wait for a while and then access the microphone again.
- **When using the self-signed certificate:**
If the microphone is accessed using the HTTPS protocol for the first time, the warning window will be displayed. In this case, follow the instructions of the wizard to install the self-signed (security) certificate. (→page 49)
- **When using the server certificate:**
In advance, install the root certificate and intermediate certificate on the browser in use. Follow the instructions of CA for information on how to obtain and install these certificates.

10.2.4 Configure the settings relating to DDNS

To access this microphone via the Internet, it is necessary to configure the settings for the DDNS function.

10 Configuring the network settings [Network]

Refer to page 55 for information on how to configure the settings relating to DDNS.



[Service]

Select the DDNS service to determine whether or not to use DDNS.

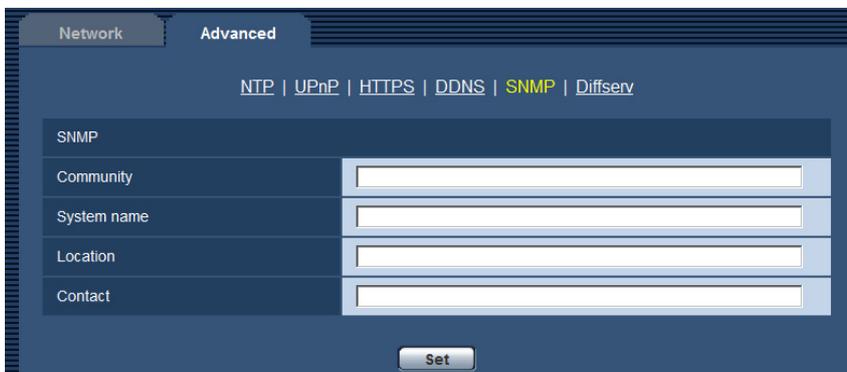
- **Off:** Does not use the DDNS function.
- **Dynamic DNS Update:** Uses Dynamic DNS Update (RFC2136 compliant) without the DHCP cooperation.
- **Dynamic DNS Update(DHCP):** Uses Dynamic DNS Update (RFC2136 compliant) with the DHCP cooperation.
- **Default:** Off

Note

- When using Dynamic DNS Update (RFC2136 compliant), refer to the network administrator for whether or not to cooperate with the DHCP.

10.2.5 Configure the settings relating to SNMP

The settings relating to SNMP can be configured on this page. It is possible to check the status of the microphone by connecting to the SNMP manager. When using the SNMP function, contact the network administrator.



[Community]

Enter the community name to be monitored.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

IMPORTANT

- When using the SNMP function, it is necessary to enter the community name. When no community name is entered, the SNMP function will not work.

[System name]

Enter a system name to be used to manage the microphone with the SNMP function.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

[Location]

Enter the name of the location where the microphone is installed.

- **Available number of characters:** 0 - 32 characters
- **Default:** None (blank)

[Contact]

Enter the E-mail address or the phone number of the SNMP manager.

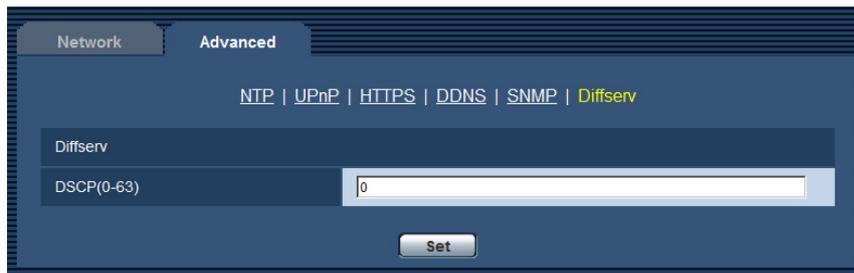
- **Available number of characters:** 0 - 255 characters
- **Default:** None (blank)

10.2.6 Configure the Diffserv settings

The settings relating to Diffserv can be configured on this page. The Diffserv function can be used to set the priority of image/audio data sent from routers.

The priority set to this function must match the DSCP value configured to the router.

When using the Diffserv function, contact the network administrator.



The screenshot shows a web-based configuration interface. At the top, there are two tabs: 'Network' and 'Advanced'. Below the tabs, there is a navigation menu with links for 'NTP', 'UPnP', 'HTTPS', 'DDNS', 'SNMP', and 'Diffserv'. The 'Diffserv' link is highlighted. Below the navigation menu, there is a section titled 'Diffserv'. Under this section, there is a label 'DSCP(0-63)' followed by a text input field containing the value '0'. At the bottom of the section, there is a 'Set' button.

[DSCP(0-63)]

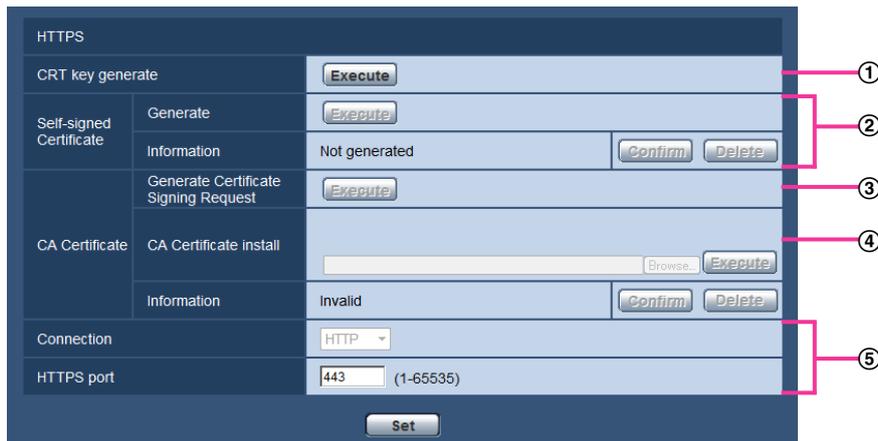
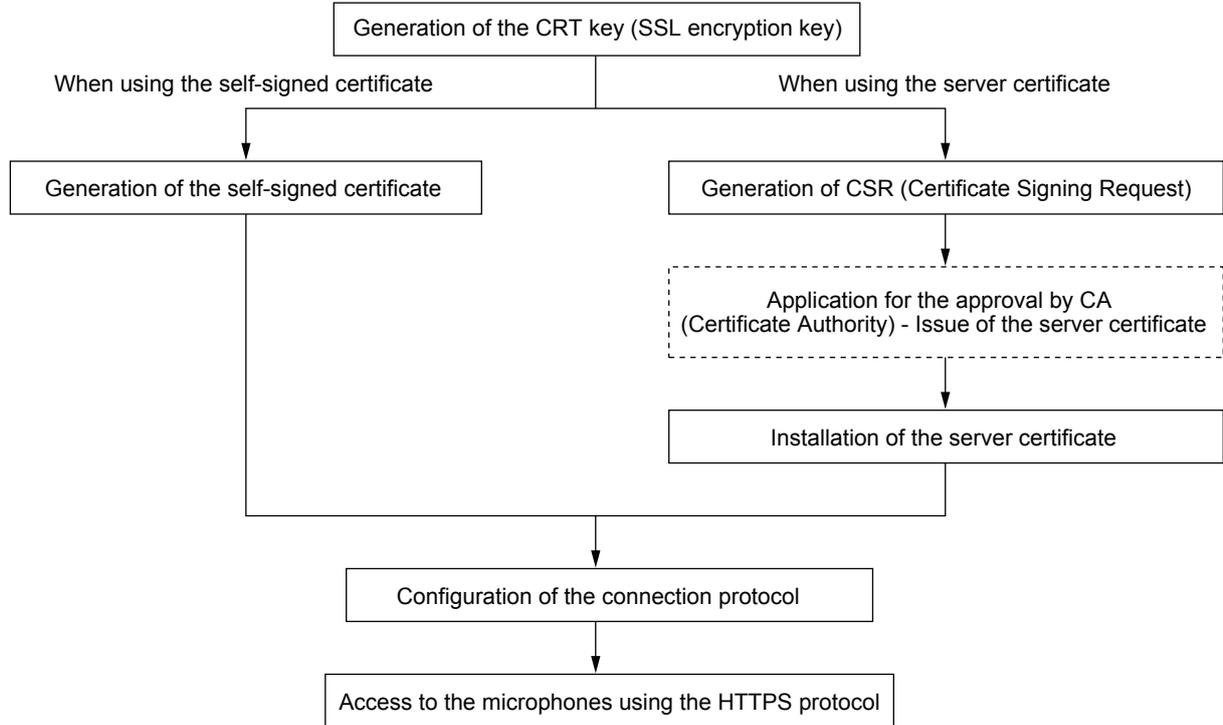
Enter the order of priority for packets.

- **Available values:** 0 - 63
- **Default:** 0

10.3 How to configure HTTPS settings

The settings relating to the HTTPS protocol that can enhance the network security by encrypting the access to microphones on this page.

The HTTPS settings will be configured in the following procedure.



- ① Generation of the CRT key (SSL encryption key) (→page 43)
- ② Generation of the self-signed certificate (→page 44)
- ③ Generation of CSR (Certificate Signing Request) (→page 46)
- ④ Installation of the server certificate (→page 47)
- ⑤ Configuration of the connection protocol (→page 48)

Note

- To use the server certificate, you need to apply for the approval and the issue of the server certificate by CA.
- Either the self-signed certificate or the server certificate will be used. If both of them are installed, the server certificate will take priority over the self-signed certificate.

10.3.1 Generation of the CRT key (SSL encryption key)

IMPORTANT

- When the self-signed certificate or server certificate is valid, it is impossible to generate the CRT key.
- When server certification is used, the available key size varies depending on the CA. Confirm the available key size in advance.
- To generate the CRT key, it may take about 1 minute when the key size is 1024 bit and about 2 minutes when the key size is 2048 bit. Do not operate the web browser until the generation of the CRT key is complete. While the CRT key is being generated, the refresh interval and line speed may be lower.

1. Click the [Execute] button of “CRT key generate”.
→ The “CRT key generate” dialog box will be displayed.

Current CRT key		
CRT key	RSA key size	
	Last modified	Not generated
History		
CRT key generate		
RSA key size	<input checked="" type="radio"/> 1024bit <input type="radio"/> 2048bit	Execute
*Generating a CRT key takes about 2 minutes.		Close

2. Select “1024bit” or “2048bit” for the length of the CRT to generate for “CRT key generate” - “RSA key size”.

Note

- To use the server certificate, follow the requests from the CA about the RSA key size.

