Canon

Network Camera

Network Operation Guide

ME20F-SHN

HDMI

This User Manual should be read before using the network camera.

ENGLISH

Introduction

This “Network Operation Guide” explains the camera settings and operations to be performed when using the camera via a network. Read "Setup Guide" first to complete the setup of the camera, and then read this guide carefully before using the camera to ensure correct use.

Network Security

The user is responsible for the network security of this product and its use.
Take appropriate network security measures to avoid security breaches. To the full extent permitted by laws and regulations, neither Canon Inc. nor any of its subsidiaries or affiliates shall be liable for any losses, direct, incidental or consequential damages, or liabilities that may be incurred as a result of network security incidents such as unauthorized accesses.

<Network Security Recommendations>

- Register a strong administrator password that cannot be easily guessed by a third party.
- Change the HTTP or HTTPS port number of the camera.
- Limit access to the camera by network devices.

License Agreement of Software

For the license agreement of the software, please refer to the text file provided along with the installer.

This product is licensed under AT&T patents for the MPEG-4 standard and may be used for encoding MPEG-4 compliant video and/or decoding MPEG-4 compliant video that was encoded only (1) for a personal and non-commercial purpose or (2) by a video provider licensed under the AT&T patents to provide MPEG-4 compliant video. No license is granted or implied for any other use for MPEG-4 standard.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (''AVC VIDEO'') AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE **HTTP://WWW.MPEGLA.COM**

Trademarks

- Microsoft, Windows, Internet Explorer, Windows Server, Surface and ActiveX are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Windows is legally recognized as the Microsoft Windows Operating System.
- This product comes with exFAT, a licensed file system technology from Microsoft.
- IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.
- Android is a trademark of Google LLC.
- microSD, microSDHC and microSDXC logos are trademarks of SD-3C, LLC.
- HDMI, the HDMI logo and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.
- ONVIF® is a trademark of Onvif, Inc.
- All other company or product names used in this manual are trademarks or registered trademarks of their respective holders.

Open Source Software

The camera contains Open Source Software modules. Confirm each modules license conditions in [Maintenance] > [General] > [Tool] > [View License] on the Setting Page.

Software under GPL and LGPL

If you would like to obtain the source code under GPL/LGPL, please contact us at nvsossg@canon.co.jp and provide the following information in English or Japanese:

1. Product name and firmware version.
2. Name of the software module or modules you would like to obtain.

You can obtain the source code for at least three years from the day you purchased this product. Please note we may bill you for any costs we incur in providing you the source code.

User Manuals

Notes

1. Any unauthorized reproduction of this guide is prohibited.
2. The contents of this guide are subject to change without any prior notice.
3. This document has been prepared with the utmost attention to accuracy. If you have any comments, however, please contact a Canon sales representative.
4. Canon shall assume no liability for any outcome of using this product, notwithstanding items 2 and 3 above.

How to Use This Operation Guide

The assumed reading format of this operation guide is on a computer screen.

Software Screenshots

The software screenshots samples shown in this guide are for illustration only. The screenshots may differ from the actual screens displayed.
In the descriptions, sample screens connected to a camera are generally used, with Windows 10 being used as the operating system and Internet Explorer 11 as the web browser.

Symbols Used in This Guide

Symbols Indicating Safety Precautions

This section explains the symbols used in this guide. The following symbols used in this guide indicate information for safe use of the product, as well as important and supplemental information the user should know. Be sure to read and understand this information when using the product.

Symbol	Meaning
Caution	Failure to follow the instructions indicated by this symbol may result in property damage. Be sure to follow these precautions.
Important	Cautions and restrictions during operation. Make sure to read these carefully.
Note	Supplementary descriptions and reference information.

