New functions and addendum

・This document contains descriptions of how to set the new functions and their restrictions. It is recommended to read them while referring to the Operating Instructions provided with this product together.
・Depending on the model used, the screens shown in the explanations may differ to the actual camera screens.
・The model number is abbreviated in some descriptions in this manual.
・This document is for the following models.
WV-U2542L, WV-U2540L, WV-U2532L, WV-U2530L, WV-U1542L, WV-U1532L, WV-U2142L, WV-U2140L, WV-U2132L, WV-U2130L, WV-U1142, WV-U1132, WV-U1130

Due to software upgrade, the following functions have been added and changed to this product.

・Firmware Ver.1.00 for WV-U2540L, WV-U2530L, WV-U2140L, WV-U2130L
Ver.1.02 except for WV-U2540L, WV-U2530L, WV-U2140L, WV-U2130L

No.	Functions	Item (Page)	Page
1	Change of [Viewer software (nwcv5Ssetup.exe)] - [Smoother live video display on the browser (buffering)] default setting	Basic (Basic)	3
2	Change of [Internet mode] default setting	Image(Image)	4

・Firmware Ver.1.10

No.	Functions	Item (Page)	Page
3	Add the image capture size 2688 x 1520 in the image capture mode (WV-U2542L, WV-U2540L, WV-U2142L, WV-U2140L WV-U1542L, WV-U1142)	Image(Image)	5
4	Improve the maximum frame rate of the stream	Image(Image)	6
5	Change the initial value of Network Settings and DHCP behavior in IPv4 network of Network	Network (Network)	8
6	Add ONVIF® settings in Network	Network (Network)	9
7	Added “SNMP transmission upon alarm detection” to “Camera action on alarm	Alarm (Alarm)	10
8	Enhanced the access restriction function of SNMP v1/v2	Advanced (Network)	11
9	Added “SNMP trap setting” to “SNMP”	Advanced (Network)	12
10	Enable the HTTP alarm notification function to support the HTTPS communication and the Digest authentication	Notification(Alarm)	15
11	Add to the system log when authentication fails for the HTTP alarm notification function	System log(Others)	17

・Firmware Ver.1.21

No.	Functions	Item (Page)	Page
12	Add a notify to the [SNMP trap setting]	Advanced (Network)	18
13	Add to the system log when recording stream fails to write	Maintenance (Status)	19
14	Add a function to notify the user of writing failures in the recording stream with a unique alarm	Notification (Alarm)	20
15	Add a note when the bit rate of the recording stream is set to a value exceeding recommended value	Image (Image)	21
16	Extend authentication password for the destination of notification	Network (Advanced)	22

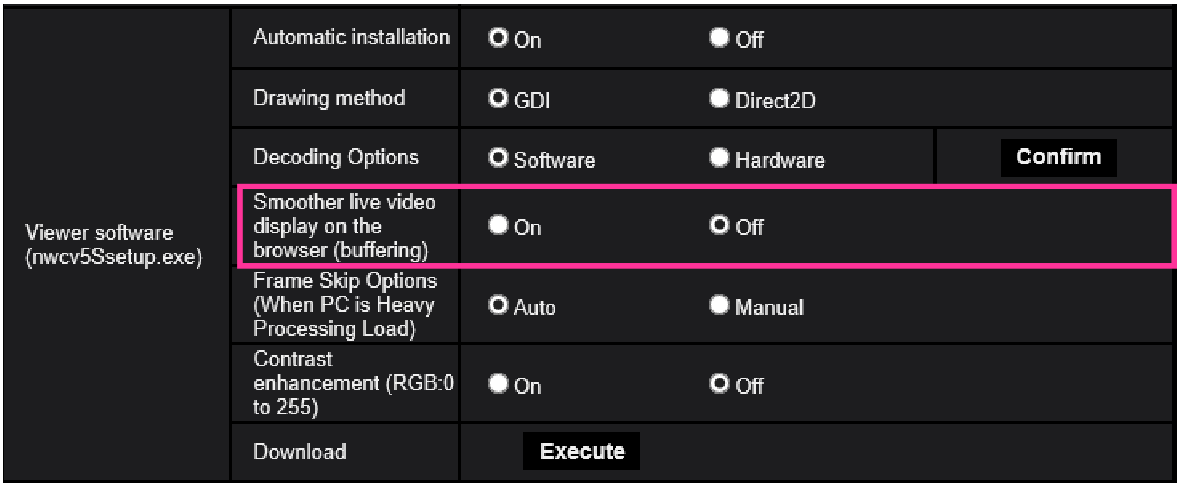
・Firmware Ver.1.50

No.	Functions	Item (Page)	Page
17	Change the initial value of “Overwrite” of SD memory card to On	SD memory card (Basic)	23
18	Add the supplementary explanation of On/Off of Internet mode to the setting screen	Advanced (Network)	24
19	Add NTP test function	Advanced (Network)	25
20	Add TLS settings to HTTPS	Advanced (Network)	26
21	Add MQTT function	Advanced (Network)	27
22	Add a system log when MQTT function fails	Status (Maintenance)	30
23	Add LLDP function	Advanced (Network)	31

1. Change of [Viewer software (nwcv5Ssetup.exe)] - [Smoother live video display on the browser (buffering)] default setting

(Operating Instructions “Configure the basic settings of the camera” [Basic]-“Configure the basic settings” [Basic])

Change of [Viewer software (nwcv5Ssetup.exe)] - [Smoother live video display on the browser (buffering)] default setting.



Viewer software (nwcv5Ssetup.exe)	Automatic installation	○ On	● Off	
	Drawing method	○ GDI	● Direct2D	
	Decoding Options	○ Software	● Hardware	Confirm
	Smoother live video display on the browser (buffering)	● On	○ Off	
	Frame Skip Options (When PC is Heavy Processing Load)	○ Auto	● Manual	
	Contrast enhancement (RGB:0 to 255)	● On	○ Off	
	Download	Execute		

[Viewer software (nwcv5Ssetup.exe)] - [Smoother live video display on the browser (buffering)]
Perform settings to display camera images on the viewer software.

- **On**: Images are temporarily stored on the computer and are displayed smoother.
- **Off**: Images are displayed in real-time and are not stored on the computer.
- **Default**: Off

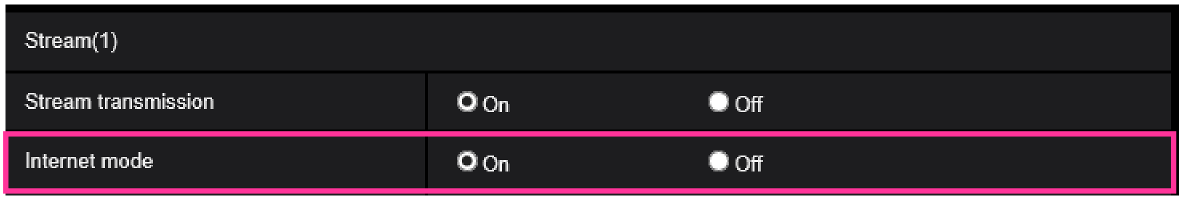
Note

- If the image is not displayed smoothly, set to “On”.

2. Change of [Internet mode] default setting

(Operating Instructions “Configure the settings relating to images” [Image]- “Configure the settings relating to Stream” [Image])

Change of [Internet mode] default setting.



Stream(1)		
Stream transmission	◉ On	● Off
Internet mode	◉ On	● Off

[Internet mode]

Select “On” when transmitting H.265 images via the Internet. It is possible to transmit stream without changing the broadband router settings configured for JPEG image transmission.

- **On**: H.265 images will be transmitted using the HTTP port. Refer to [HTTP port] for further information about the HTTP port number settings.
- **Off**: H.265 images will be transmitted using the UDP port.
- **Default**: On

Note

- When “On” is selected, only “Unicast port (AUTO)” will be available for “Transmission type”.
- When “On” is selected, it may take time to start displaying stream images.
- When “On” is selected, stream images may not be displayed depending on the number of the concurrent access user, etc.
- When “On” is selected, only IPv4 access is available.

3. Add the image capture size 2688 x 1520 in the image capture mode (WV-U2542L, WV-U2540L, WV-U2142L, WV-U2140L, WV-U1542L, WV-U1142)

(Operating Instructions “Configure the settings relating to images” [Image]- “Configure the settings relating to the image capture mode” [Image])

Add “16:9 (2688x1520 30fps mode)” and “16:9 (2688x1520 25fps mode)” in the “image capture mode”.