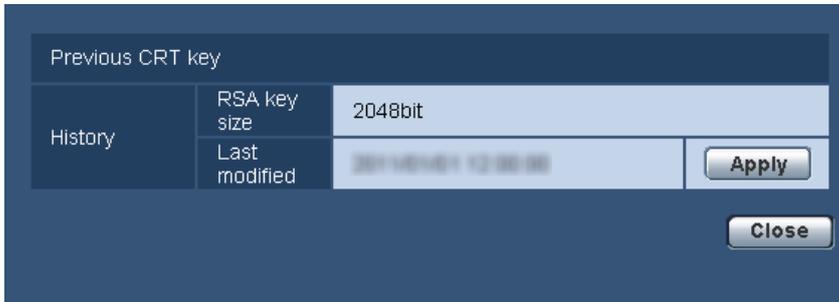
3. Click the [Execute] button.

→ The generation of the CRT key will be started. When the generation is finished, the key size and generation time & date of the generated key will be displayed on “Current CRT key”.

Note

- To change (or update) the generated CRT key, perform step 1 to 3. The CRT key, self-signed certificate and server certification are validated in a set together. When the CRT key is changed, it is necessary to re-generate the self-signed certificate or re-apply for the server certificate.
- When the CRT key is updated, the log of the previous CRT key is saved. When the [History] button of “Current CRT key” on the “CRT key generate” dialog box is clicked, the “Previous CRT key” dialog box will be displayed, and it is possible to check the key size and generation time & date of the previous

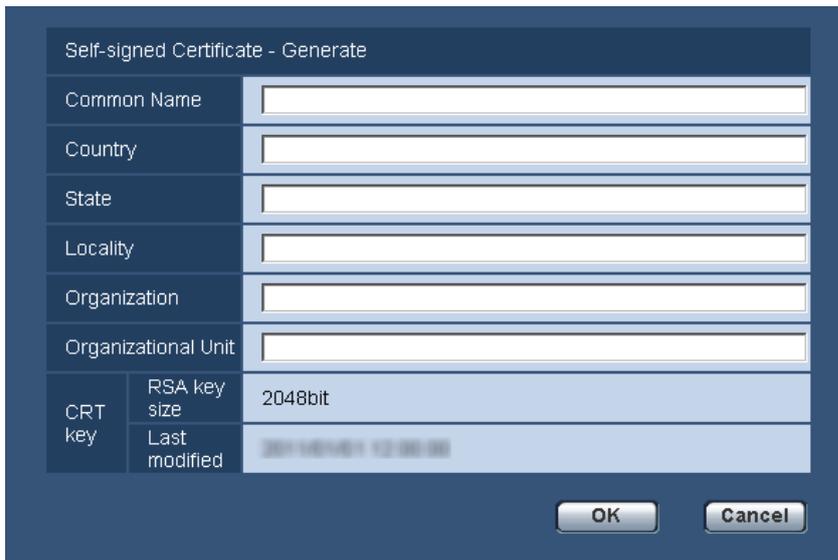
key. When the [Apply] button is clicked on the “Previous CRT key” dialog box, it is possible to replace the current CRT key with the previous one.



10.3.2 Generation of the self-signed certificate (security certificate)

IMPORTANT

- If the CRT key is not generated, it is impossible to generate the self-signed certificate.
1. Click the [Execute] button of “Self-signed Certificate - Generate”.
→ The “Self-signed Certificate - Generate” dialog box will be displayed.



2. Enter the information of the certificate to be generated.

Item	Description	Available number of characters
[Common Name]	Enter the microphone address or host name.	64 characters
[Country]	Enter the country name. (Omission is OK.)	2 characters (Country code)
[State]	Enter the state name. (Omission is OK.)	128 characters
[Locality]	Enter the locality name. (Omission is OK.)	128 characters
[Organization]	Enter the organization name. (Omission is OK.)	64 characters

Item	Description	Available number of characters
[Organizational Unit]	Enter the unit name of the organization. (Omission is OK.)	64 characters
[CRT key]	Displays the key size and generation time & date of the current key.	

Note

- The available characters for [Common Name], [State], [Locality], [Organization], and [Organizational Unit] are 0-9, A-Z, a-z and the following marks.
- . _ , + / ()
- When the microphone is connected to the Internet, enter the address name or host name to access via the Internet for “Common Name”. In this case, the security alert window will be displayed each time the microphone is locally accessed, even if the security certificate is installed.
- When entering the IPv6 address for “Common Name”, put the address in brackets [].
Example: [2001:db8::10]

- Click the [OK] button after entering the items.
→ The self-signed certificate will be generated.

Note

- The information of the generated self-signed certificate will be displayed on “Self-signed Certificate” - “Information”.
Depending on the status of the self-signed certificate, the following are displayed.

Indication	Description
Not generated	The self-signed certificate is not generated.
Invalid (Reason: CA Certificate installed)	The self-signed certificate has already been generated, and the server certificate has been installed. <ul style="list-style-type: none"> In this case, the server certificate is validated.
Common name of the self-signed certificate	The self-signed certificate has already been generated and validated.

- When the [Confirm] button is clicked, the registered information of the self-signed certificate (security certificate) will be displayed in the “Self-signed Certificate - Confirm” dialog box.

Self-signed Certificate - Confirm

Common Name		
Country		
State		
Locality		
Organization		
Organizational Unit		
CRT key	RSA key size	2048bit
	Last modified	2011/04/01 12:00:00

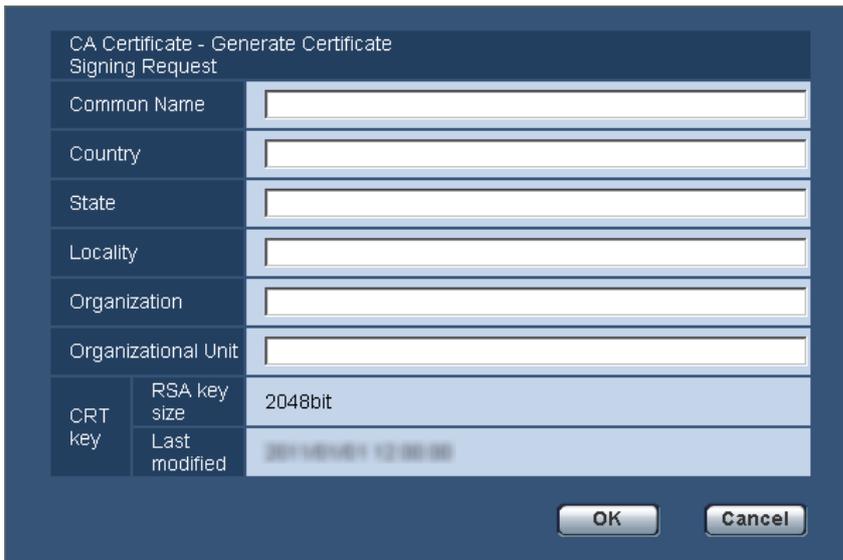
Close

- When the [Delete] button is clicked, the generated self-signed certificate (security certificate) will be deleted.
- When “HTTPS” is selected for “Connection”, it is impossible to delete the self-signed certificate.

10.3.3 Generation of CSR (Certificate Signing Request)

IMPORTANT

- If the CRT key is not generated, it is impossible to generate the CSR.
 - Before generating the CSR file, configure the following settings on [Internet Options] of the web browser in advance. Click [Internet Options...] under [Tools] of the menu bar of Internet Explorer, and then click the [Security] tab.
 - Register the microphone for [Trusted Sites].
 - Click the [Custom level...] button to open the [Security Settings] window, and check the [Enable] radio button of [File Download] under [Downloads].
 - Click the [Custom level...] button to open the [Security Settings] window, and check the [Enable] radio button of [Automatic prompting for file downloads] under [Downloads].
1. Click the [Execute] button of “CA Certificate - Generate Certificate Signing Request”.
 → The “CA Certificate - Generate Certificate Signing Request” dialog box will be displayed.



2. Enter the information of the certificate to be generated.

Item	Description	Available number of characters
[Common Name]	Enter the microphone address or host name.	64 characters
[Country]	Enter the country name.	2 characters (Country code)
[State]	Enter the state name.	128 characters
[Locality]	Enter the locality name.	128 characters
[Organization]	Enter the organization name.	64 characters
[Organizational Unit]	Enter the unit name of the organization.	64 characters

Item	Description	Available number of characters
[CRT key]	Displays the key size and generation time & date of the current key.	

Note

- To use the server certificate, follow the requests from the CA about the information to be entered.
 - The available characters for [Common Name], [State], [Locality], [Organization], and [Organizational Unit] are 0-9, A-Z, a-z and the following marks.
- . _ , + / ()
- Click the [OK] button after entering the items.
→ The [Save As] dialog box will be displayed.
 - Enter a file name for the CSR in the [Save As] dialog box to save on the PC.
→ The saved CSR file will be applied to the CA.

IMPORTANT

- The server certificate will be issued for the set of the generated CSR and CRT key. If the CRT key is re-generated or updated after applying to the CA, the issued server certificate will be invalidated.

Note

- This microphone generates the CSR file in the PEM format.

10.3.4 Installation of the server certificate

IMPORTANT

- If the CSR file is not generated, it is impossible to install the server certificate (security certificate).
 - For the installation, the server certificate issued by CA is required.
- Click the [Browse...] button of "CA Certificate - CA Certificate install".
→ The [Open] dialog box will be displayed.
 - Select the server certification file and click the [Open] button. Then, click the [Execute] button.
→ The server certification will be installed.

Note

- The host name registered in the installed server certificate will be displayed on "CA Certificate - Information". Depending on the status of the server certificate, the following are displayed.

Indication	Description
Invalid	The server certification is not installed.
Common name of the server certificate	The server certificate has already been installed and validated.
Expired	The server certification has already expired.

10 Configuring the network settings [Network]

- When the [Confirm] button is clicked, the registered information of the installed server certificate will be displayed in the “CA Certificate - Confirm” dialog box. (Only “Organizational Unit” will be displayed with an asterisk (*).)



- When the [Delete] button is clicked, the installed server certificate will be deleted.
- When “HTTPS” is selected for “Connection”, it is impossible to delete the server certificate.
- To change (or update) the server certificate, perform step 1 and 2.

IMPORTANT

- Before deleting the valid server certificate (security certificate), confirm that there is a backup file on the PC or another media. The backup file will be required when installing the server certificate again.
- When the server certificate has expired, the HTTPS function will become unavailable. When the microphone is restarted, the connection protocol will be changed to HTTP. Update the server certificate before it expires.
- The expiration date of the server certificate can be checked by double-clicking the server certification file issued by CA.