Table of Contents

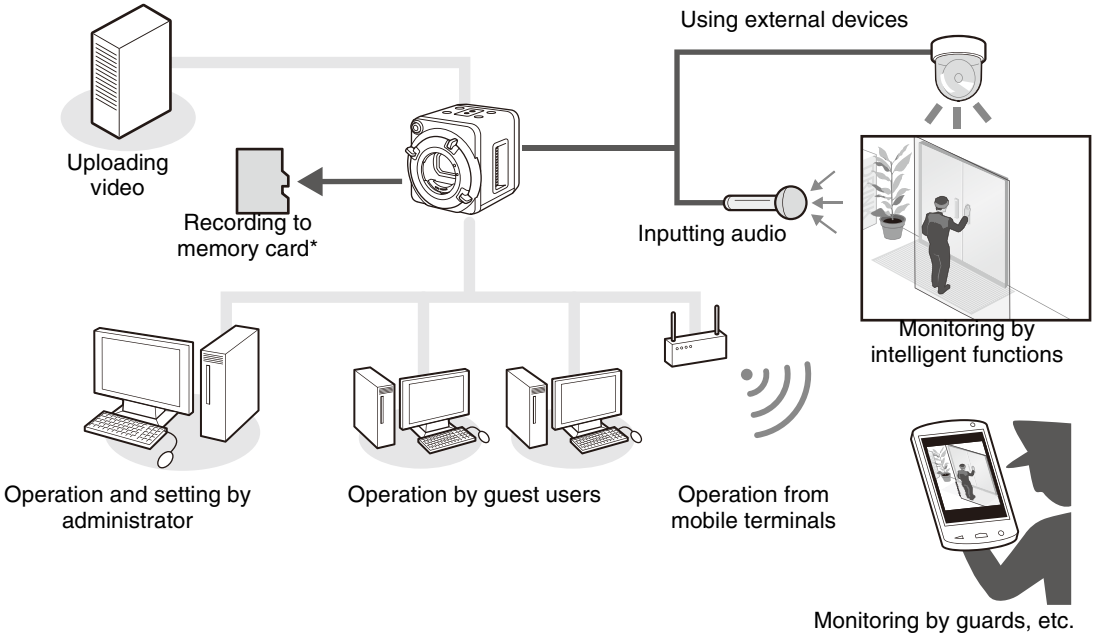
Chapter 1

Before Use

This chapter explains the camera functions, software and operating environment.
It also describes the flow from preparation and setup through to actual use.

Functions of the Network Camera

A network camera not only enables you to operate the camera, but also allows you to record and upload the video, and perform monitoring using the various intelligent functions of the camera.
The figure below shows examples of what the camera can do via a network.



* In this guide, “memory card” refers to the various types of memory cards that can be used with the camera.

Camera Software

The following software is available for efficiently configuring and operating the camera.

Camera Operations and Settings

Camera operations are performed using the Camera Viewer/Mobile Camera Viewer.
Camera settings are specified from the Setting Page.

Camera Viewer (P. 29) /Mobile Camera Viewer

Controls the camera, and monitors video and various events.
You can use the Camera Viewer (mainly for computers) and the Mobile Camera Viewer (mainly for devices with a screen size of 7 inches or less).
The functions available in the Viewer differ according to the user authority (P. 33).

Note

For details on using Mobile Camera Viewer, please refer to “Mobile Camera Viewer Operation Guide”.

Setting Page (P. 61)

The Setting Page is for the administrator to configure and manage the camera.

Software to Install on the Computer

The following software can be installed on the computer to be used.

Note

.NET Framework 3.5 SP1 (when using Internet Explorer 9) or .NET Framework 4.5 (when using Internet Explorer 10/11) is necessary to use Camera Management Tool and Recorded Video Utility.
If it is not installed on the computer, it will be automatically installed when using the installer (P. 20).

Camera Management Tool

This tool is used for batch managing multiple cameras, from initial settings to performing maintenance. The Camera Management Tool can perform the following tasks.

- Detecting cameras
- Set various camera settings.
- Display the Viewer and the Setting Page.
- Update firmware, back up/restore settings, perform memory card and other operations, as well as camera maintenance.

For details on uses and functions, please refer to “Camera Management Tool User Manual”.

The Camera Management Tool can be installed from the installer.
Installer name: VBToolsInstall.exe

Recorded Video Utility

This utility is used for viewing and managing the videos recorded on the memory card mounted in the camera. The Recorded Video Utility enables you to perform the following operations on recorded videos.

- Displaying a list of videos
- Playing and deleting videos
- Downloading videos to a computer

For details on using the utility and its functions, please refer to “Recorded Video Utility User Manual”.

The Recorded Video Utility can be installed from the installer.

Installer name: VBToolsInstall.exe

Additional Software/Licenses (Sold Separately)

You can purchase additional software and licenses as necessary.

Canon H.264 Additional User License AUL-VB

Additional license for viewing H.264 video with multiple computers via the Viewer or Recorded Video Utility. Each camera includes one license. Additional licenses are necessary for multiple computers to view H.264 video from a single camera.

Operating Environment

For the latest information on this product (firmware and software, user manual, operating environment, etc.), please refer to the Canon website.