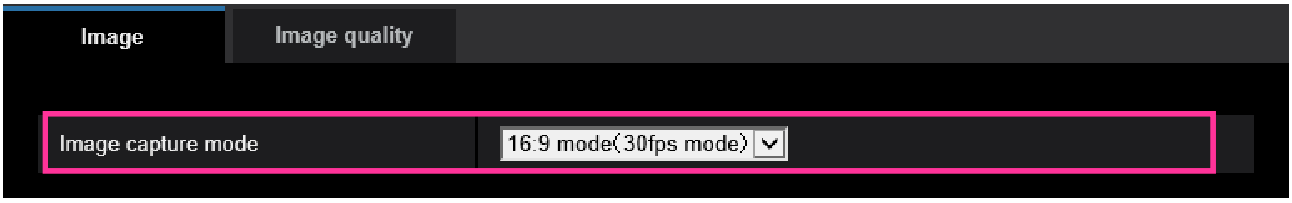


Image capture mode: 16:9 mode(30fps mode)

[Image capture mode]

Select an image to be displayed on the “Live” page.

16:9 (30fps mode)/16:9 (25fps mode)/16:9 (2688x1520 30fps mode)/16:9 (2688x1520 25fps mode)

Default: 16:9(30fps mode)

For 16:9 (2688 x 1520 30 fps mode) or 16:9 (2688 x 1520 25 fps mode), the JPEG (1)/ JPEG (2)/ Stream (1)/ Stream (2)/ Stream (3) items are listed below

Settings Item		Settings
JPEG(1)	Image capture size	2688x1520 1920x1080 640x360 320x180
JPEG(2)		Not available
Stream(1)	Stream Transmission	On/ Off
	Image capture size	2688x1520 1920x1080 640x360 320x180
	Frame rate	Max. 30fps/ 25fps
	Smart Coding - GOP control	Not available (Off)
	Smart Coding – AUTO VIQS	Not available (Off)
Stream(2)/ Stream(3)		Not available (Off)
Image rotation		0°(Off), 180°(Upside-down)

Note

- The maximum refresh interval of JPEG(1) / JPEG(2) will be as follows.

Image capture mode	Stream transmission			
	On		Off	
	JPEG(1)	JPEG(2)	JPEG(1)	JPEG(2)
16:9 (2688x1520 30fps mode)	Max. 3fps	Not available	Max. 10fps	Not available
16:9 (2688x1520 25fps mode)	Max. 3.1fps	Not available	Max. 8.3fps	Not available

- ”Image rotation” cannot be set “90°” and “270°”.

4. Improve the maximum frame rate of the stream

(Operating Instructions “Configure the settings relating to images” [Image]- “Configure the settings relating to Stream” [Image])

The default JPEG and stream values have been changed so that the frame rate can be delivered at 30 fps and 25 fps even if Stream (1) and Stream (2) are set to On.

Note

- When the image capture mode is changed to 25 fps mode, the frame rate is increased up to 25 fps.
- When Stream (1) and Stream (2) are set to On, if the "Stream Transmission" of Stream (3) is set to "On", the "Frame rate" for Stream (1) and Stream (2) will be "15 fps"/"12.5 fps". However, for 4M models, the image capture size of Stream (1) should be greater than 1920 x 1080.
- If the "Frame rate" for Stream (1) or Stream (2) is "30 fps"/"25 fps", the "Refresh interval (JPEG)*" is limited to a maximum of 1 fps.
- If the "Frame rate" for Stream (1) and Stream (2) is set to "15 fps"/"12.5 fps", the "Refresh interval (JPEG) *" will be up to "3 fps"/"3.1 fps".
- To set "GOP control" and "AUTO VIQS" of "Smart Coding" to "On", please set the "Frame rate" for Stream (1) and Stream (2) to "15 fps"/"12.5 fps" or below

WV-U2532L, WV-U2530L, WV-U1532L, WV-U2132L, WV-U2130L, WV-U1132, WV-U1130

Settings Item		Settings(Default)
Image capture mode		16:9 (30fps mode)
Refresh interval (JPEG)*		1fps
JPEG(1)	Image capture size	1920x1080
JPEG(2)	Image capture size	640x360
Stream(1)	Stream Transmission	On
	Image capture size	1920x1080
	Frame rate	30fps
	Smart Coding - GOP control	Not available (Off)
	Smart Coding – AUTO VIQS	Not available (Off)
Stream(2)	Stream Transmission	On
	Image capture size	640x360
	Frame rate	30fps
	Smart Coding - GOP control	Not available (Off)
Stream(3)	Stream Transmission	Off

Note

- When Stream (1) and Stream (2) are set to On, if the "Image capture size" for Stream (2) is set to "1280 x 720" ("1280 x 960"), the "Frame rate" for Stream (1) and Stream (2) will be "15 fps"/"12.5 fps"

WV-U2542L, WV-U2540L, WV-U2142L, WV-U2140L, WV-U1542L, WV-U1142

Settings Item		Settings(Default)
Image capture mode		16:9 (30fps mode)
Refresh interval (JPEG)*		1fps
JPEG(1)	Image capture size	2560x1440
JPEG(2)	Image capture size	640x360
Stream(1)	Stream Transmission	On
	Image capture size	2560x1440
	Frame rate	30fps
	Smart Coding - GOP control	Not available (Off)
	Smart Coding – AUTO VIQS	Not available (Off)
Stream(2)	Stream Transmission	On
	Image capture size	640x360
	Frame rate	30fps
	Smart Coding - GOP control	Not available (Off)
Stream(3)	Stream Transmission	Off

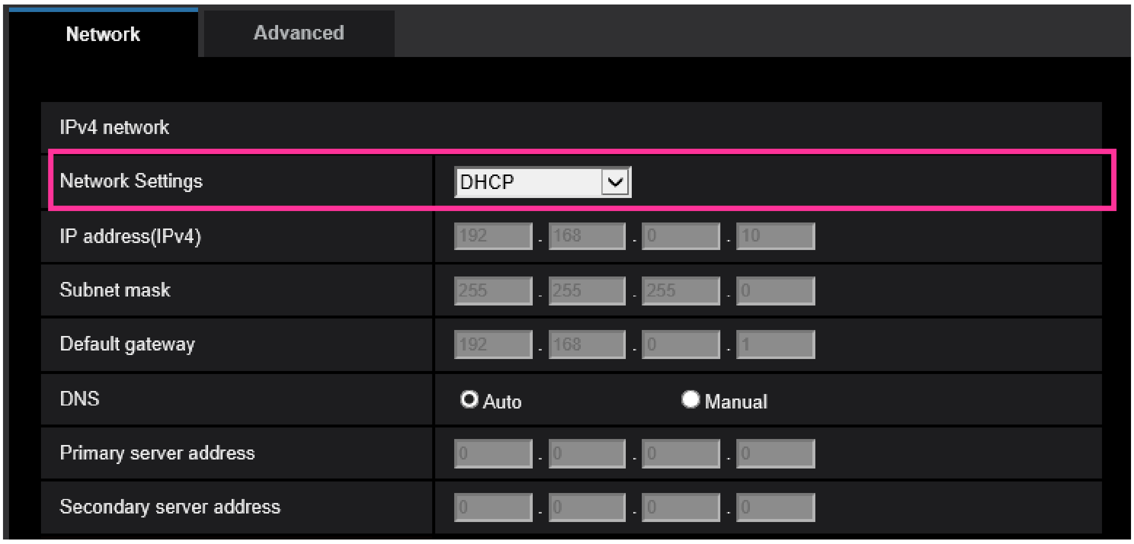
Note

- When Stream (1) and Stream (2) are set to On, if the "Image capture size" for Stream (2) is set to "1920 x 1080", the "Frame rate" for Stream (1) and Stream (2) will be "15 fps"/"12.5 fps".

5. Change the initial value of Network Settings and DHCP behavior in IPv4 network of Network

(Operating Instructions “Configuring the network settings” [Network]- “Configuring the network settings” [Network])

Change the initial value of Network Settings and DHCP behavior in IPv4 network of Network.