10.3.5 Configuration of the connection protocol

1. Select “HTTP” or “HTTPS” for “Connection” to determine the protocol used to access the microphone.
 - **HTTP:** Only the HTTP connection is available.
 - **HTTPS:** Only the HTTPS connection is available.
2. Designate the HTTPS port number to be used for “HTTPS port”.
 - **Available port number:** 1 - 65535
 - **Default:** 443

The following port numbers are unavailable since they are already in use.
20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 554, 995, 10669, 10670, 59000 - 61000
3. Click the [Set] button.
 - The microphone will restart, and it will become possible to access to the microphones using the HTTPS protocol. (→page 6)

Note

- After the connection setting is changed, wait for a while and then access the microphone again.
- **When using the self-signed certificate:**
If the microphone is accessed using the HTTPS protocol for the first time, the warning window will be displayed. In this case, follow the instructions of the wizard to install the self-signed (security) certificate. (→page 49)

- **When using the server certificate:**
In advance, install the root certificate and intermediate certificate on the browser in use. Follow the instructions of CA for information on how to obtain and install these certificates.

10.4 Access the microphone using the HTTPS protocol

1. Start up the web browser.
2. Enter the IP address of the microphone in the address box of the browser.
 - **Example of entry:** https://192.168.0.10/

IMPORTANT

- When the HTTPS port number is changed from “443”, enter “https://IP address of the microphone + : (colon) + port number” in the address box of the browser.
(**Example:** https://192.168.0.11:61443)
 - When the microphone is in a local network, configure the proxy server setting of the web browser (under [Internet Options...] under [Tools] of the menu bar) to bypass the proxy server for the local address.
3. Press the [Enter] key on the keyboard.
 - The “Live” page will be displayed.
When the security alert window is displayed, install the security certificate. (→page 50)
When “On” is selected for “User auth.”, the authentication window will be displayed before displaying live images for the user name and password entries.

IMPORTANT

- When the microphone is accessed using the HTTPS protocol, the refresh interval and frame rate of images may be lower.
- When using the HTTPS protocol, up to 2 users can access the microphone and receive audio data concurrently.

10.4.1 Install the security certificate

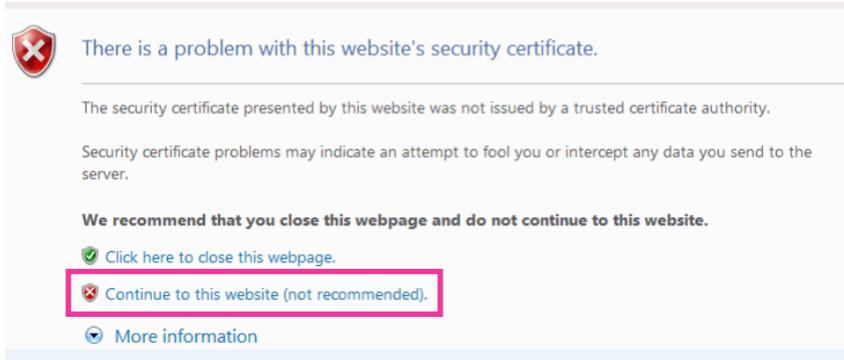
When the security certificate of the microphone to access is not installed on the PC, the security alert window will be displayed each time the microphone is accessed using the HTTPS protocol. To have the security alert window not displayed, it is necessary to install the security certificate in the following procedure. If the certificate is not installed, the alert window will be displayed each time the microphone is accessed.

Note

- The security certificate is installed on the PC with the information registered for “Common Name”. Therefore, the information registered for “Common Name” must be same as the address or host name for the microphone access. If the certificate is not the same, the security alert window will be displayed each time the microphone is accessed.
- When the address or host name of the microphone is changed, the security alert window will be displayed each time the microphone is accessed even if the security certificate is installed. Install the security certificate again.
- When the microphone access is open to the Internet, enter the address name or host name to access via the Internet for “Common Name”. In this case, the security alert window will be displayed each time the microphone is locally accessed, even if the security certificate is installed.

10 Configuring the network settings [Network]

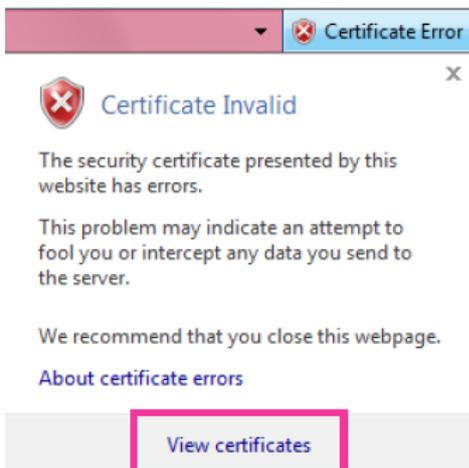
- When the security certificate is properly installed, a key icon is displayed in the address box of the web browser that has accessed the microphone.
 - When using Internet Explorer 10 or Internet Explorer 11, note that some of the displayed windows may differ from the following descriptions.
1. Access the microphone using the HTTPS protocol.
 2. When the security alert window is displayed, click “Continue to this website (not recommended).”



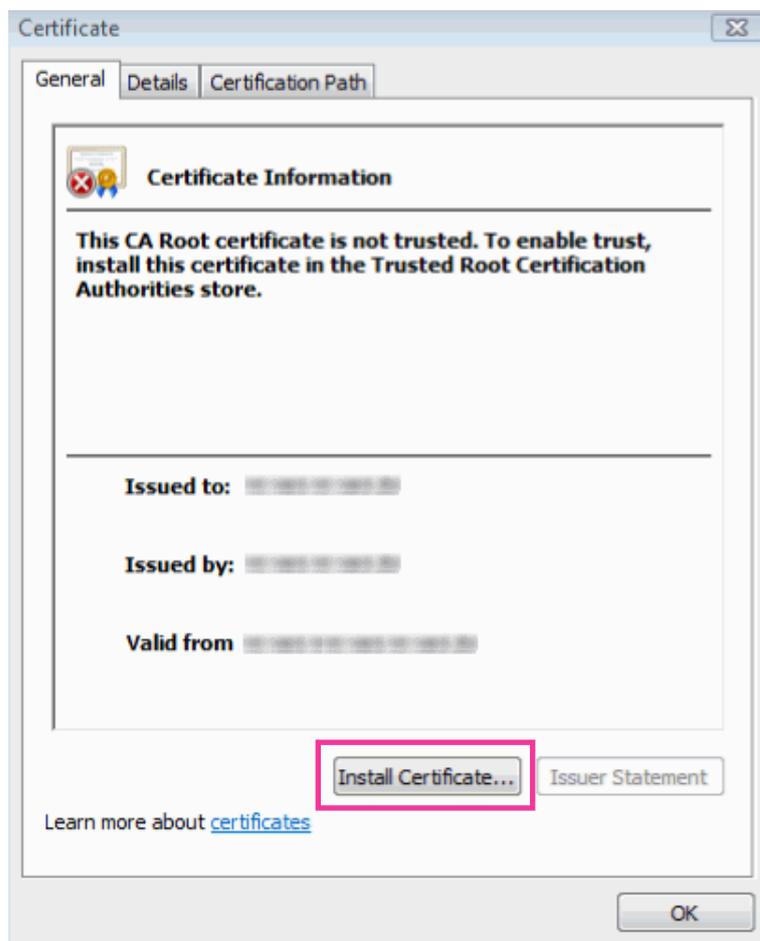
→ The “Live” page will be displayed. If an authentication window is displayed, enter the user name and password.

Note

- If this window is displayed when accessing a device other than the microphone or a website, a security problem may have occurred. In this case, check the system status.
3. Click “Certificate Error” over the URL, and click “View certificates”.

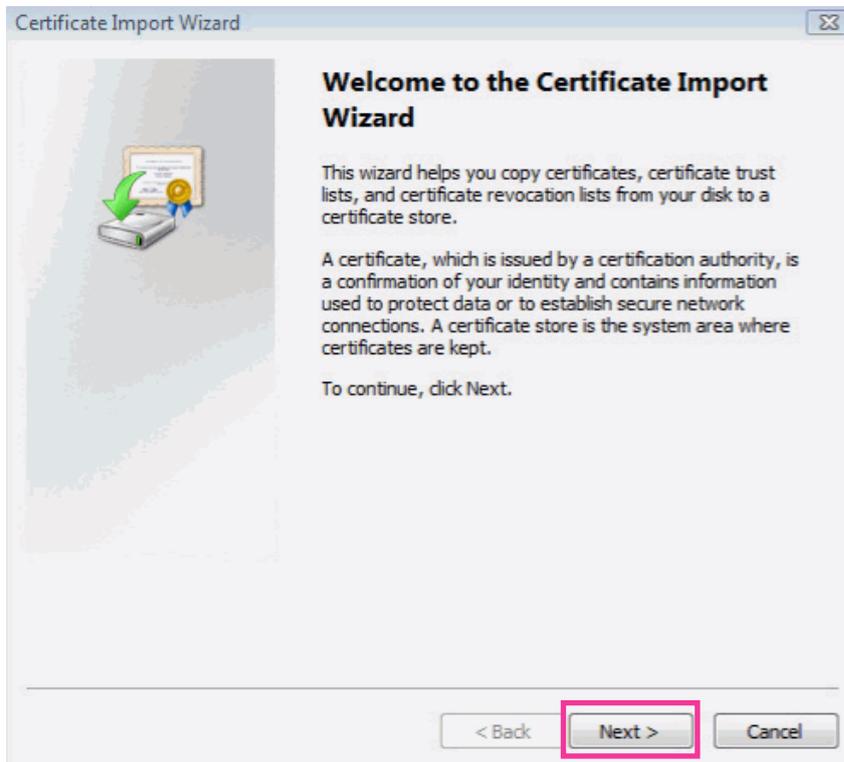


4. Click “Install Certificate...”.

**Note**

- If [Install Certificate...] is not displayed, close Internet Explorer once, and select [Run as Administrator] to launch Internet Explorer again. Click [Start] → [All Programs] → right click [Internet Explorer] → click [Run as Administrator].
- When using Windows 8.1 or Windows 8, right click [iexplore] under “C:\Program Files\Internet Explorer” and select [Run as Administrator].