PC Environment Details

CPU (Recommended)	Intel Core i7-2600 or higher	
Graphics Board (Recommended)	Not specified	
Memory (Recommended)	2 GB or higher	
Viewer Display (Recommended)	1920 x 1080 or higher	
OS and Compatible Web Browser	Windows 7 Ultimate/Windows 7 Professional/ Windows 7 Enterprise/Windows 7 Home Premium SP1 32/64-bit	Internet Explorer 11 32/64-bit, Chrome 74*2
	Windows 8.1/Windows 8.1 Pro/Windows 8.1 Enterprise 32/64-bit*1	Internet Explorer 11 32/64-bit, Chrome 74*2
	Windows 10 Pro/Windows 10 Enterprise/Windows 10 Education/Windows 10 Home 32/64-bit	Internet Explorer 11 32/64-bit, Chrome 74*2
	Windows Server 2008 Standard SP2 32/64-bit	Internet Explorer 9 32-bit
	Windows Server 2008 R2 Standard SP1 64-bit	Internet Explorer 11 32/64-bit, Chrome 74*2
	Windows Server 2012 Standard 64-bit*1	Internet Explorer 10 32/64-bit, Chrome 74*2
	Windows Server 2012 R2 Standard 64-bit*1	Internet Explorer 11 32/64-bit, Chrome 74*2
	Windows Server 2016 Standard 64-bit	Internet Explorer 11 64-bit, Chrome 74*2
	Windows Server 2019 Standard 64-bit	Internet Explorer 11 64-bit
	– Must be configured to allow use of JavaScript, IFRAME (html tag), and web storage – For Camera Viewer only, cookies must be enabled	
Operating System Language	Setting Page, Camera Viewer, Mobile Camera Viewer: German/English/Spanish/French/Italian/Russian/Turkish/Japanese	

*1 Cannot be started from the Windows start screen

*2 Does not support playback of Video (H.264) or audio transmission/reception

Note

- For information on the operating environment of the Camera Management Tool, please refer to “Camera Management Tool User Manual”.
- For information on the operating environment of the Recorded Video Utility, please refer to “Recorded Video Utility User Manual”.

Mobile Environment Details (Setting Page, Camera Viewer, Mobile Camera Viewer)

OS	Web Browser	Reference
iOS 12.2 iOS 11.4.1	Safari	– Must be configured to allow use of JavaScript, and web storage – For Camera Viewer only, cookies must be enabled – Does not support playback of Video (H.264) or audio transmission/ reception – Setting Page and Camera Viewer are not supported for the mobile device where the display size is smaller than 7"
Android 9.0	Chrome 74	– Does not support playback of Video (H.264) or audio transmission/ reception – Setting Page and Camera Viewer are not supported for the mobile device where the display size is smaller than 7"

Steps for Setting Up the Camera

Step 1 Preparing to Install the Camera

Make preparations to use the camera via a network.

Connect the power supply/to the network.

→ “Setup Guide”

Install the necessary software.

→ “Installing Software” (P. 20)

Check/configure the computer and web browser security settings.

→ “Checking/Configuring Security Settings” (P. 23)

Use the Camera Management Tool to configure initial camera settings.

→ “Configuring Initial Camera Settings” (P. 27)

Step 2 Setting Up the Camera

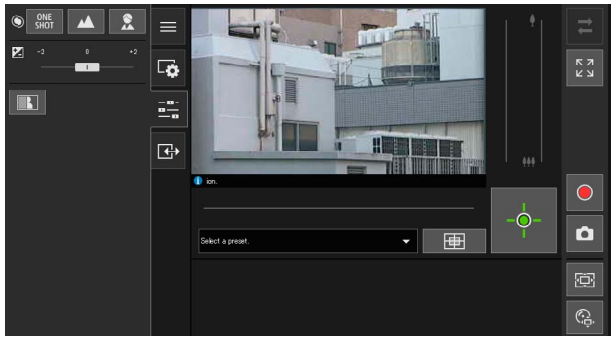
Set up the camera to suit the environment it will be used in.

→ “Setup Guide”

Step 3 Using the Camera Viewers

Operate the camera while viewing the video in the Viewer.

→ “Camera Viewer” (P. 29)



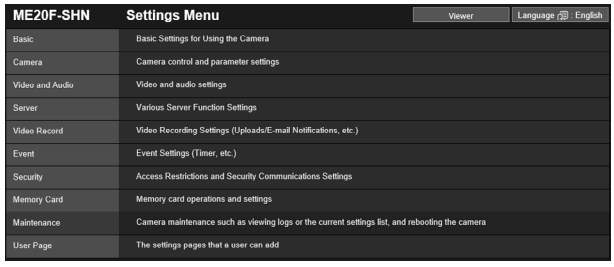
Camera Viewer

Step 4 Adjusting Advanced Settings According to Its Use

Advanced settings can be made in the Settings Menu, such as for camera control and security, according to how the camera will be used.

Settings can also be made using the Camera Management Tool. For details, please refer to “Camera Management Tool User Manual”.

→ “Setting Page” (P. 61)



Setting Page

Troubleshooting

Please refer to “Appendix” (P. 165), in case of error messages or problems.

Chapter 2

Camera Setup

To prepare the camera for use, install the necessary software on the computer, and configure the initial settings for web browser security and the camera.

Installing Software

Install the necessary software.

Necessary Software

You will need the following software:

- Camera Management Tool
- Recorded Video Utility
- .NET Framework 3.5 SP1/.NET Framework 4.5 (unnecessary if already installed on computer)

Note

If .NET Framework 3.5 SP1/.NET Framework 4.5 is not installed on the computer, the installer will automatically install the version appropriate for the version of Internet Explorer used on the computer.