IPv4 network

Network Settings	DHCP
IP address(IPv4)	192 . 168 . 0 . 10
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 0 . 1
DNS	◉ Auto ○ Manual
Primary server address	0 . 0 . 0 . 0
Secondary server address	0 . 0 . 0 . 0

IPv4 network

[Network Settings]

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

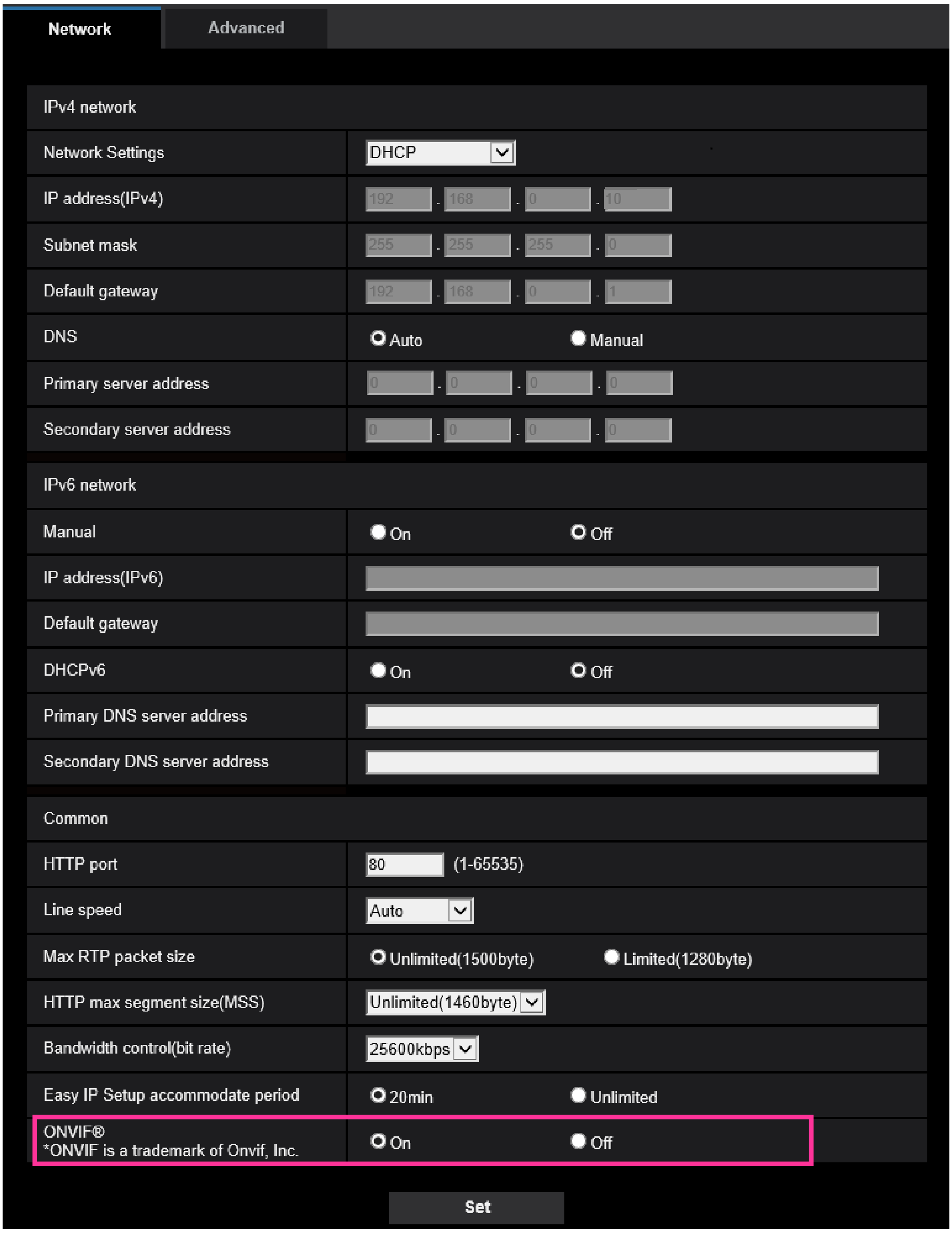
- **Static:** The IP address is configured by entering manually on “IP address(IPv4)”.
- **DHCP:** The IP address is configured using the DHCP function.
  If the camera cannot acquire an IP address from the DHCP server, set the IP address to 192.168.0.10.
  After that, once an IP address is acquired from the DHCP server, change it to that IP address.
- **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 camera as a static IP address. The configured IP address is automatically determined within the subnet mask range by the camera. When the DHCP server is not found, the IP address is set to 192.168.0.10.

- **Default:** DHCP

6. Add ONVIF® settings in Network

(Operating Instructions “Configuring the network settings” [Network]-“Configuring the network settings” [Network])

Add ONVIF® settings in the network settings.



IPv4 network	
Network Settings	DHCP
IP address(IPv4)	192 . 168 . 0 . 10
Subnet mask	255 . 255 . 255 . 0
Default gateway	192 . 168 . 0 . 1
DNS	○ Auto ● Manual
Primary server address	0 . 0 . 0 . 0
Secondary server address	0 . 0 . 0 . 0
IPv6 network	
Manual	● On ○ Off
IP address(IPv6)	
Default gateway	
DHCPv6	● On ○ Off
Primary DNS server address	
Secondary DNS server address	
Common	
HTTP port	80 (1-65535)
Line speed	Auto
Max RTP packet size	○ Unlimited(1500byte) ● Limited(1280byte)
HTTP max segment size(MSS)	Unlimited(1460byte)
Bandwidth control(bit rate)	25600kbps
Easy IP Setup accommodate period	○ 20min ● Unlimited
ONVIF® *ONVIF is a trademark of Onvif, Inc.	○ On ● Off

[ONVIF®]

Set the ONVIF to On/Off.

On: Enables the access from the ONVIF camera.

Off: Disables the access from the ONVIF camera

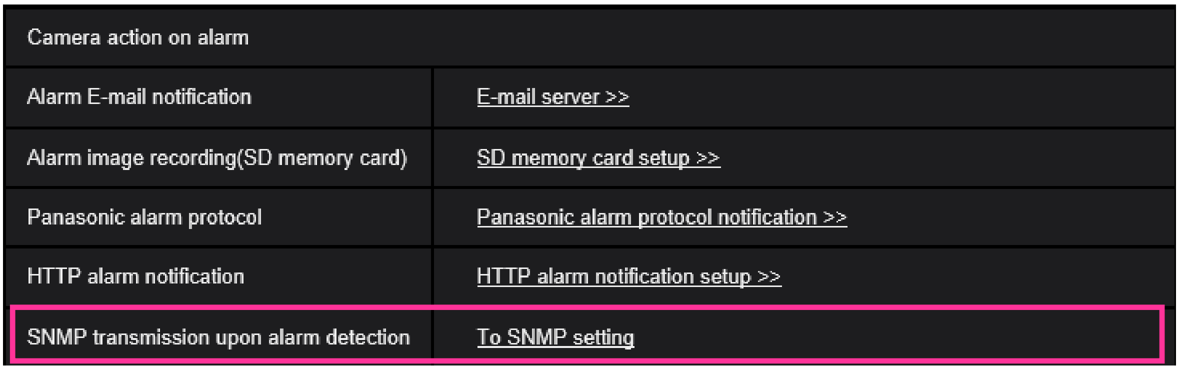
Default: On

*ONVIF is the trademark of ONVIF, Inc.

7. Added “SNMP transmission upon alarm detection” to “Camera action on alarm”

(Operating Instructions “Configure the alarm settings” [Alarm] - “Configure the settings relating to the camera action on alarm occurrence” [Alarm])

“SNMP transmission upon alarm detection” is newly added to the settings relating to the camera action on alarm.
Click “To SNMP setting” to display the setup menu that can configure the settings relating to SNMP transmission when an alarm occurs. The setup menu will be displayed in a newly opened window.
(→ 9. Added “SNMP trap setting” to “SNMP”)

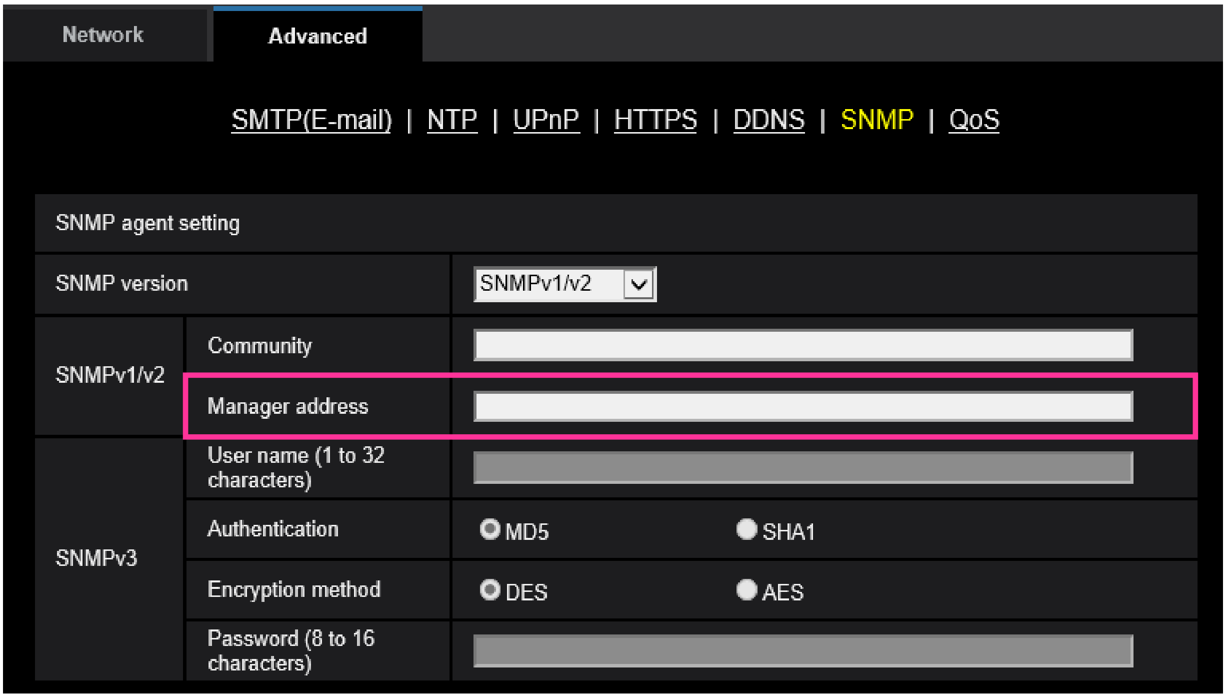


Camera action on alarm	
Alarm E-mail notification	E-mail server >>
Alarm image recording(SD memory card)	SD memory card setup >>
Panasonic alarm protocol	Panasonic alarm protocol notification >>
HTTP alarm notification	HTTP alarm notification setup >>
SNMP transmission upon alarm detection	To SNMP setting

8. Enhanced the access restriction function of SNMP v1/v2

(Operating Instructions “Configuring the network settings” [Network]
- “Configure advanced network settings” [Advanced]
- “Configure the settings relating to SNMP”)

The address range setting of the SNMP manager that receives requests from the camera is newly added.