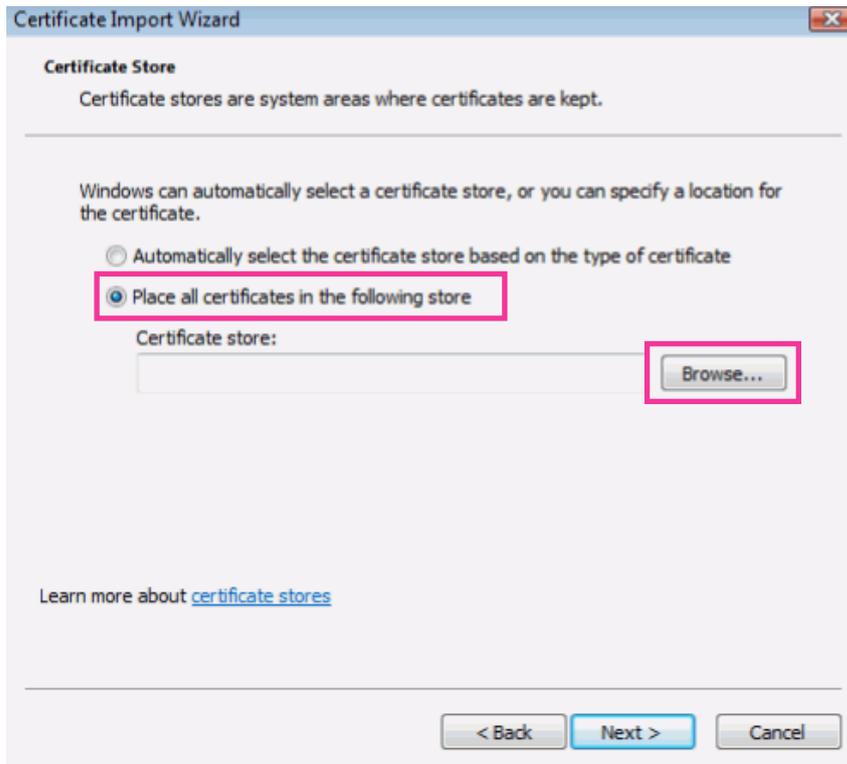
5. Click “Next” displayed on “Certificate Import Wizard”.



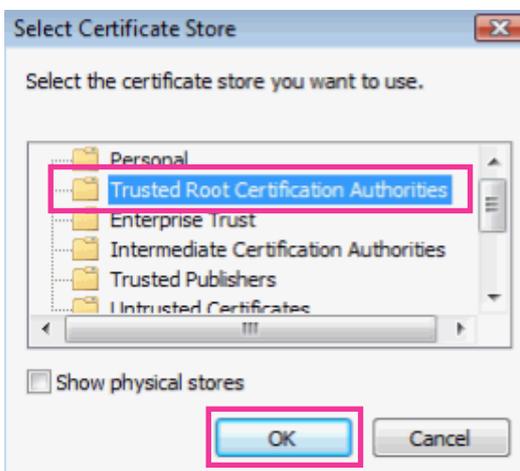
Note

- When using Internet Explorer 10 or Internet Explorer 11, select “Store Location”, and then click “Next”.

6. Select “Place all certificates in the following store”, and click “Browse...”.

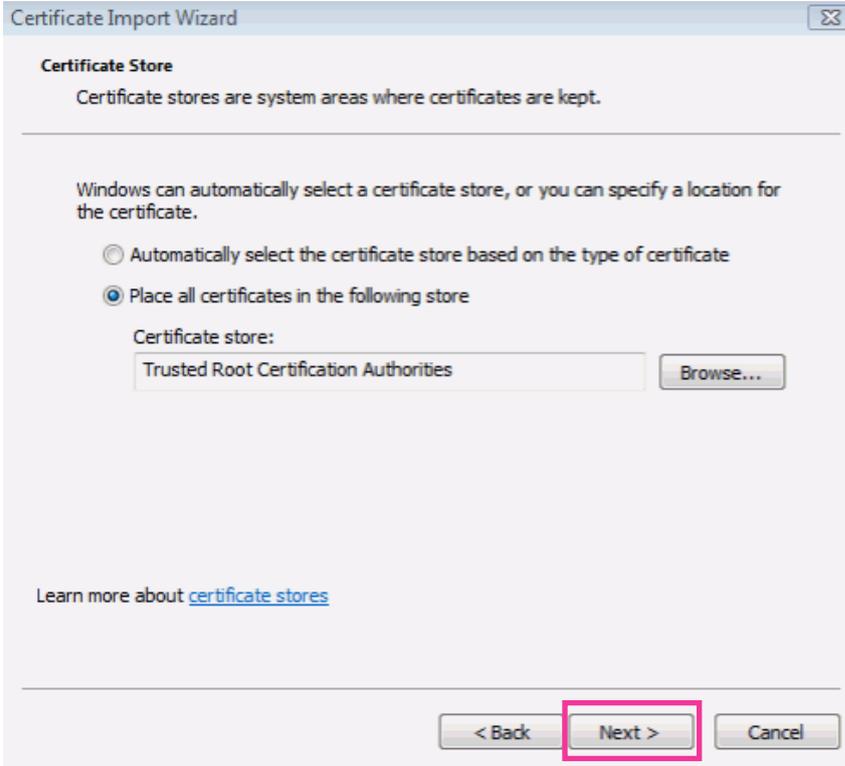


7. Select “Trusted Root Certificate Authorities”, and click “OK”.

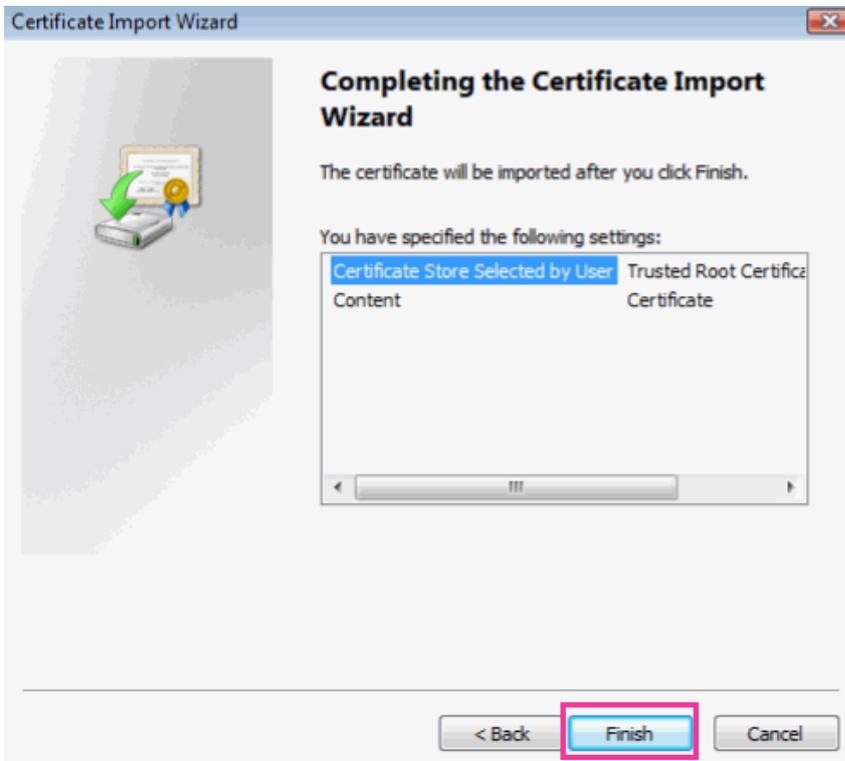


10 Configuring the network settings [Network]

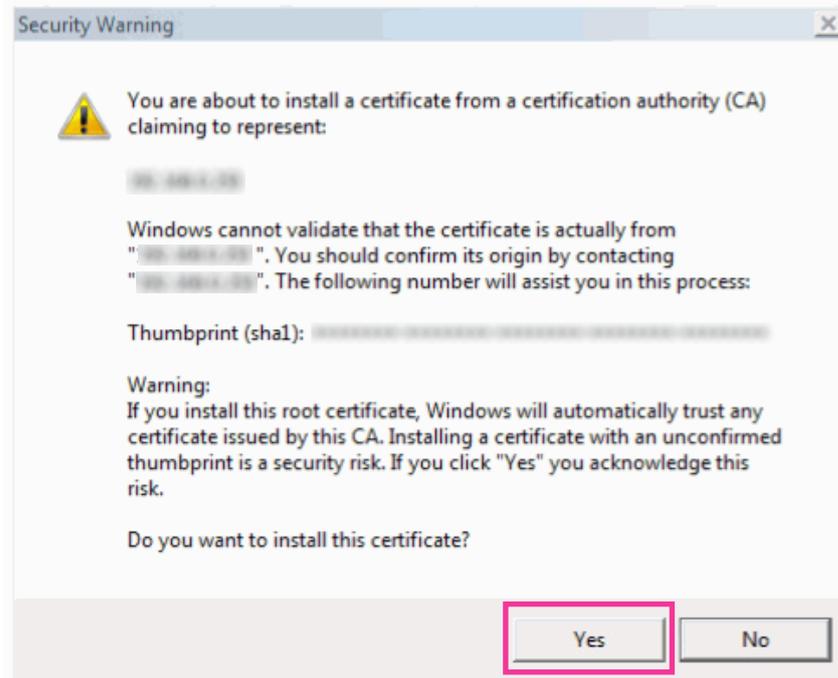
8. Click "Next".



9. Click "Finish".



10. Click “Yes”.



→ When the import is successfully completed, the screen “The import was successful.” will be displayed.

11. Click “OK”.



→ When the browser is restarted after the certificate is imported, “Certificate Error” will not be displayed.

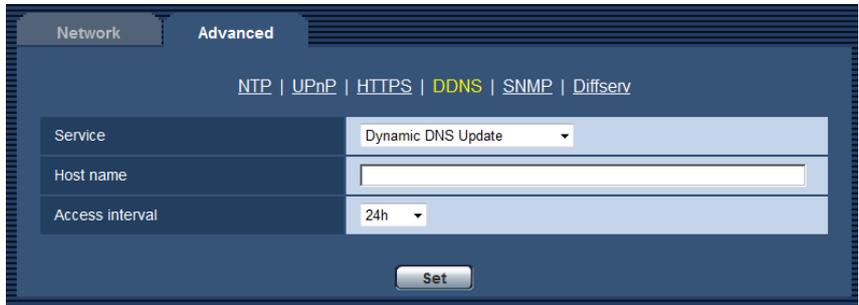
10.5 How to configure the settings relating to DDNS

By using the DDNS function, the microphone can be accessed at all times through the designated domain name, even in an environment where the IP address changes dynamically. The DDNS function associates dynamic IP addresses and domain names. When activating the DDNS function using the microphone, the Dynamic DNS Update (RFC2136 compliant) service is available.

IMPORTANT

- **About Dynamic DNS Update (RFC2136 compliant)**
Operation using DDNS services is not guaranteed. We are not responsible for any troubles or accidents on the circumstances where the unit is used arising out of such services. Refer to the DDNS service providers for the selection and configuration of the DDNS services.

10.5.1 When using “Dynamic DNS Update”



[Host name]

Enter the host name to be used for the Dynamic DNS Update service.

- **Available number of characters:** 3 - 250 characters
Enter in the form of “(host name). (domain name)”.
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

Note

- Refer to the network administrator for further information about the available host names.