Software Installation

Installation Methods

The software can be installed together using [Easy Installation], or you can select which software to install using [Custom Installation].

Installing Software

1 Confirm that all other applications have been closed.

2 Double-click [VBToolsInstall.exe].

The installation screen is displayed.

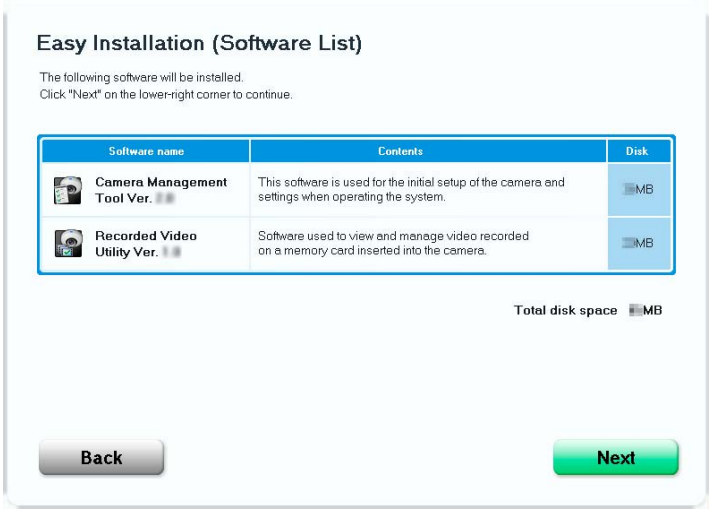
Note

If the [User Account Control] screen is displayed, click [Yes] or [Continue].

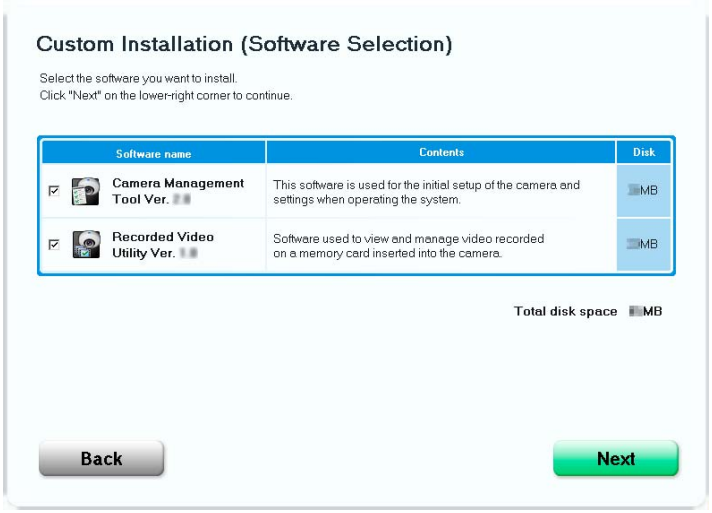
3 Select the installation method.

4 Confirm or select the software that will be installed.

If you select [Easy Installation], confirm the software that will be installed and click [Next].

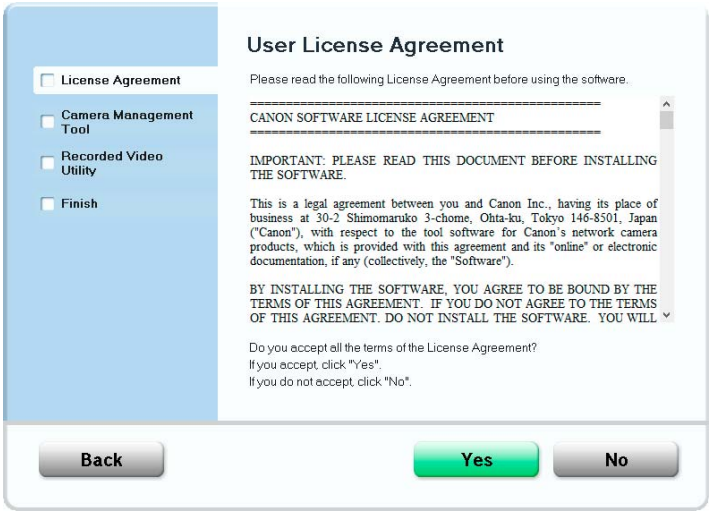


If you select [Custom Installation], select the software to be installed and click [Next].