SNMP agent setting		
SNMP version		SNMPv1/v2
SNMPv1/v2	Community	
	Manager address	
SNMPv3	User name (1 to 32 characters)	
	Authentication	◉ MD5 ○ SHA1
	Encryption method	◉ DES ○ AES
	Password (8 to 16 characters)	

- **[Manager address]**

Enter the IP address of the SNMP manager from which requests are to be permitted when the SNMP version is v1 or v2. When left blank, requests from all IP addresses will be permitted.

Note

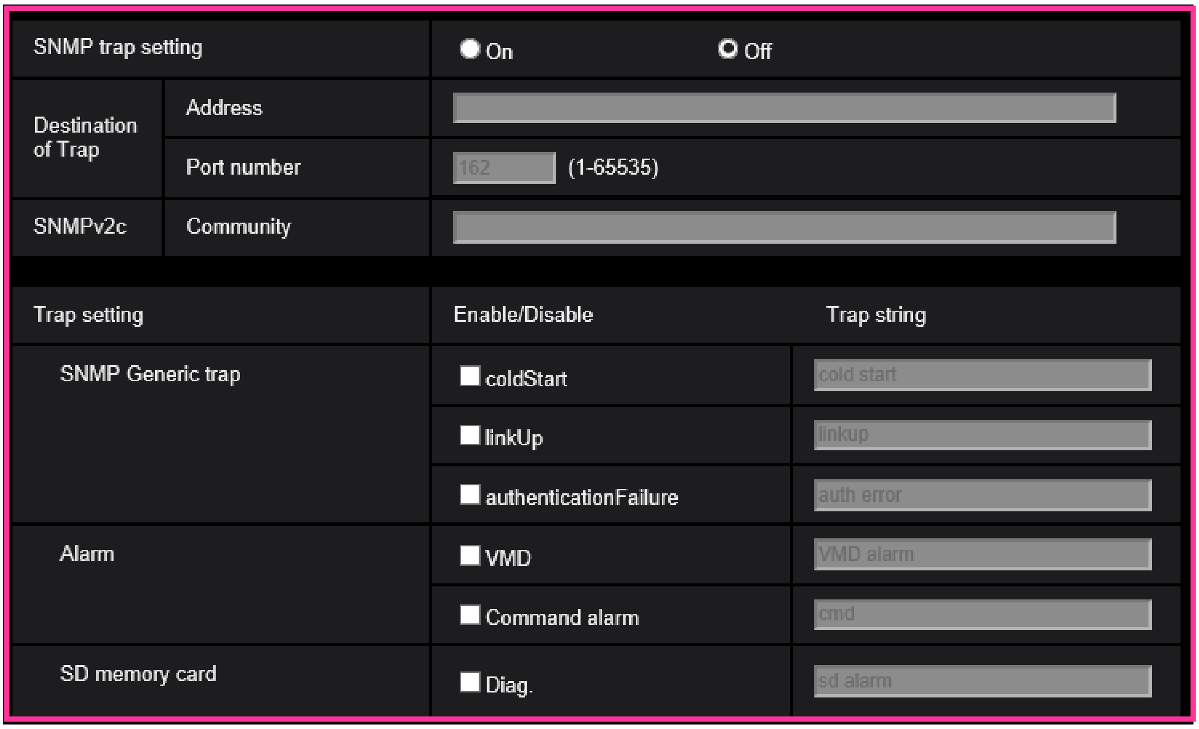
- When “IP address/subnet mask” is entered, it is possible to restrict IP address of SNMP manager from which request is permitted by subnet.
  For example, when “192.168.0.1/24” is entered, all requests from the SMNP managers in the range from “192.168.0.1” to “192.168.0.254” will be permitted.

Available number of characters: 0 - 128 characters
Available characters: Alphanumeric characters, the colon (:), the period (.) and the slash (/).
Default: None (blank)

9. Added “SNMP trap setting” to “SNMP”

(Operating Instructions “Configuring the network settings” [Network] - “Configure advanced network settings” [Advanced] - “Configure the settings relating to SNMP”)

“SNMP trap setting” is newly added to the settings relating to SNMP.
Configure settings relating to SNMP trap when an alarm occurs.



SNMP trap setting		○ On ● Off	
Destination of Trap	Address		
	Port number	162 (1-65535)	
SNMPv2c	Community		
Trap setting		Enable/Disable	Trap string
SNMP Generic trap		□ coldStart	cold start
		□ linkUp	linkup
		□ authenticationFailure	auth error
Alarm		□ VMD	VMD alarm
		□ Command alarm	cmd
SD memory card		□ Diag.	sd alarm

- **[SNMP trap setting]**
  Set On/Off of the SNMP trap.
  Default: Off

- **[Destination of Trap] - [Address]**
  Enter the destination address of the SNMP trap.
  Available number of characters: 0 - 128 characters
  Available characters: Alphanumeric characters, the colon (:) and the period (.).
  Default: None (blank)

- **[Destination of Trap] - [Port number]**
  Enter the port number of the destination address of the SNMP trap.
  Available port number: 1 - 65535
  Default: 162
  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, 443, 554, 995, 10669, 10670, 59000 - 61000

- **[SNMPv2c] - [Community]**
  Enter the community name of the destination address of the SNMP trap.
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: None (blank)

IMPORTANT

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

- **[SNMP Generic trap] - [coldStart] - [Enable/Disable]**
  When the check box is checked, a trap (SNMPv2-MIB::coldStart) will be sent.
  Default: Not checked (Disable)

- **[SNMP Generic trap] - [coldStart] - [Trap string]**
  When a camera startup trap is to be extended and sent, set the string of characters of the extended trap.
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: cold start

- **[SNMP Generic trap] - [linkUP] - [Enable/Disable]**
  When the check box is checked, a trap (SNMPv2-MIB:: linkup) will be sent at the time when the camera is linked up.
  Default: Not checked (Disable)

- **[SNMP Generic trap] - [linkUP] - [Trap string]**
  When a camera linkup trap is to be extended and sent, set the string of characters of the extended trap.
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: linkup

- **[SNMP Generic trap] - [authenticationFailure] - [Enable/Disable]**
  When the check box is checked, a trap (SNMPv2-MIB::coldStart) will be sent at the time when an SNMP authentication error occurs.
  Default: Not checked (Disable)

- **[SNMP Generic trap] - [authenticationFailure] - [Trap string]**
  When a SNMP authentication error occurrence trap is to be extended and sent, set the string of characters.
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: auth error

- **[Alarm] - [VMD] - [Enable/Disable]**
  When the check box is checked, a trap will be sent at the time when a video motion detection is activated.
  Default: Not checked (Disable)

- **[Alarm] - [VMD] - [Trap string]**
  Set the string of characters to be used for the trap of [VMD].
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: VMD alarm

- **[Alarm] - [Command alarm] - [Enable/Disable]**
  When the check box is checked, a trap will be sent at the time when a command alarm occurs.
  Default: Not checked (Disable)

- **[Alarm] - [Command alarm] - [Trap string]**
  Set the string of characters to be used for the trap of [Command alarm].
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: cmd

- **[SD memory card] - [Diag.] - [Enable/Disable]**
  When the check box is checked, a trap will be sent in the following cases.
  – When a notification of the remaining capacity of SD memory card has been provided
  – When the SD memory card has become full
  – When the SD memory card cannot be recognized
  Default: Not checked (Disable)