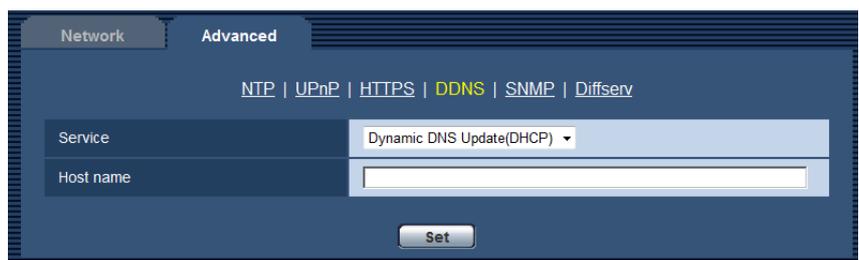
[Access interval]

Select the interval to access the Dynamic DNS Update service server to check the IP address and the host name from the following.

10min/ 20min/ 30min/ 40min/ 50min/ 1h/ 6h/ 24h

- **Default:** 24h

10.5.2 When using “Dynamic DNS Update(DHCP)”



[Host name]

Enter the host name to be used for the Dynamic DNS Update service.

- **Available number of characters:** 3 - 250 characters
Enter in the form of “(host name). (domain name)”.
- **Available characters:** Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).
- **Default:** None (blank)

Note

- Refer to the network administrator for further information about the available host names.

11 Maintenance of the microphone [Maintenance]

System log check, firmware upgrade, status check and initialization of the setup menu can be performed on this page.

The “Maintenance” page has the [System log] tab, the [Upgrade] tab, [Status] tab, the [Default reset] tab, and the [Data] tab.

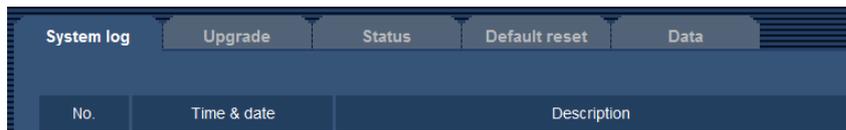
11.1 Check the system log [System log]

Click the [System log] tab of the “Maintenance” page. (→page 14, page 15)

Up to 100 system logs can be saved on the built-in memory of the microphone.

When the saved system logs have reached the maximum number, the newer logs will overwrite the older system logs. In this case, the oldest log is the first to be overwritten.

The logs will be saved even when the power of the microphone is turned off.



No.	Time & date	Description
-----	-------------	-------------

[No.]

The serial number of the system log will be displayed.

[Time & date]

Time and date at the error occurrence will be displayed.

Note

- When “Off” is selected for “Time display format” on the [Basic] tab (→page 18), time & date of logs will be displayed in 24-hour format.

[Description]

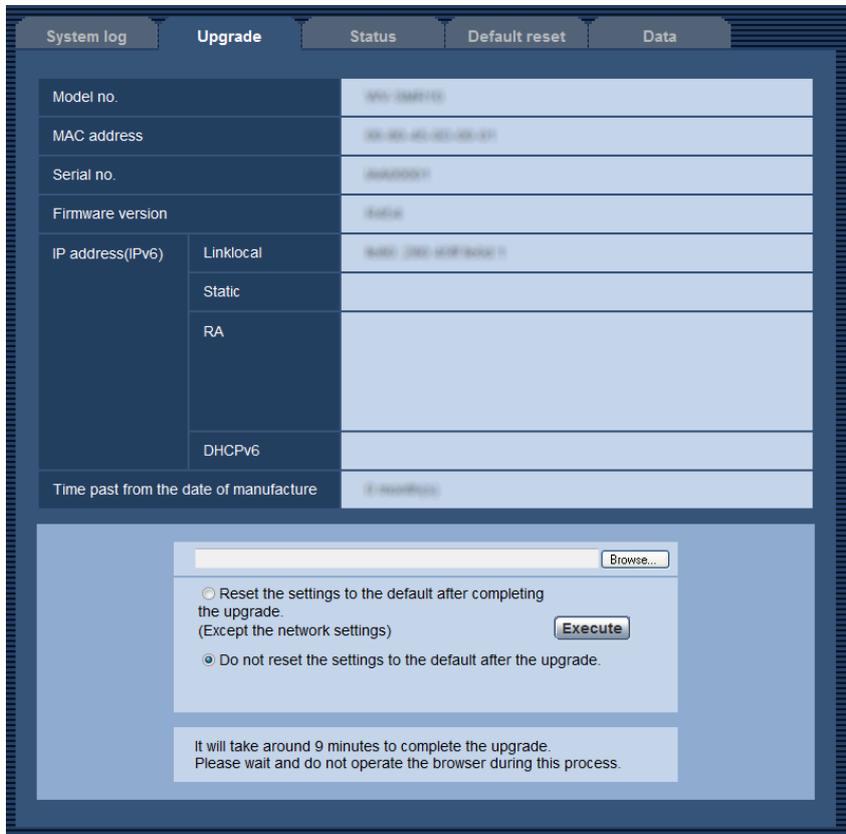
The descriptions about the system log will be displayed. Refer to page 68 for further information about the system logs.

11.2 Upgrade the firmware [Upgrade]

Click the [Upgrade] tab of the “Maintenance” page. (→page 14, page 15)

11 Maintenance of the microphone [Maintenance]

The current firmware can be checked and upgraded to the latest version on this page. Contact the dealer for further information about the firmware upgrade.



[Model no.], [MAC address], [Serial no.], [Firmware version], [IP address(IPv6)], [Time past from the date of manufacture]

Information of each item will be displayed.

1. Contact the dealer and download the latest firmware onto a PC.

IMPORTANT

- A blank (space) cannot be used for the name of the directory where the downloaded firmware to be saved.

2. Click the [Browse...] button and designate the downloaded firmware.
3. Click the radio button respective to the desired option to determine whether or not to initialize the settings after completing the firmware upgrade.

Note

- Note that the settings cannot be restored after an initialization is operated.

4. Click the [Execute] button.
→ The confirmation window will be displayed.

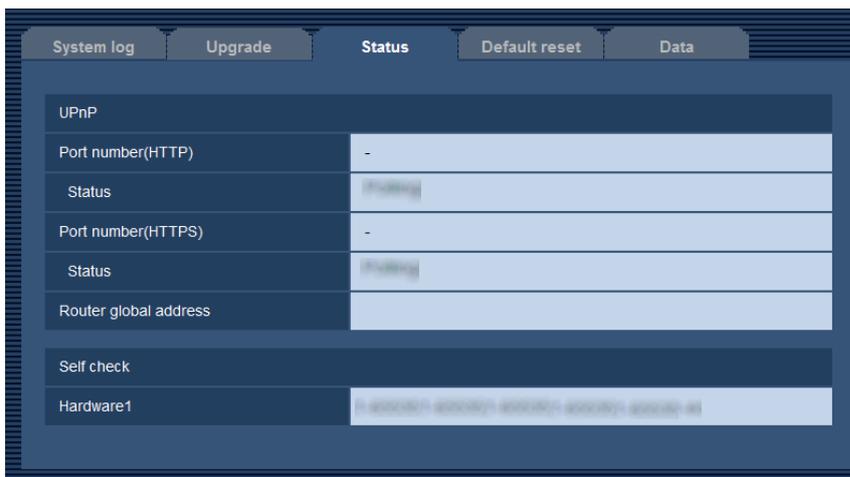
IMPORTANT

- After completing the upgrade, delete temporary Internet files. (→page 70)
- Upgrade the firmware using a PC in the same subnet as the microphone.
- Follow the instructions from the dealer when upgrading the firmware.

- When upgrading the application software, use the designated file (extension: img) for the firmware upgrade.
The name of the firmware to be used for the upgrade should be “model name (Use small letters. “WV-” is not required.)_xxxxx.img”.
* (“xxxxx” indicates the version of the firmware.)
- Do not turn off the power of the microphone during the upgrade process.
- Do not perform any operation during upgrading and wait until it completes.
- The following network settings will not be reset when upgrading the firmware after selecting “Reset the settings to the default after completing the upgrade. (Except the network settings)”.
Primary server address and secondary server address DNS settings for IPv4, primary DNS server address and secondary DNS server address settings for IPv6, On/Off for DHCP, IP address, subnet mask, default gateway, HTTP port, HTTPS port, connection protocol (HTTP/HTTPS), CRT key, server certificate, UPnP setting, line speed, and time & date

11.3 Check the status [Status]

Click the [Status] tab of the “Maintenance” page. (→page 14, page 15)
The status of this microphone can be checked on this page.



[UPnP]

- **Port number(HTTP), Port number(HTTPS):** The port number that is set for UPnP port forwarding will be displayed.
- **Status:** The port forwarding status will be displayed.
- **Router global address:** The global address of the router will be displayed.

[Self check]

The self check result of the hardware will be displayed.

Note

- Refer to our website (<http://security.panasonic.com/pss/security/support/info.html>) for further information about the contents of the displayed statuses.

11.4 Reset the settings/Reboot the microphone [Default reset]

Click the [Default reset] tab of the “Maintenance” page. (→page 14, page 15)
The settings and reboot of the microphone can be performed on this page.



[Reset to the default (Except the network settings)]

Click the [Execute] button to reset the settings to the default. Note that the network settings will not be reset. It is impossible to operate the microphone for about 3 minutes after the initialization.

[Reboot]

Click the [Execute] button to reboot the microphone. It is impossible to operate the microphone for about 3 minutes after rebooting the microphone.

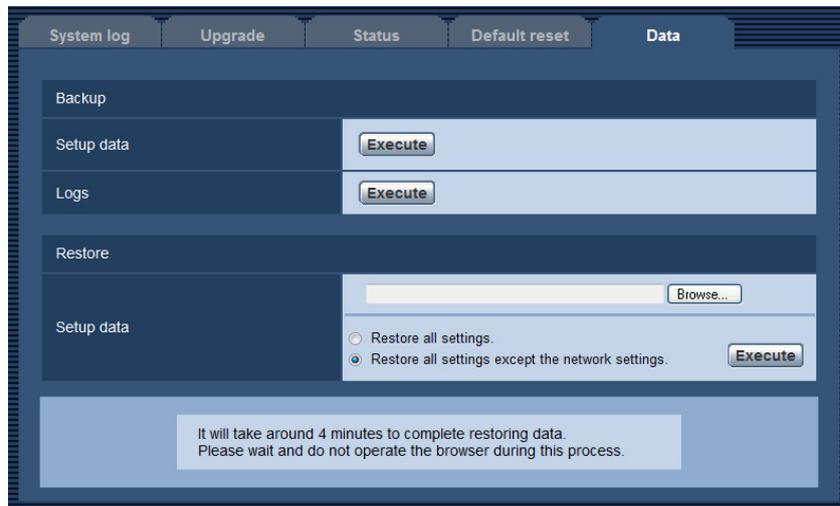
Note

- To initialize the network settings (→page 32), turn off the power of the microphone, then turn on the power again while holding down the INITIAL SET button on the microphone, and keep the INITIAL SET button held down for about 5 seconds. Wait about 3 minutes after releasing the button. The microphone will start up and the settings including the network settings will be initialized. Do not turn off the power of the microphone for about 3 minutes after turning on the power.