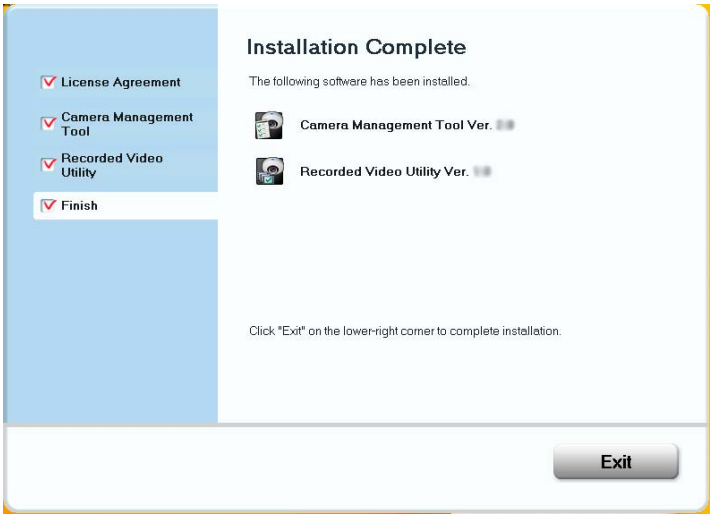
The User License Agreement screen is displayed.

5 Read through the user license agreement and click [Yes] if you accept it.



Installation starts.

6 Click [Exit] or [Reboot].



The Camera Management Tool icon and Recorded Video Utility icon will be displayed on the desktop.

Checking/Configuring Security Settings

Camera configuration and operation may be blocked, depending on the security functions of the operating system and web browser.
Change or check security settings beforehand.

Checking Firewall Settings

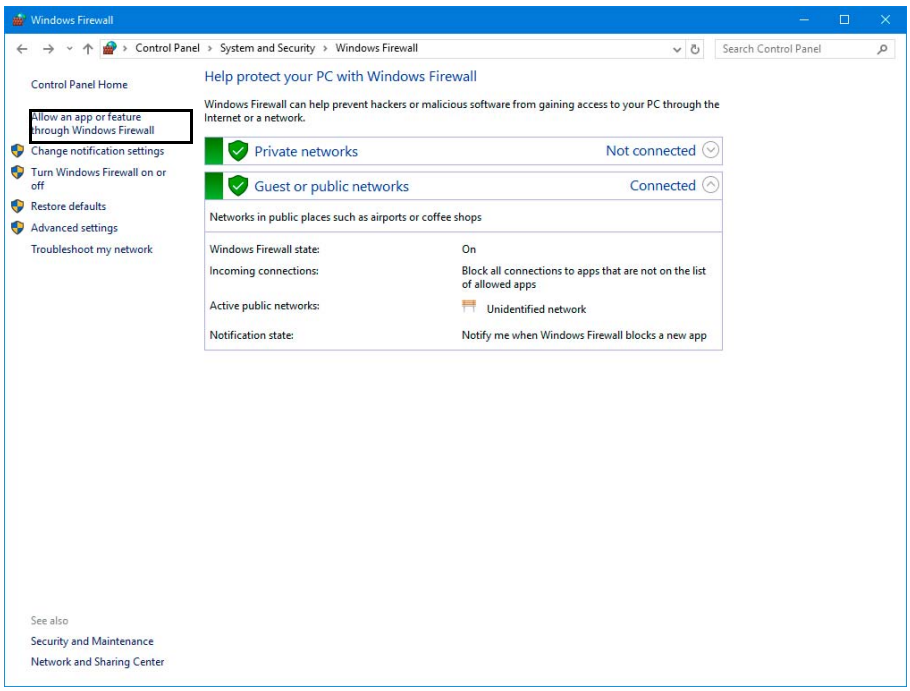
To use the software on computers where Windows Firewall is enabled, you may need to add each software as an application allowed to communicate via the firewall.

Note

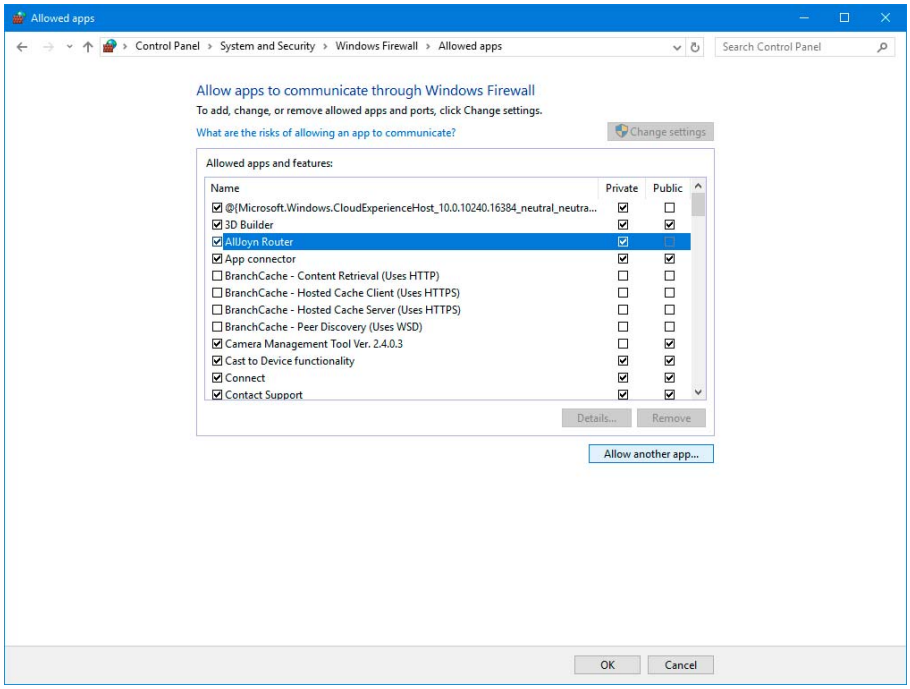
Even if you do not perform the following steps, you can still add each software with the [Windows Security Alert] dialog box that is displayed when you launch the software.