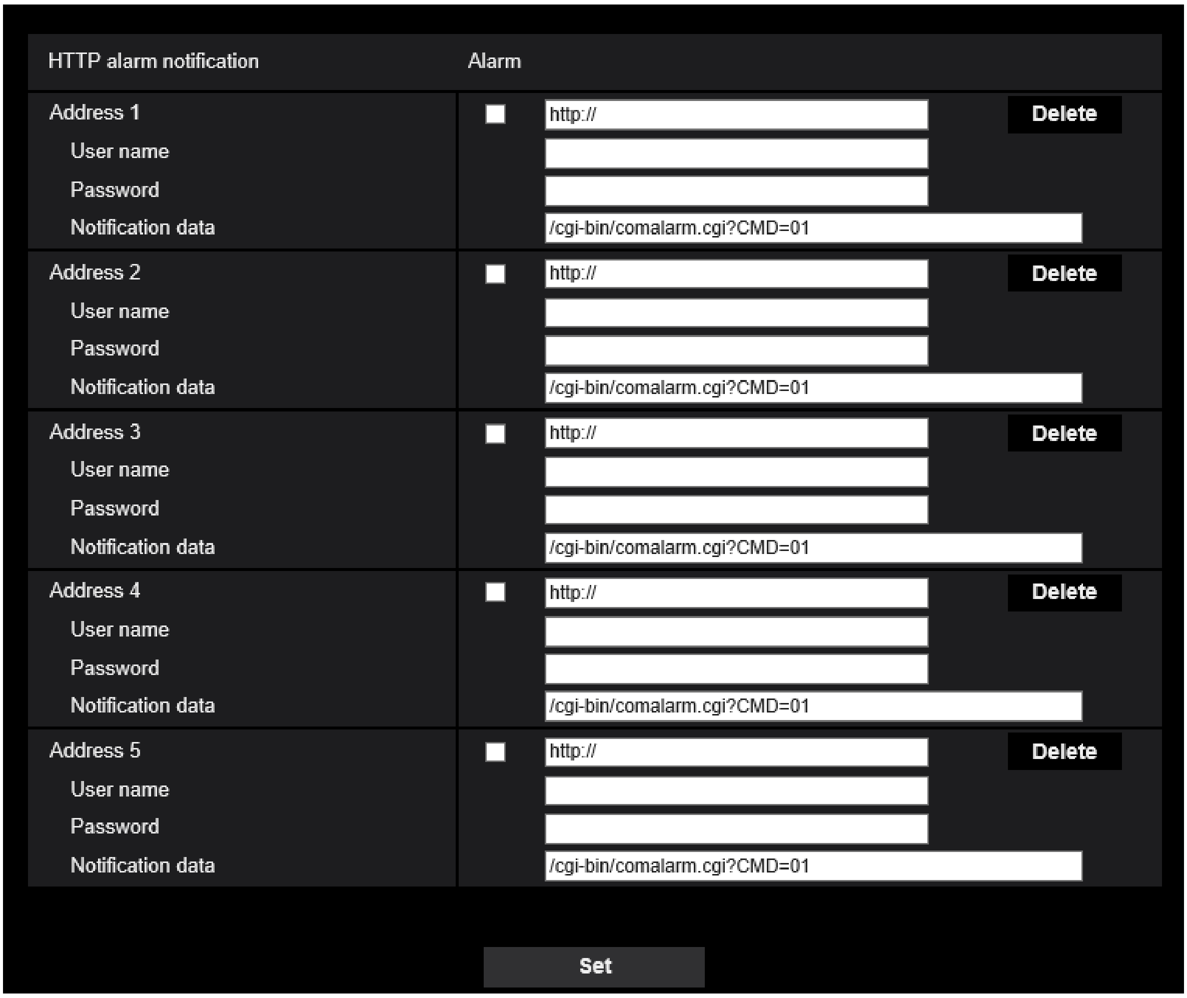
- **[SD memory card] - [Diag.] - [Trap string]**
  Set the string of characters to be used for the trap of [Diag.]
  Available number of characters: 0 - 32 characters
  Unavailable characters: 2-byte characters
  Default: sd alarm

10. Enable the HTTP alarm notification function to support the HTTPS communication and the Digest authentication

(Operating Instructions “Configure the alarm settings” [Alarm] – “Configuration of the settings relating to alarm notification” [Notification] – “Configure the settings relating to HTTP alarm notification”)

The HTTP alarm notification function is now supporting the HTTPS communication and Digest authentication.

- **HTTPS Communication**: Implement alarm notification over HTTPS communication by entering https:// in [Address].
- **Digest authentication**: Support Digest authentication with the HTTP server.



HTTP alarm notification	Alarm	
Address 1	□	http://
User name		
Password		
Notification data		/cgi-bin/comalarm.cgi?CMD=01
Address 2	□	http://
User name		
Password		
Notification data		/cgi-bin/comalarm.cgi?CMD=01
Address 3	□	http://
User name		
Password		
Notification data		/cgi-bin/comalarm.cgi?CMD=01
Address 4	□	http://
User name		
Password		
Notification data		/cgi-bin/comalarm.cgi?CMD=01
Address 5	□	http://
User name		
Password		
Notification data		/cgi-bin/comalarm.cgi?CMD=01

[Address 1] - [Address 5]

Enter the destination IP address or host name of the HTTP alarm notification. Up to 5 destination server addresses can be registered.

• Available characters: Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).

• Default: http://

Example of entry: “http://IP address of the HTTP server + : (colon) + port number” or
http://Host name: (colon)+ port number
“https://IP address of the HTTP server + : (colon) + port number” or
https://Host name: (colon)+ port number

[User name]

Enter the user name (login name) to access the HTTP server.

- **Available number of characters:** 0 - 63 characters
- **Unavailable characters:** " & : ; ¥

[Password]

Enter the password to access the HTTP server.

- **Available number of characters:** 0 - 63 characters
- **Unavailable characters:** " &

Note

- Basic authentication or Digest authentication is performed on authentication request of the HTTP server.

11. Add to the system log when authentication fails for the HTTP alarm notification function

(Operating Instructions “Others” – “About the displayed system log”)

When the HTTP server user authentication fails, an error is added to "Error indications relating to HTTP alarm notification".

Category	Indication	Description
HTTP alarm notification	Authentication error	• Entered user name or password may be incorrect. Check if the HTTP alarm notification settings are configured correctly.

12. Add a notify to the [SNMP trap setting]

(Operating Instructions Configure the network settings [Network] – Configure advanced network settings [Advanced])

Add the notifications to [SNMP trap settings].

Note

- In order to activate SNMP trap notifications for when alarms occur, alarm operation settings are required.
  For information on settings related alarm operations, refer to Configure the alarm settings [Alarm] in Operating Instructions.

13. Add to the system log when recording stream fails to write

(Operating Instructions “Others” – “Maintenance” - Check the status [Status])

A system log has been added for errors in the write process of the recording stream to the log related to SD memory cards.

Category	Indication	Description
SD memory card	<SD>Format	Successfully formatted the SD memory card.
	<SD>Format error	Error occurred when formatting the SD memory card.
	<SD> Write-protect ON (Locked card)	A write-protected SD memory card is inserted.
	<SD> Detection error	The SD memory card could not be correctly recognized.
	<SD> Write error	An error occurred when writing to the SD memory card.
	<SD> Read error	An error occurred when reading from the SD memory card.
	<SD> Delete error	An error occurred when deleting data from the SD memory card.
	<SD> File system error	An error occurred in File system of the SD memory card.
	<SD> Undefined error	An error other that the ones above has occurred for the SD memory card.
	<SD> An abnormality occurs in continuity of the SD memory recording. Check the recording bit rate setting of the SD memory recording.	An error occurred when writing to the SD memory card.
	<SD> An error occurs in the SD memory card. Check the status of the SD memory card.	The SD memory card write process still generates data loss. Make sure that the SD memory card is properly recognized. If the card is not recognized, reboot the unit, or remove and reinsert the SD memory card to check.

14. Add a function to notify the user of writing failures in the recording stream with a unique alarm

(Operating Instructions “Others” – “Maintenance” - Configure the alarm settings [Alarm])

ーConfiguration of the settings relating to alarm notification［Notification］ー

Configure the settings relating to Panasonic alarm protocol)

Add the write processing error of the recording stream to the occurrence condition of the Panasonic alarm protocol notification of “Diag.”

Panasonic alarm protocol

•［Panasonic alarm protocol］

Select “On” or “Off” to determine whether or not to provide notification by Panasonic alarm protocol according to the settings for the “Alarm” and “Diag.” checkboxes of “Destination of notification” below.

- When an alarm is detected (“Alarm”)
- When a notification of the remaining capacity of the SD memory card has been provided (“Diag.”)
- When the SD memory card has become full (“Diag.”)
- When the SD memory card cannot be recognized (“Diag.”)
- <u>When there is a write error on the SD memory card (“Diag.”)</u>

Default: Off

Destination of notification

• [Address 1] - [Address 8]

Enter the destination IP address or host name of the Panasonic alarm protocol from the following.

Up to 8 destination server addresses can be registered.

[Alarm] checkbox: When the checkbox is checked, the Panasonic alarm notification will be provided upon an alarm occurrence.

[Diag.] checkbox: When the checkbox is checked, notification using Panasonic alarm protocol will be provided in the following cases.