11.5 Settings data/backing up or restoring logs [Data]

Click the [Data] tab of the “Maintenance” page. (→page 14, page 15)

The setting related to settings data and backing up or restoring logs can be configured in this section.



Backup

- **[Setup data]**
Click the [Execute] button to backup the setup data of the microphone to a PC.
- **[Logs]**
Click the [Execute] button to backup the log data of the microphone to a PC.

Restore

- **[Setup data]**
Press the [Browse...] button and select the setup data files to restore.
Click the radio button respective to the desired option to determine whether or not to also restore network related setting contents.
Click the [Execute] button to start restoring. Do not perform operations until the restoration is complete. (The microphone will be rebooted when the restoration is complete.)
Make sure to set the file name of setup data files used when restoring to "model name.dat". (The model name must be written in lower case letters and "WV-" is not needed.)

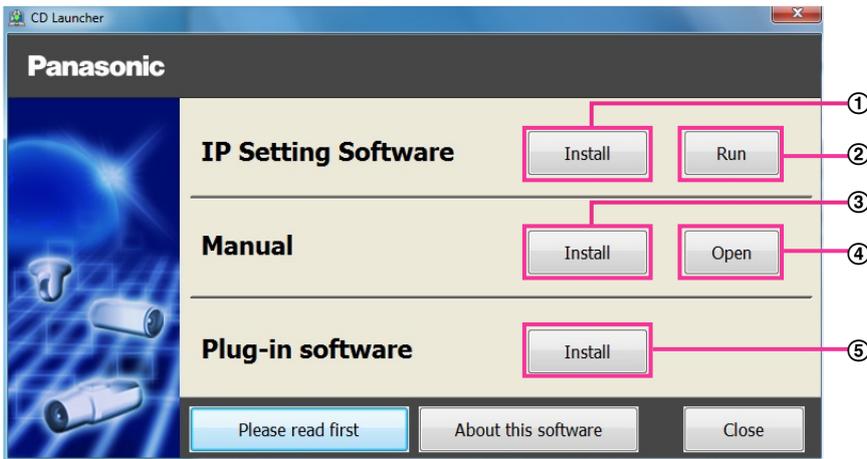
12 Using the CD-ROM

12.1 About the CD launcher

By inserting the provided CD-ROM into the CD-ROM drive of your PC, the CD launcher is automatically started and the license agreement is displayed. Read the agreement and select "I accept the terms in the license agreement", and then click "OK".

The CD launcher window is displayed.

- If the launcher window is not displayed, double click the "CDLauncher.exe" file on the CD-ROM.

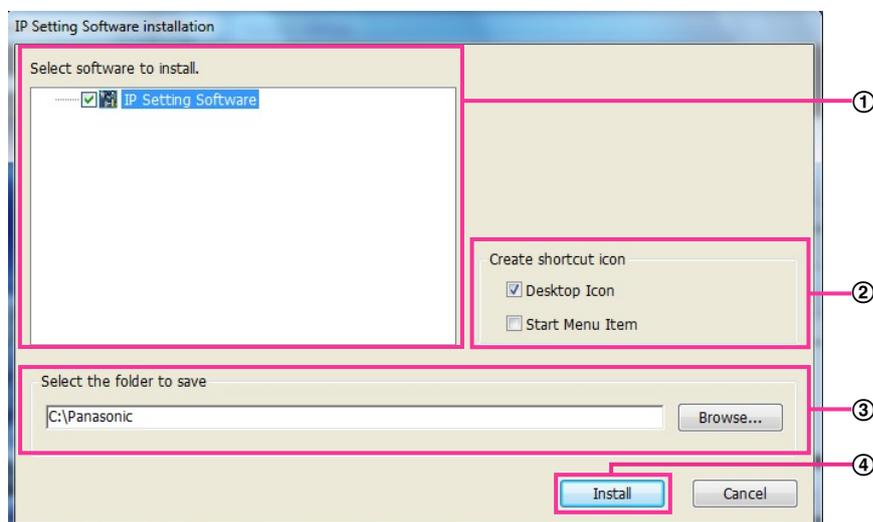


Using the supplied CD-ROM, the following actions can be performed.

- ① The Panasonic "IP Setting Software" can be installed on the PC. (→page 63)
- ② Settings related to the microphone's network can be set from the Panasonic "IP Setting Software". (→page 65)
- ③ The manuals can be installed on the PC. (→page 64)
- ④ You can also view the manuals without installing them to the PC by clicking the [Open] button.
- ⑤ The plugin software can be installed on the PC. (→page 64)

12.2 Installing Panasonic “IP Setting Software”

On the CD launcher window, click the [Install] button next to [IP Setting Software] to display the Panasonic “IP Setting Software” installation window. Confirm the following settings before starting the installation.



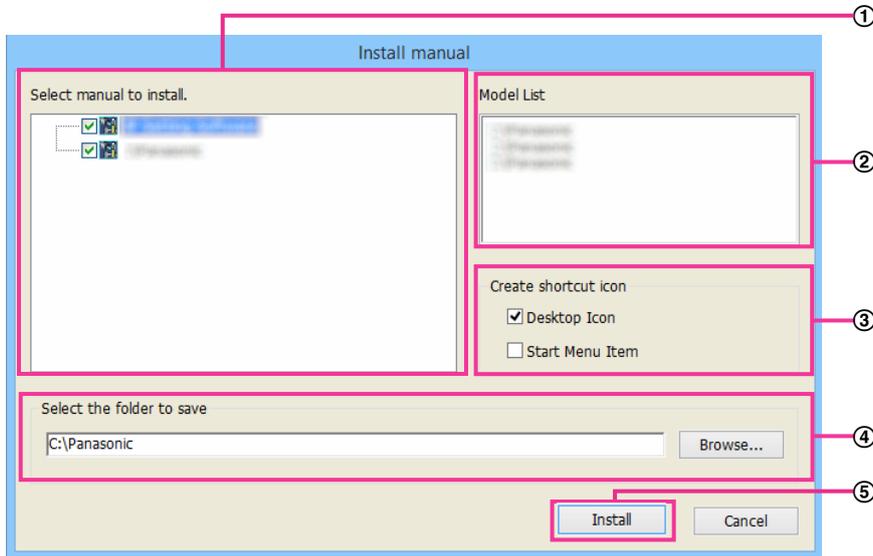
- ① Select the Panasonic “IP Setting Software” to install.
- ② Select where to create the Panasonic IP setting shortcut icon when the Panasonic “IP Setting Software” is installed.
- ③ Specify which folder on the PC to install the Panasonic “IP Setting Software” to.
- ④ Click the [Install] button to start the installation.

Note

- To uninstall the Panasonic “IP Setting Software” delete the shortcut icon from where you specified it to be installed (the default is on the desktop) during installation and the [EasyIPConfig] folder from the folder (the default is C:\Panasonic) you specified during installation.

12.3 Installing the manuals

On the CD launcher window, click the [Install] button next to [Manual] to display the Manual installation window. Confirm the following settings before starting the installation.



- ① Select which manuals to install. The models that the manuals support are displayed in ② “Model List”.
- ② The models that are supported by the manuals selected in ① are displayed here.
- ③ Select where to create the manuals shortcut icon when the manuals are installed.
- ④ Specify which folder on the PC to install the manuals to.
- ⑤ Click the [Install] button to start the installation.

Note

- To uninstall the manuals, delete the shortcut icon from where you specified it to be installed (the default is on the desktop) during installation and the [Manual] folder from the folder (the default is C:\Panasonic) you specified during installation.

12.4 Installing the plugin software

The plugin software “Network Microphone Plugin” must be installed on the PC in order to monitor microphone audio. On the CD launcher window, click the [Install] button of the “Plug-in software”, and follow the instructions displayed on the window to install the software.

A message is displayed if a PC that does not have the software installed tries to access the microphone. Install the software by following the instructions displayed on the window. Refer to page 2 for further information.

Note

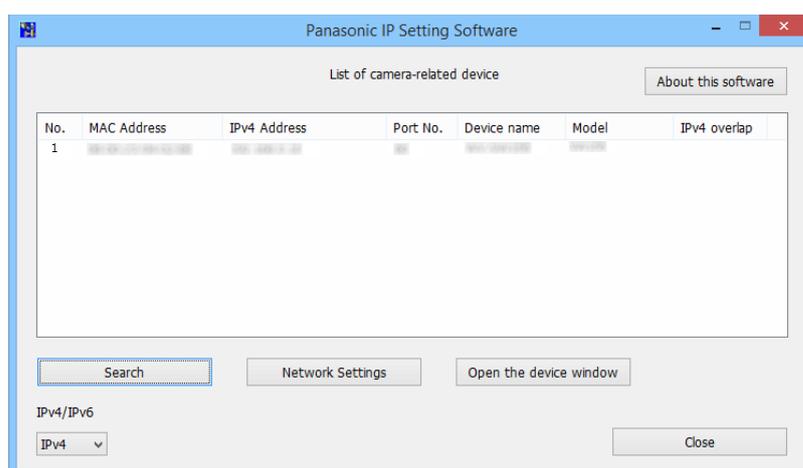
- To uninstall the plugin software, follow the steps below depending on the OS used on your PC. Delete [Network Microphone Plugin] from [Control Panel] - [Programs] - [Uninstall a program].

12.5 Configure the network settings of the microphone using the Panasonic “IP Setting Software”

It is possible to perform the network settings of the microphone using the “IP Setting Software” on the provided CD-ROM. When using multiple microphones, it is necessary to configure the network settings of each microphone independently. If the Panasonic “IP Setting Software” does not work, access the “Network” page from the setup menu of the microphone in the browser and perform settings separately. (→page 32)

IMPORTANT

- The “Windows Security Alert” window may be displayed when starting the “IP Setting Software”. In this case, disable “User Account Control” from the control panel.
 - Panasonic “IP Setting Software” is inoperable in other subnets via the same router.
 - This microphone cannot be displayed or set with an older version of the “IP Setting Software” (version 2.xx).
 - Due to security enhancements in “IP Setting Software”, “Network Settings” of the microphone to be configured cannot be changed when around 20 minutes have passed after turning on the power of the microphone. (When the effective period is set to “20min” in the “Easy IP Setup accommodate period”.) However, settings can be changed after 20 minutes for microphones in the initial set mode.
1. To start the Panasonic “IP Setting Software”, click the [Run] button next to [IP Setting Software] from the CD launcher menu window, or double-click on the shortcut icon created after installing the software on the PC.
 - The License Agreement will be displayed. Read the Agreement and choose “I accept the terms in the license agreement”, and click [OK].
 - The “IP Setting Software” screen is displayed. If a microphone is found, information about it, such as the MAC address and IP address, is displayed.
 2. Click the [Open the device window] button after selecting the MAC address/IP address of the microphone to be configured.