1 Click [System and Security] > [Windows Firewall] in [Control Panel].

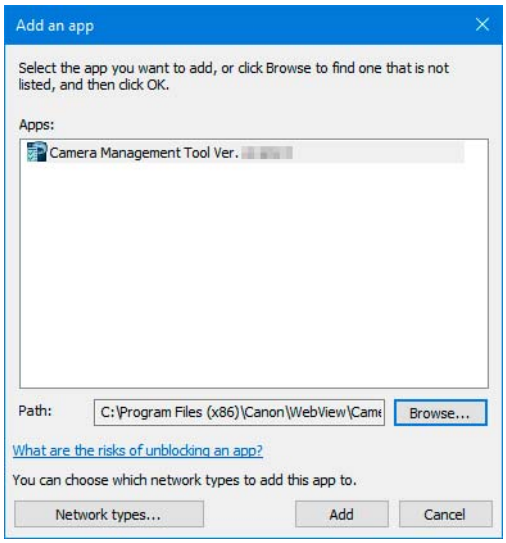
2 Click [Allow an app or feature through Windows Firewall].



3 Click [Change settings] > [Allow another app].



4 Select the software to use, such as [Camera Management Tool], and click [Add].



Settings When Using Windows Server

■ Adding the Camera IP Address as a Trusted Site

When the security level for internet sites and intranet sites is set to [High], it is necessary to add the IP address of the camera to the list of trusted sites.

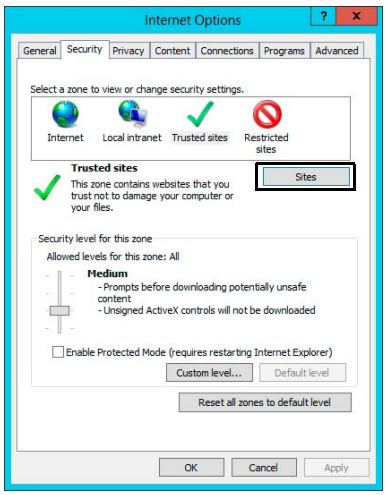
Note

Set the camera IP address with the Camera Management Tool. For details, please refer to “Camera Management Tool User Manual”.

1 Click [Network and Internet] > [Internet Options] in [Control Panel].

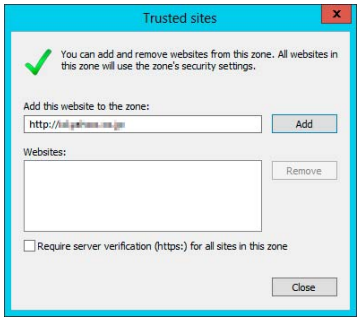
2 Click the [Security] tab.

3 Click [Trusted sites] > [Sites].



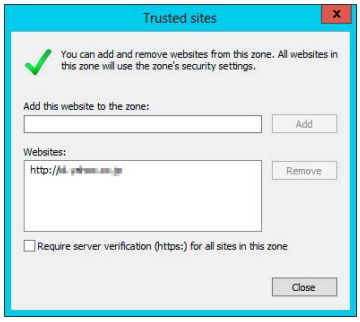
The [Trusted sites] dialog box is displayed.

4 Enter the IP address of the camera under [Add this website to the zone], then click [Add].



Note

- Clear the [Require server verification (https:) for all sites in this zone] checkbox if it is selected.
  The camera's IP address will be added to the [Websites] list.

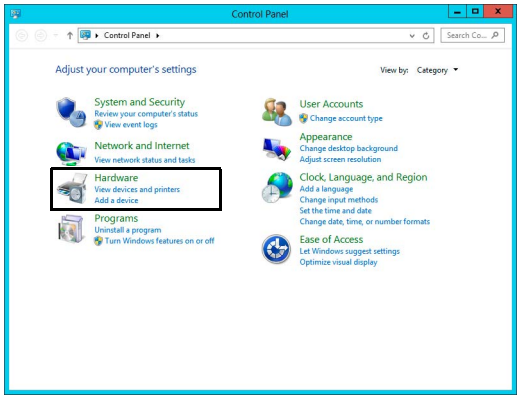


- You can add IP addresses for multiple cameras by using a wildcard (*) when entering the IP address.
  For example, if you enter "192.160.1.*", all cameras that share the "192.160.1" portion of the address will be added as trusted sites.