– When notification of the remaining capacity of the SD memory card has been provided

– When the SD memory card has become full

– When the SD memory card cannot be recognized

– When the SD memory card cannot be written

[Destination server address]: Enter the destination server address or host name.

Available characters: Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-).

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

15. Add a note when the bit rate of the recording stream is set to a value exceeding recommended value

(Operating Instructions “Image” - Configure the settings relating to Stream [Image]

Add the statement that it is possible that an error may occur in the continuity of SD memory card recording, if you set a bit rate that exceeds the recommended value in “Note” of “Max bit rate (per client) *”.

[Max bit rate (per client)*]:

Note

• The bit rate for “Stream” is restricted by “Bandwidth control (bit rate)” on the [Network] tab on the “Network” page. When a value with “*” attached is set, images may not be streamed.

• It is recommend that the bit rate setting of the stream to be 6144 kbps or lower. Setting a value higher than 6144 kbps may cause abnormalities in the continuity of the recorded video.

• When the refresh interval is too short, the actual bit rate may exceed the set bit rate depending on the subject.

• Depending on the number users connecting at the same time or the combination of features used, the bit rate may be lower than the configured value. Check the transmission of images after changing settings.

16. Extend authentication password for the destination of notification

(Operating Instructions – Configure the network settings [Network] – Configure advanced network settings [Advanced] - Configure the settings related to sending E-mails)

The number of characters that can be entered for the authentication password of the destination of notification has been expanded to 128 characters.

- ［**Authentication − Password**］

Enter the password to access the server.

Available number of characters: 0 - 128 characters

Unavailable characters: " &

17. Change the initial value of “Overwrite” of SD memory card to On

(Operating Instructions – Configure the basic settings of the camera [Basic]) – Configure the settings relating to the SD memory card [SD memory card])

[Overwrite]

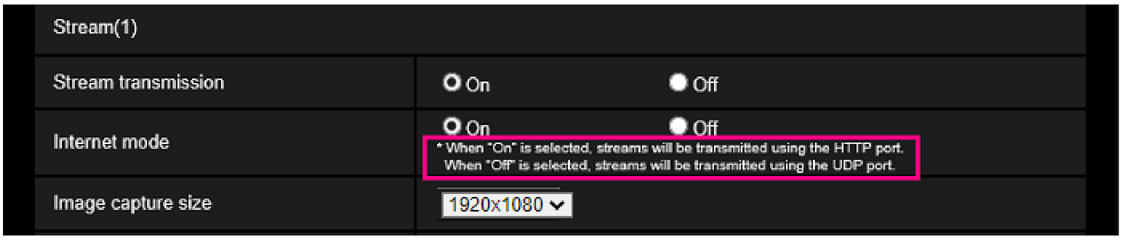
Determine whether or not to overwrite when the remaining capacity of the SD memory card becomes insufficient.

- **On:** Overwrites when the remaining capacity of the SD memory card becomes insufficient. (The oldest image is the first to be overwritten.)
- **Off:** Stops saving images on the SD memory card when the SD memory card becomes full.
- **Default:** On

18. Add the supplementary explanation of On/Off of Internet mode to the setting screen

(Operating Instructions – Configure the settings relating to images [Image] – Configure the settings relating to Stream [Image])

Add the supplementary explanation of On/Off of Internet mode setting.



Stream(1)	
Stream transmission	◉ On ○ Off
Internet mode	◉ On ○ Off * When "On" is selected, streams will be transmitted using the HTTP port. When "Off" is selected, streams will be transmitted using the UDP port.
Image capture size	1920x1080

[Internet mode]

Select “On” when transmitting H.265 images via the Internet. It is possible to transmit stream without changing the broadband router settings configured for JPEG image transmission.

- **On:** H.265 images will be transmitted using the HTTP port. Refer to [HTTP port] for further information about the HTTP port number settings.
- **Off:** H.265 images will be transmitted using the UDP port.
- **Default:** On

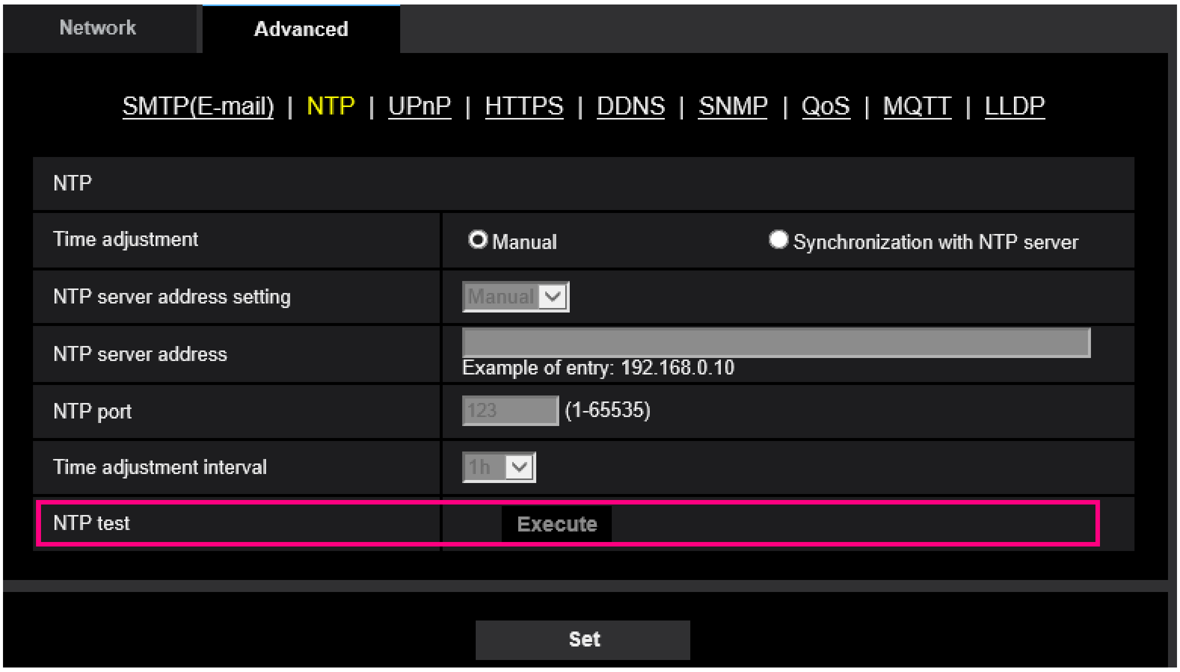
<u>**Note**</u>

- When “On” is selected, only “Unicast port (AUTO)” will be available for “Transmission type”.
- When “On” is selected, it may take time to start displaying stream images.
- When “On” is selected, stream images may not be displayed depending on the number of the concurrent access user, etc.
- When “On” is selected, only IPv4 access is available.

19. Add NTP test function

(Operating Instructions – Configuring the network settings [Network] – Configure advanced network settings [Advanced] – Configure the settings relating to the NTP server)

Add a test function for time synchronization to check if it can communicate with NTP server.



Network
Advanced
SMTP(E-mail) | NTP | UPnP | HTTPS | DDNS | SNMP | QoS | MQTT | LLDP
Execute
Set

NTP	
Time adjustment	● Manual ○ Synchronization with NTP server
NTP server address setting	Manual
NTP server address	Example of entry: 192.168.0.10
NTP port	123 (1-65535)
Time adjustment interval	1h
NTP test	Execute

[NTP test]

Select “Synchronization with NTP server” for “Time adjustment”, set the NTP server information, and then click the “Execute” button. You can communicate with the NTP server, synchronize the time, and check the NTP operation.

Note

・If the NTP test succeeds, “NTP time correction has succeeded.” is displayed.

・If the NTP test fails, “NTP time correction has failed.” is displayed.