Note

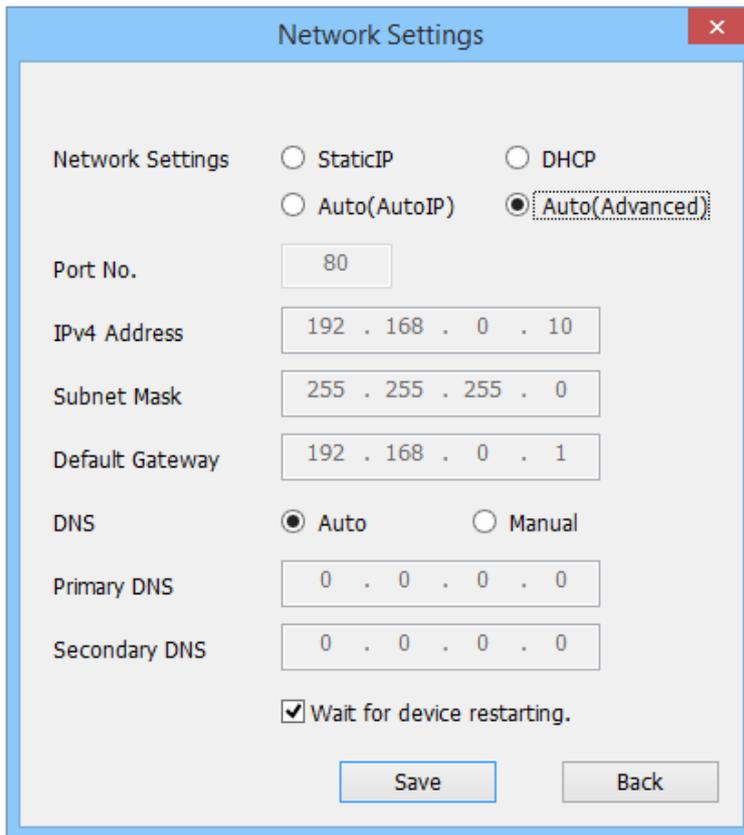
- When using a DHCP server, the IP address assigned to the microphone can be displayed by clicking the [Search] button of the “IP Setting Software”.
- When duplicate IP addresses are used, the number of devices with the duplicate address is displayed in overlap.

- It is possible to change the “List of camera-related device” display between IPv4 addresses and IPv6 addresses in accordance with the protocol in use.
 - The information displayed can be sorted by clicking the title of each displayed item.
 - When the [Network Settings] button is clicked, the “Network Settings” screen is displayed and network settings can be changed. For further information, refer to page 66.
 - Click the [Search] button to display the latest information.
3. When the plugin software “Network Microphone Plugin” installation screen is displayed, follow the on-screen instructions to install the software. (The plugin software “Network Microphone Plugin” is installed from the microphone.)
- The “Live” page of the microphone is displayed.
 - If the plugin software “Network Microphone Plugin” cannot be installed or live images are not displayed, click the [Install] button next to [Plug-in software] from the CD launcher window to install the software.

Changing Network Settings

When changing settings related to the network settings, such as connection mode, IP address, and subnet mask, click the [Network Settings] button in [IP Setting Software] screen.

The “Network Settings” screen is displayed. Enter each item and then click the [Save] button.



Note

- By unchecking the “Wait for device restarting.” checkbox, multiple microphones can be continuously configured.
- For further information about each setting of the “Network Settings” page, refer to page 32.

IMPORTANT

- It may take for around 2 minutes to complete uploading the settings to the microphone after clicking the [Save] button. The settings may be invalidated when the LAN cable is disconnected before completing the upload. In this case, perform the settings again.
- When using a firewall (including software), allow access to all UDP ports.

13 About the displayed system log

Error indications relating to Dynamic DNS Update

Category	Indication	Description
DDNS server error	Failed to resolve the DDNS server address from DNS.	<ul style="list-style-type: none"> The designated IP address of the DNS may be incorrect. Check if the DNS settings are configured correctly. The DNS server may be down. Ask the network administrator.
Connection error	No response from the DDNS server.	<ul style="list-style-type: none"> The DDNS server may be down. Ask the network administrator.
	Same host name has registered.	<ul style="list-style-type: none"> The same host name has already been registered in the DDNS server. Check if the DDNS Update settings are configured correctly.
Internal error	Undefined error.	<ul style="list-style-type: none"> An error occurred in the DDNS function. Check if the DDNS Update settings are configured correctly.

Error indications relating to NTP

Category	Indication	Description
Connection error	No response from the NTP server.	<ul style="list-style-type: none"> The IP address of the server may be incorrect. Check if the IP address of the server is configured correctly. The NTP server may be down. Ask the network administrator.
Internal error	Undefined error.	<ul style="list-style-type: none"> An error occurred in the NTP function. Check if the NTP settings are configured correctly.
Synchronizing with NTP succeeded.	NTP update succeeded.	<ul style="list-style-type: none"> Time correction succeeded.

Log indications relating to HTTPS

Category	Indication	Description
HTTPS	Self-signed Certificate - Generated	<ul style="list-style-type: none"> • Generation of the self-signed certificate is complete.
	Self-signed Certificate - Deleted	<ul style="list-style-type: none"> • Deletion of the self-signed certificate is complete.
	Certificate Signing Request - Generated	<ul style="list-style-type: none"> • Generation of the CSR (Certificate Signing Request) is complete.
	CA Certificate - Installed	<ul style="list-style-type: none"> • Installation of the server certificate is complete.
	CA Certificate - Deleted	<ul style="list-style-type: none"> • Deletion of the server certificate is complete.
	Previous CRT key - Applied	<ul style="list-style-type: none"> • Previous CRT key is applied.
	CRT key - Generated	<ul style="list-style-type: none"> • Generation of the CRT key is complete.

Log indications relating to login

Category	Indication	Description
Login	User name or IP address	<ul style="list-style-type: none"> • The login user name will be displayed when "On" is selected for "User auth." • The IP address of the PC currently accessing the microphone will be displayed when "On" is selected for "Host auth."

Error indications relating to malfunction notifications

Category	Indication	Description
Panasonic alarm protocol notification error	Failed to find destination of notification.	<ul style="list-style-type: none"> • The IP address of the destination of notification may be incorrect. Check if the IP address of the destination of notification is configured correctly. • The destination of notification may be down. Ask the network administrator.
	Failed to resolve destination addr. from DNS.	<ul style="list-style-type: none"> • The DNS server settings may be incorrect. Check if the DNS settings are configured correctly. • The DNS server may be down. Ask the network administrator.

14 Troubleshooting

Before asking for repairs, check the symptoms with the following table.

Contact your dealer if a problem cannot be solved even after checking and trying the solution in the table or a problem is not described below.

Symptom	Cause/solution	Reference pages
Cannot access from the web browser.	<ul style="list-style-type: none"> Is the LAN cable (category 5 or better) firmly connected to the network connector of the microphone? 	Installation Guide
	<ul style="list-style-type: none"> Is the link indicator lit? When it is not lit, connection to a LAN may not be established or a network may be not working correctly. Check if the cables have any contact failure or if the wiring is correct or not. 	Installation Guide
	<ul style="list-style-type: none"> Is the power of the microphone on? Check if the power of the microphone is turned on. 	Installation Guide
	<ul style="list-style-type: none"> Are the set IP addresses valid? 	32
	<ul style="list-style-type: none"> Are you accessing the wrong IP address? Check the connection as follows. With the Windows command prompt, > ping "IP address of the microphone". If there is reply from the microphone, the connection is normal. If there is no reply, check the connection with the following methods using a computer connected to the same network as the microphone. If the firewall settings on the PC are enabled, temporarily disable them before performing settings on the microphone. <ul style="list-style-type: none"> Start the Panasonic "IP Setting Software", confirm the microphone's IP address, and then access that IP address. If the network settings (IP address, subnet mask, and default gateway) are incorrect, reboot the microphone and change the network settings by using the Panasonic "IP Setting Software" within 20 minutes after the restart. In networks that do not have a DHCP server, the IP address of the microphone will be configured to "192.168.0.10" when the microphone is rebooted by holding the INITIAL SET button on the microphone. After the microphone is initialized, access the microphone and set the IP address again. (When the microphone is initialized, all the settings of the microphone previously configured on the setup menus will be initialized.) 	65 Installation Guide

Symptom	Cause/solution	Reference pages
	<ul style="list-style-type: none"> Is “554” selected for the HTTP port number? For the HTTP port number, select a port number other than the following port numbers used by the microphone. The number used by the microphone: 20, 21, 23, 25, 42, 53, 67, 68, 69, 110, 123, 161, 162, 443, 554, 995, 10669, 10670, 59000 - 61000 	34
Cannot access from the web browser.	<ul style="list-style-type: none"> Is the same IP address provided to other devices? Are there contradictions between the address and the network subnet to be accessed? When the microphone and the PC are connected in the same subnet: Are the IP addresses of the microphone and the PC set in a common subnet? Or is “Use Proxy Server” for the settings of the web browser checked? When accessing the microphone in the same subnet, it is recommended to enter the address of the microphone in the “Don’t Use Proxy For These Addresses” box. When the microphone and the PC are connected in the different subnet: Is the IP address of the default gateway set for the microphone correct? 	-
	<ul style="list-style-type: none"> Did you access “http://” while using the HTTPS function? To use the HTTPS function, access “https://”. It is also necessary to enter the port number. 	49
Cannot access the microphone via the Internet.	<ul style="list-style-type: none"> Are the network settings of the microphone correct? Set the default gateway or DNS server address correctly. To use the DDNS service, check that the settings are correct. Is the setting for “Default gateway” on the “Network” page configured? Or is the setting correct? When communicating using IPv4: Configure the setting for “Default gateway” of “IPv4 network” on the [Network] tab of the setup menu. 	32
	<ul style="list-style-type: none"> Is the setting of port forwarding configured for the router? To enable the access to the microphone via the Internet, it is necessary to perform the port forwarding setting when the router in use does not support the UPnP function. Refer to the manuals provided with the router for further information. Is the UPnP function of the router disabled? Refer to the manuals provided with the router in use to enable the UPnP function. Is packet filtering set for the router to forbid the access via the Internet? Configure the settings of the router in use to enable the access via the Internet. Refer to the manuals provided with the router for further information about the settings. 	37