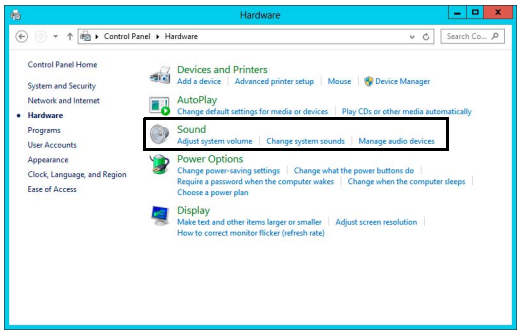
Sound Settings for Using the Audio Functions

In Windows Server, the sound function is disabled by default.
To use audio functions with the viewer, follow the steps below to enable the sound function.

1 Open [Control Panel] and click [Hardware].

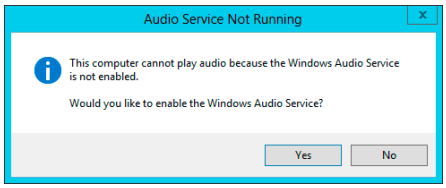


2 Click [Sound].



The [Audio Service Not Running] dialog box is displayed.

3 Click [Yes].



The [Sound] dialog box is displayed.

4 Click the [Playback] tab to confirm that an audio device has been installed.

If no audio device is installed, refer to your computer manual.

Configuring Initial Camera Settings

To use a camera, it is necessary to first set the administrator account for the camera, then configure the network settings, and then connect the camera and computer via the network. Use the Camera Management Tool to configure these settings. The Camera Management Tool also enables multiple cameras to be configured at the same time.
For information on how to use the Camera Management Tool, please refer to the “Camera Management Tool User Manual”.

Flow of Configuration Using the Camera Management Tool

Launching the Camera Management Tool

↓

Searching for Cameras

Search for cameras connected to the same network as the computer in which the Camera Management Tool is installed.

↓

Registering the Administrator Account (Administrator Name and Administrator Password)

↓

Configuring Initial Camera Settings

Configure the basic settings of the camera, such as the network settings and camera name.

Setting Up the Network without a DHCP Server

Cameras with the factory default settings are configured to obtain an IP address from the DHCP server. Detect the camera using the Camera Management Tool with a DHCP environment or an IPv6 environment.
However, you can access a camera connected to a network environment without a response from the DHCP server by entering a specific IP address (192.168.100.1) in a web browser.

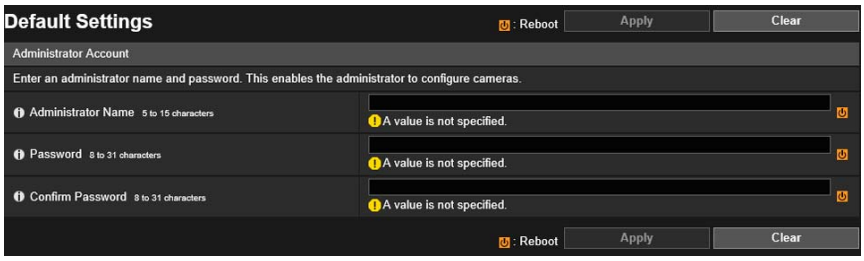
Important

- You can only access a camera 30 seconds after connecting the camera to the network environment without a response from the DHCP server using the 192.168.100.1 IP address.
- If there is a response from the DHCP server after 30 seconds has elapsed, the camera switches to the address assigned by the DHCP server.
- When accessing a camera by entering 192.168.100.1 in a web browser, set the computer to an IP address with the same subnet (255.255.255.0).
- If multiple cameras with the factory default settings exist on the same network, the cameras cannot be accessed.

1 Launch the web browser.

2 Enter 192.168.100.1, and press the Enter key.

The [Default Settings] top page will be displayed.



3 Enter the administrator name and administrator password, and click [Apply].

After the camera reboots, the Setting Page is displayed and you can configure the settings.

Chapter 3

Camera Viewer

Use the web browser to access the Viewer in the camera to perform camera operations, view live video, and check the status of events.

Viewing Video with the Camera Viewer

You can start the Camera Viewer to switch users and check/configure the status of the camera as well as the video display.

Note

If you open another window or tab to access the camera while an authenticated web page is displayed, the authentication information of the displayed web page may be discarded.
In this case, enter the authentication information again.

Launching the Camera Viewer

You can enter the IP address set with the Camera Management Tool directly into a web browser to display the Setting Page of the camera, and start the Viewer from the Setting Page.