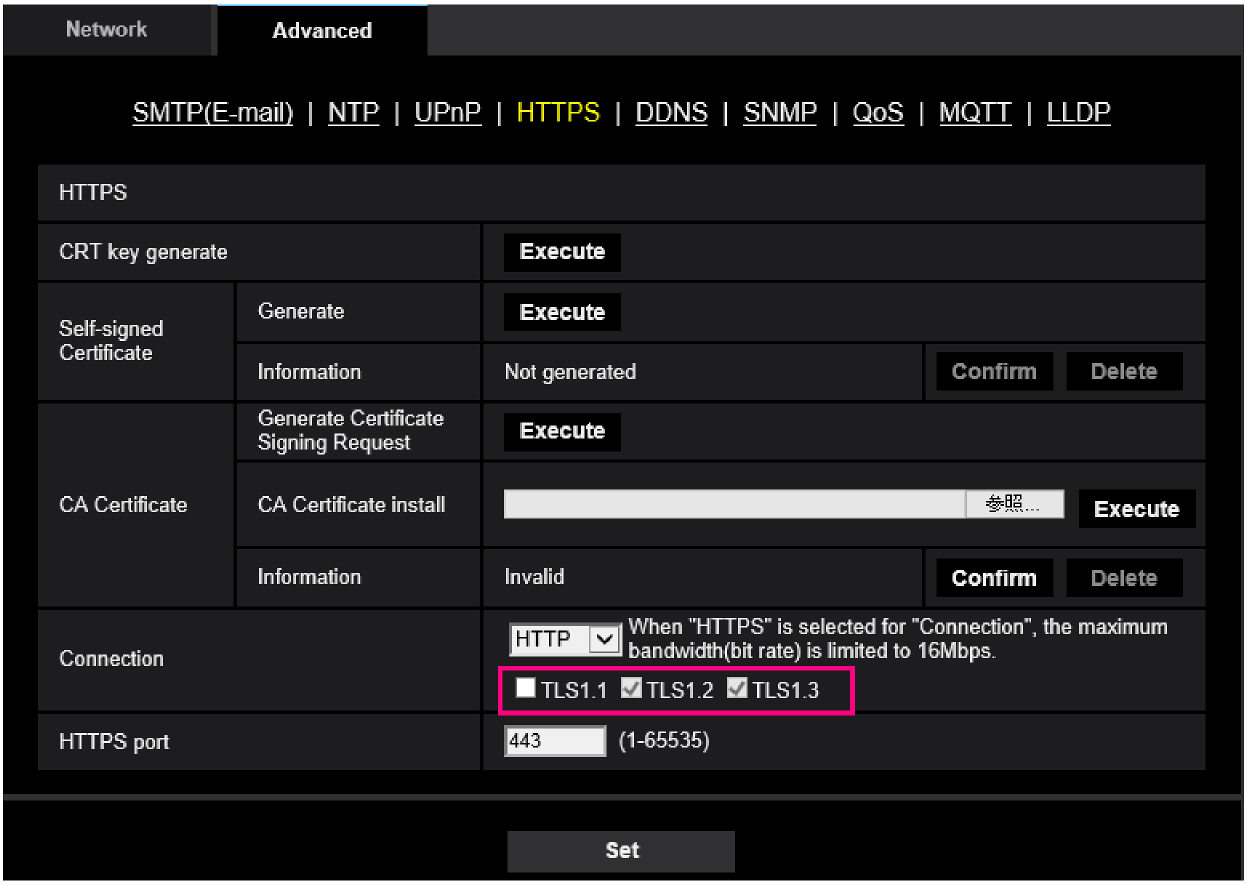
・When “Time adjustment” is set to “Manual”, the “Execute” button of NTP test is grayed out.

・When “Time adjustment” is set to “Synchronization with NTP server” and the “NTP server address” is not set, the “Execute” button for the NTP test will be grayed out.

20. Add TLS settings to HTTPS

(Operating Instructions – Configuring the network settings [Network] – Configure advanced network settings [Advanced] – Configure the HTTPS settings)

Add TLS1.1, TLS1.2 and TLS1.3 selection items to the HTTPS connection method.


Network
Advanced
SMTP(E-mail) | NTP | UPnP | HTTPS | DDNS | SNMP | QoS | MQTT | LLDP
Set

HTTPS			
CRT key generate		Execute	
Self-signed Certificate	Generate	Execute	
	Information	Not generated	Confirm Delete
CA Certificate	Generate Certificate Signing Request	Execute	
	CA Certificate install	参照...	Execute
	Information	Invalid	Confirm Delete
Connection		HTTP When "HTTPS" is selected for "Connection", the maximum bandwidth(bit rate) is limited to 16Mbps. □ TLS1.1 ☑ TLS1.2 ☑ TLS1.3	
HTTPS port		443 (1-65535)	

[HTTPS - Connection]

Select the protocol used to connect the camera.

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

Select the TLS to use when HTTPS is selected.

- **TLS1.1**: Enable/Disable.
- **TLS1.2**, **TLS1.3**: Always enabled and cannot be disabled.
- **Default: TLS1.1**:Disabe、**TLS1.2**: Enable, **TLS1.3**: Enable

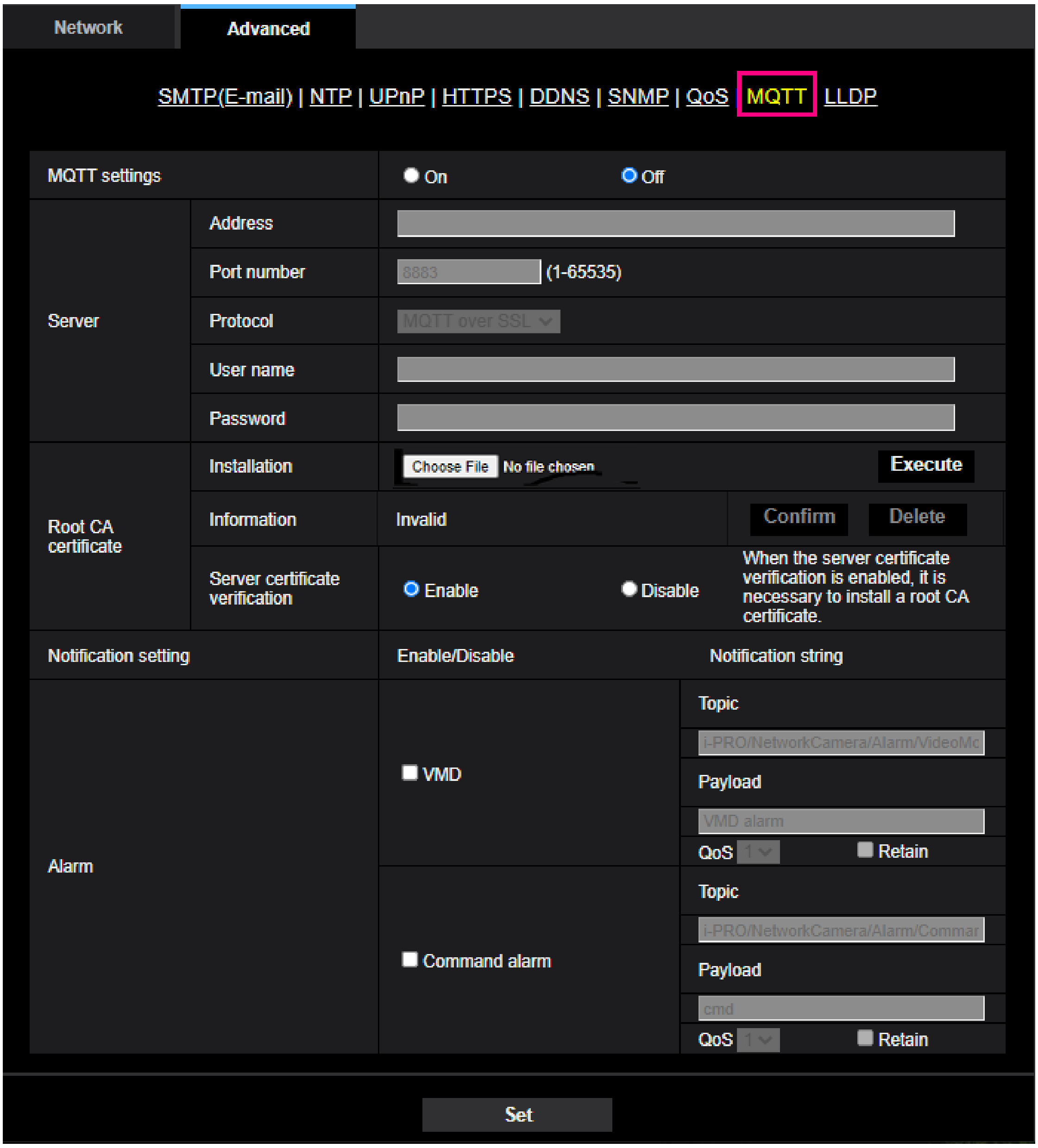
Note

• To change to an HTTPS connection when HTTP is selected, perform HTTPS connection settings first. The HTTPS connection will be available even if the setting is changed to HTTP afterwards.

21. Add MQTT function

(Operating Instructions – Configuring the network settings [Network] – Configure advanced network settings [Advanced])

MQTT (Message Queueing Telemetry Transport) has been added to “Advanced” of “Network”. When an alarm occurs, the MQTT server can be notified of the event action by the alarm.



Network | Advanced

SMTP(E-mail) | NTP | UPnP | HTTPS | DDNS | SNMP | QoS | MQTT | LLDP

MQTT settings		○ On	● Off
Server	Address		
	Port number	8883 (1-65535)	
	Protocol	MQTT over SSL	
	User name		
	Password		
Root CA certificate	Installation	Choose File No file chosen	Execute
	Information	Invalid	Confirm Delete
	Server certificate verification	● Enable ○ Disable	When the server certificate verification is enabled, it is necessary to install a root CA certificate.
Notification setting		Enable/Disable	Notification string
Alarm		□ VMD	Topic i-PRO/NetworkCamera/Alarm/VideoMc Payload VMD alarm QoS 1 □ Retain
		□ Command alarm	Topic i-PRO/NetworkCamera/Alarm/Commar Payload cmd QoS 1 □ Retain

Set

[MQTT settings]

Set On/Off whether to enable/disable the MQTT function.