Symptom	Cause/solution	Reference pages
	<ul style="list-style-type: none"> Are you accessing the microphone using the local address (the IP address used in a local network)? When accessing the microphone, use the global address (or the URL registered in the DDNS service) and the port number of the microphone as the IP address to be used in the Internet. 	<p>32 33 55</p>
<p>Authentication window is displayed repeatedly.</p>	<ul style="list-style-type: none"> Is the user name and password changed? While accessing the microphone, when changing the user name and password of another user logging into the microphone on another web browser, the authentication window will be displayed each time the screen is changed or refreshed. Have you changed the [Authentication] setting? When the [Authentication] setting has been changed, close the web browser, and then access the microphone again. The authentication window may be for the network camera, not the network microphone. Check the IP address displayed on the authentication window to see whether or not it is the authentication window of the network camera. 	<p>-</p>
<p>It takes time to display the screen.</p>	<ul style="list-style-type: none"> Are you accessing the microphone in the HTTPS mode? In this mode, the refresh interval becomes slower due to decode processing. Are you accessing another microphone in the same local network via a proxy server? Configure the web browser to not use the proxy server. Are two or more users browsing the live images simultaneously? It may take time to display the screen or the refresh interval may become slower when two or more users browse the live images simultaneously. 	<p>- - -</p>

Symptom	Cause/solution	Reference pages
Cannot hear audio.	<ul style="list-style-type: none"> Is the speaker connected correctly and firmly? Confirm that it is connected correctly and firmly. Is the speaker on the Windows desktop muted? Is the mute on the “Live” page turned off? 	-
	<ul style="list-style-type: none"> Is the plugin software installed on the PC? Confirm that the plugin software “Network Microphone Plugin” is installed. 	2
	<ul style="list-style-type: none"> When using a 360° camera installed in the center of the unit, the microphone directionality that can be configured using the unit according to the type of the camera image to be displayed is limited. 	24
	<ul style="list-style-type: none"> Are the “Live” pages of the camera and microphone displayed on the same PC? When displaying the “Live” page of the camera, turn off the audio in the camera settings. Refer to the operating instructions of the network camera in use for further information. 	-
Cannot hear because the audio is low.	<ul style="list-style-type: none"> Is the microphone sensitivity setting too low? On the audio setup page, try setting the microphone sensitivity to a higher value. 	-
There is noise in the audio or the audio is interrupted.	<ul style="list-style-type: none"> Is the microphone sensitivity setting too high? Are multiple users concurrently connected to the microphone? When multiple users are concurrently connected to the microphone, the audio may contain noise or be interrupted. Audio may be improved by changing operation to multicast. Is there sufficient bandwidth on the network? Reserve sufficient network bandwidth. Is the microphone installed in a place with large vibrations? Install the microphone in a place with less frequent vibrations. 	-

14 Troubleshooting

Symptom	Cause/solution	Reference pages
Cannot hear audio with configured directionality very well.	<ul style="list-style-type: none"> • When using the microphone with a 360° camera, check the following. <ul style="list-style-type: none"> – When the 360° camera and microphone are not properly attached, the direction of the image and audio may not match. Check the attachment. (→ Installation Guide) – Check if the microphone directionality can be designated and configured to the type of camera image. (→page 10) • In the following situations, the directionality may deteriorate. <ul style="list-style-type: none"> – The target person is very far (approx. 6 m (19.6 ft) or more) – The voice of the target person is low, or the target person is facing in the opposite direction – There are many obstacles surrounding the microphone that reflect sound – There is another sound source near the microphone – There is very loud noise where the microphone is used – The sound where the microphone is used echoes frequently 	-
The directional position of the audio does not match the image of the 360° camera.	<ul style="list-style-type: none"> • Install the firmware of a supported 360° camera. For information about the firmware of supported 360° cameras, refer to our website below. http://security.panasonic.com/pss/security/support/info.html 	-
	<ul style="list-style-type: none"> • Follow the Installation Guide, and attach the 360° camera and the unit correctly. 	-
Old logs are displayed.	<ul style="list-style-type: none"> • When [Every time I visit the webpage] is not selected for [Check for newer versions of stored pages:] in the [Temporary Internet Files] section, old logs sometimes may be displayed. In this case, do the following. <ol style="list-style-type: none"> 1. Select “Internet Options...” under “Tools” on the menu bar of Internet Explorer. 2. Click the [Settings] button in the [Browsing history] section on the [General] tab, and then select [Every time I visit the webpage] for [Check for newer versions of stored pages:] in the [Temporary Internet Files] tab or section. 	-
The malfunction notification button on the “Live” page does not display the current status in real time.	<ul style="list-style-type: none"> • Is “Real time” selected for “Alarm status update mode”? 	18

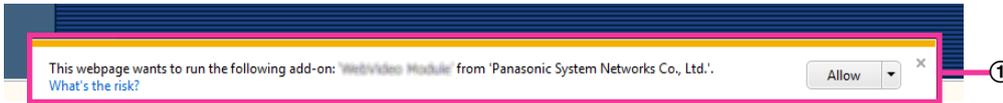
Symptom	Cause/solution	Reference pages
No image is displayed on the "Live" page.	<ul style="list-style-type: none"> Press the [F5] key on the keyboard of the PC or click the [Live] button. 	9
	<ul style="list-style-type: none"> Is the plugin software of the network camera installed? Refer to the operating instructions of the network camera in use. 	2
	<ul style="list-style-type: none"> Click "Internet Options..." under "Tools" of the menu bar of Internet Explorer, and then click the [Security] tab. Click "Internet" in the "Select a zone to view or change security settings." section. Then, click the [Custom level...] button to open the "Security Settings" window. Under "Miscellaneous", select "Enable" for "Access data sources across domains". Click the [OK] button. 	-
Shortcut icon of the microphone is not displayed on "Network" of the PC.	<ul style="list-style-type: none"> Is the Windows component of UPnP added? Add the component to the PC in use. 	37
Cannot backup settings or logs.	<ul style="list-style-type: none"> Download of files using Internet Explorer may be disabled. Click "Internet Options..." on the [Tools] menu of Internet Explorer, and [Security] tab. Then, click the [Custom level...] button to open the "Security Settings" window. Under "Downloads", select "Enable" for "Automatic prompting for file downloads" (except Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11). Click the [OK] button. The warning window will be displayed. Click the [Yes] button. 	-

Information Bar

Depending on the OS installed on the PC, the following may occur. Follow the instructions below when the following has occurred. By performing the following solutions, other applications will not be affected.

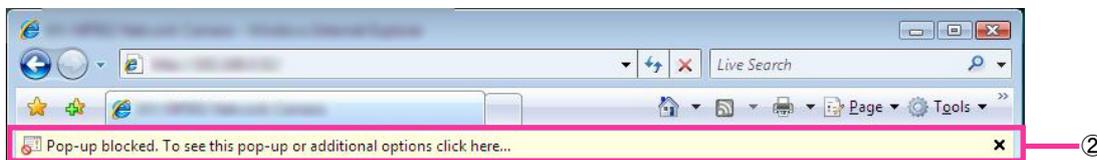
When using Internet Explorer 9, Internet Explorer 10, or Internet Explorer 11:

The “Information Bar” (①) expressed in the following symptom and solutions will be displayed just below the address bar only when there is information to communicate.



When using Internet Explorer 7 or Internet Explorer 8:

The “Information Bar” (②) expressed in the following symptom and solutions will be displayed just below the address bar only when there is information to communicate.



Symptom	Cause/solution	Reference pages
The following message is displayed on the information bar. “Pop-up blocked. To see this pop-up or additional options, click here...” (Internet Explorer 7 or Internet Explorer 8)	<ul style="list-style-type: none"> Click the information bar and select “Always Allow Pop-ups from This Site...”. The dialog window saying “Allow pop-ups from this site?” will be displayed. Click the [Yes] button. 	-
The following message is displayed on the information bar. “Internet Explorer blocked a pop-up from ***.***.***.*** (IP address).” (Internet Explorer 9, Internet Explorer 10, or Internet Explorer 11)	<ul style="list-style-type: none"> Select “Options for this site” → “Always allow”. 	-
The following message is displayed on the information bar. “This webpage wants to run the following add-on: `WebVideo Module' from `Panasonic Corporation`.” (Internet Explorer 9, Internet Explorer 10, or Internet Explorer 11)	<ul style="list-style-type: none"> Select [Allow]. 	-

Symptom	Cause/solution	Reference pages
<p>The following message is displayed on the information bar. “This site might require the following ActiveX control 'nwmpsetup.exe' from 'Panasonic Corporation'. Click here to install...” (Internet Explorer 7 or Internet Explorer 8)</p>	<ul style="list-style-type: none"> Click the information bar and select “Install ActiveX Control”. The “Security Warning” window will be displayed. Click the [Install] button on the displayed “Security Warning” window. 	-
<p>The following message is displayed on the information bar. “This site might require the following ActiveX control 'nwmpsetup.exe' from 'Panasonic Corporation'. Click here to install...” (Internet Explorer 9, Internet Explorer 10, or Internet Explorer 11)</p>	<ul style="list-style-type: none"> Select [Install]. The “Security Warning” window will be displayed. Click the [Install] button on the displayed “Security Warning” window. 	-
<p>An unnecessary status bar or scroll bar is displayed on the pop-up window.</p>	<ul style="list-style-type: none"> Click “Internet Options...” under “Tools” of the menu bar of Internet Explorer, and then click the [Security] tab. Click “Internet” in the “Select a zone to view or change security settings.” section. Then, click the [Custom level...] button to open the “Security Settings” window. Under “Miscellaneous”, select “Enable” for “Allow script-initiated windows without size or position constraints”. Click the [OK] button. When the warning window is displayed, click the [Yes] button. 	-
<p>Images do not fit in the frames.</p>	<ul style="list-style-type: none"> When “120 DPI” or higher is selected for “DPI setting”, they may not be displayed correctly. When using Windows 8.1: Right-click on the desktop, click “Screen resolution” → “Make text and other items larger or smaller”, and then move the slider of “Change the size of all items” to “Smaller” so that the screen becomes the recommended size. When using Windows 8/Windows 7: Right-click on the desktop, click “Screen resolution” → “Make text and other items larger or smaller”, and then select “Smaller - 100% (default)”. When using Windows Vista: Right-click on the screen and click “Personalize” → “Adjust font size (DPI)”, and then select “Default scale (96 DPI)”. 	-

For U.S. and Canada:

**Panasonic System Communications Company of North America,
Unit of Panasonic Corporation of North America**

www.panasonic.com/business/

For customer support, call 1.800.528.6747

Two Riverfront Plaza, Newark, NJ 07102-5490

Panasonic Canada Inc.

5770 Ambler Drive, Mississauga, Ontario, L4W 2T3 Canada

(905)624-5010

www.panasonic.ca

For Europe and other countries:

Panasonic Corporation

<http://www.panasonic.com>

Panasonic Corporation

Osaka, Japan

Authorised Representative in EU:

Panasonic Testing Centre

Panasonic Marketing Europe GmbH

Winsbergring 15, 22525 Hamburg, Germany

© Panasonic Corporation 2017