When set to On, or it is On when the camera starts up, it will connect to the set server.

When the set alarm occurs, the settings will be notified to the server.

Default: Off

Server

[Address]

Enter the IP address or host name of the MQTT server to be notified when an alarm occurs.

Available number of characters: 1 - 128 characters

Available characters: Alphanumeric characters, the colon (:), the period (.), the underscore (_), and the hyphen (-)

Default: None (blank)

[Port]

Enter the port number of the MQTT server.

Available port number: 1 - 65535

Default: 8883

The following port numbers cannot be set because they are used by this product.

20, 21, 23, 25, 42, 53, 67, 68, 69, 80, 110, 123, 161, 162, 443, 554, 995, 10669, 10670

[Protocol]

Select the protocol to use when connecting to an MQTT server from MQTT over SSL/MQTT over TCP.

Default: MQTT over SSL

[User name]

Enter the user name to access the MQTT server.

Available number of characters: 0 - 32 characters

Unavailable characters: " & : ; ¥

[Password]

Enter the password to access the MQTT server.

Available number of characters: 0 - 32 characters

Unavailable characters: " &

Root CA certificate

[Install]

Install the root CA certificate issued by the certification authority.

In the "Open File Dialog" that appears when you click the [Select File] button, select the root CA certificate file issued by the certification authority, and then click the [Execute] button to install the root CA certificate.

The data format of the root CA certificate is PEM format or DER format.

[Information]

The root CA certificate information is displayed.

Invalid：The root CA certificate is not installed.

Root CA certificate host name：Indicates that the certificate is installed.

［Confirm］The details of CA certificate can be checked with the button.

［Delete］The CA certificate will be deleted with the button.

[Server certificate verification]

When [Protocol] is set to "MQTT over SSL" and [Server certificate verification] is set to "Enable", the server certificate is verified using the root CA certificate registered during the SSL connection.

Default：Enable

Note

・When [Server certificate verification] is set to " Enable", install the root CA certificate.

Notification setting

[Alarm]

Check the alarm events to be notified to the MQTT server.

VMD: Notifies the MQTT server when motion detection occurs.

Command alarm: Notifies the MQTT server when a command alarm is entered.

[Topic]

Set the MQTT topic name to be sent. Topics have a hierarchical structure separated by "/".

Available number of characters: 1 - 128 characters

Available characters: Alphanumeric characters, "/"

Default:

VMD: i-PRO/NetworkCamera/Alarm/VideoMotionDetection
Command alarm: i-PRO/NetworkCamera/Alarm/Command

[Payload]

Set the MQTT message payload.

Available number of characters: 1 - 128 characters

Available characters: Alphanumeric characters

Default:

VMD: VMD alarm
Command alarm: cmd

[QoS]

Select the QoS level from 0, 1, 2.The communication quality improves in the order of 0<1<2.

0: The message is delivered at most once with QoS0. There is no guarantee that the message will reach the server.

1: The message is delivered at least once with QoS1. The message is guaranteed to reach the destination, but may be duplicated.

2: The message is delivered exactly once with QoS2. It guarantees that the message arrives just once.

Default: 1

[Retain]

Check this box if you want the MQTT server to save the last notified message.

Default: Unchecked

22. Add a system log when MQTT function fails

(Operating Instructions – Others – About the displayed system log)

Add a system log when an error occurs in the MQTT function.

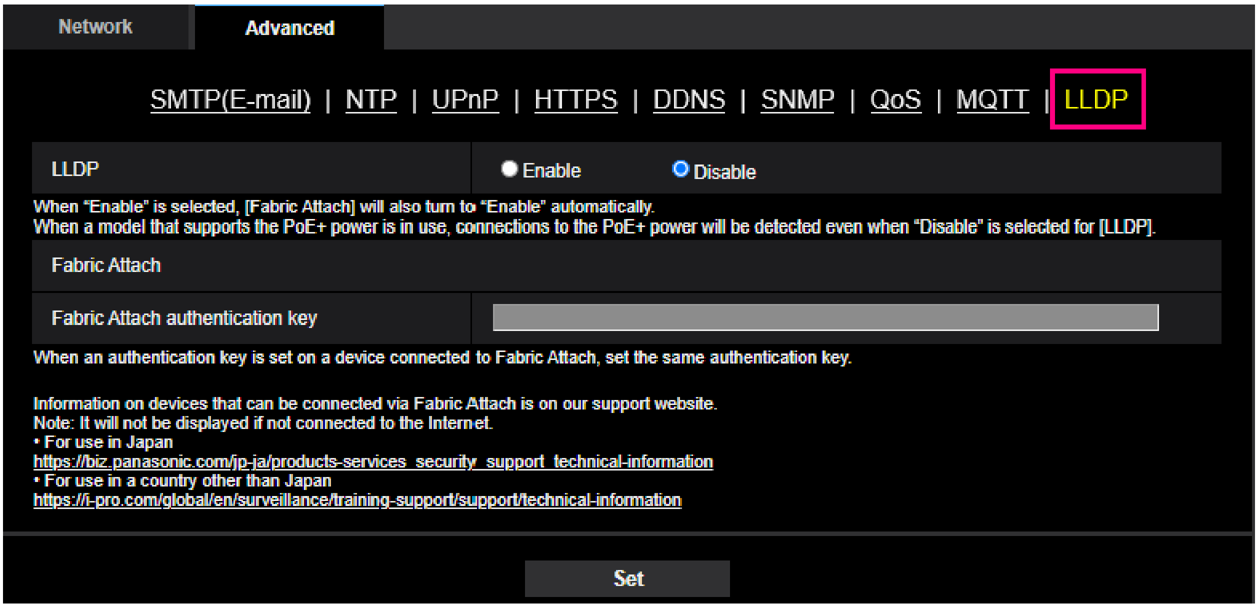
Error display related to MQTT

Category	Indication	Description
MQTT	<MQTT> Connection error	When the connection to the server fails, certification verification fails, or is disconnected (except for disconnections from the camera due to setting change)
	<MQTT> Notification error	When publishing to the server fails

23. Add LLDP function

(Operating Instructions – Configuring the network settings [Network] – Configure advanced network settings [Advanced])

LLDP (Link Layer Discovery Protocol) has been added to [Advanced] of [Network]. Interoperability can be achieved by sending and receiving camera's device information to and from LLDP-compatible devices.


Network
Advanced
SMTP(E-mail) | NTP | UPnP | HTTPS | DDNS | SNMP | QoS | MQTT | LLDP
Set

LLDP ○ Enable ● Disable

When "Enable" is selected, [Fabric Attach] will also turn to "Enable" automatically.
When a model that supports the PoE+ power is in use, connections to the PoE+ power will be detected even when "Disable" is selected for [LLDP].

Fabric Attach

Fabric Attach authentication key

When an authentication key is set on a device connected to Fabric Attach, set the same authentication key.

Information on devices that can be connected via Fabric Attach is on our support website.
Note: It will not be displayed if not connected to the Internet.
• For use in Japan
https://biz.panasonic.com/jp-ja/products-services_security_support_technical-information
• For use in a country other than Japan
https://i-pro.com/global/en/surveillance/training-support/support/technical-information

[LLDP]

Enable/Disable whether to enable the LLDP function and Fabric Attach.

Default: Disable

When set to "Enable", LLDP including TLVs with the checks in the table below will be sent.

End Of LLDPDU TLV	Chassis ID TLV	Port ID TLV	Time To Live TLV	Port Description TLV	System Name TLV	System Description TLV	System Capability TLV	Management Address TLV	IEEE802.3 Power via MDI TLV	Fabric Attach Element TLV
✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

* Models that support PoE+ power supply will send LLDP including TLVs with the checks in the table below for PoE+ power supply even if set to "Disable".

End Of LLDPDU TLV	Chassis ID TLV	Port ID TLV	Time To Live TLV	Port Description TLV	System Name TLV	System Description TLV	System Capability TLV	Management Address TLV	IEEE802.3 Power via MDI TLV	Fabric Attach Element TLV
✓	✓	✓	✓						✓	

Fabric Attach

[Fabric Attach authentication key]

Enter the key to be used for Fabric Attach authentication. Note that this is valid only when “LLDP” is “Enable”.

Available number of characters: 0 - 32 characters (If Fabric attach authentication is not performed, leave it blank.)

Available characters: Alphanumeric characters

Default: None (blank)

Note

- Click the [Set] button to restart the product. After restarting, the product cannot be operated for about 2 minutes, just like when the power is turned on.
- For information about devices that can be connected using Fabric Attach, refer to our support website.

  https://i-pro.com/global/en/surveillance/training-support/support/technical-information