Note

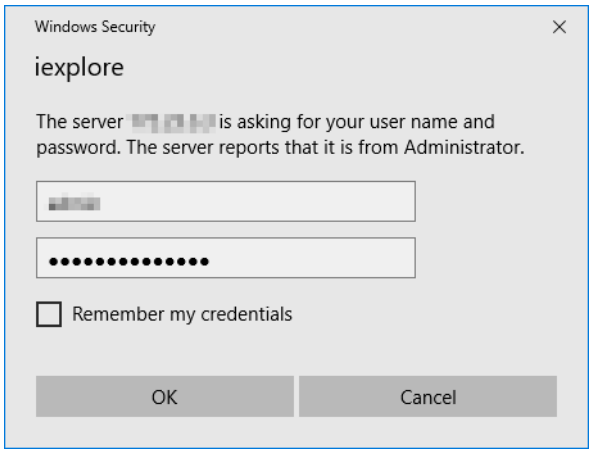
For details on settings in the Camera Management Tool, please refer to “Camera Management Tool User Manual”.

1 Launch the web browser.

2 Enter the IP address, and press the Enter key.

The authentication screen for Setting Page will be displayed.

3 Enter the Administrator Name and Administrator Password and click [OK].

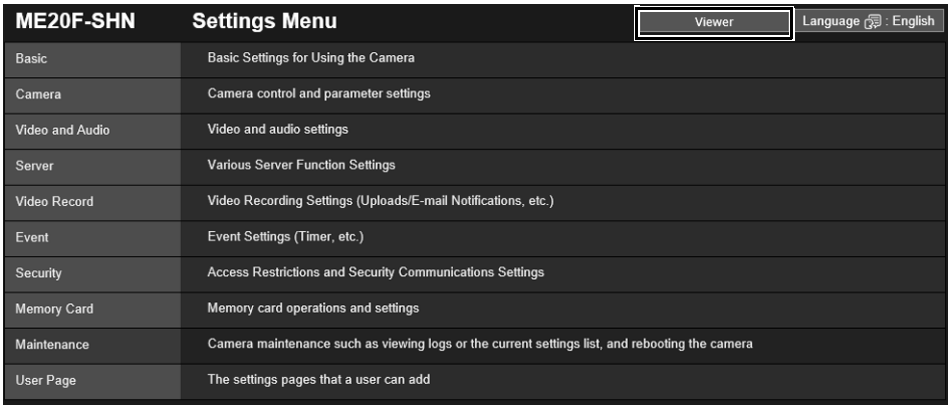


The Settings Menu is displayed.

Note

You can set [Basic] > [Viewer] > [General] > [Default Page] to [Display Viewer] in the setting menu to set the Viewer as the default page (P. 79).

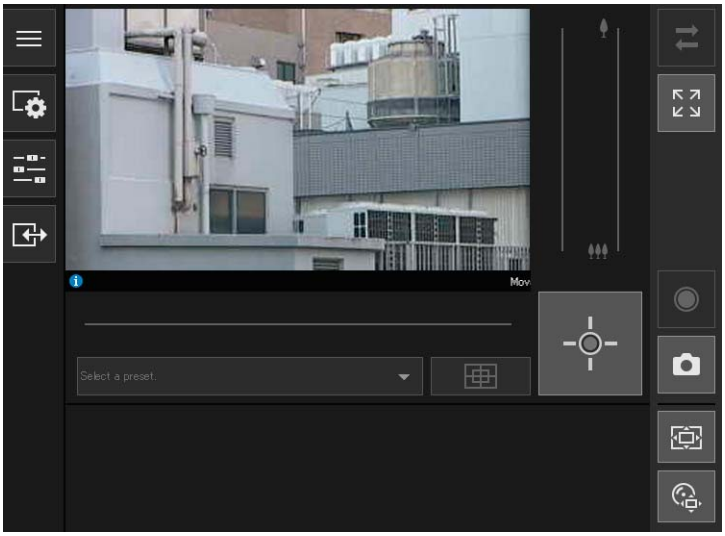
4 Click [Viewer].



The authentication screen for the Viewer is displayed.

5 Enter the administrator name and administrator password, and click [OK].

The Camera Viewer is displayed.



Note

While color bars are output (refer to "Setup Guide"), video cannot be displayed with the Camera Viewer.

User Authentication

When you use the Viewer and the Setting page, an authentication screen is displayed, and you are prompted to enter a user name and password.
If you enter the wrong user name or password, you will not be able to connect to the camera. Enter the correct user name and password and connect to the camera.
When [Basic] > [Viewer] > [Viewer Settings] > [User Authentication] on the Setting Page is set to [Do not authenticate], the authentication screen is not displayed when connecting the Viewer.

Authentication screen for the Setting Page

Authentication screen for the Viewer

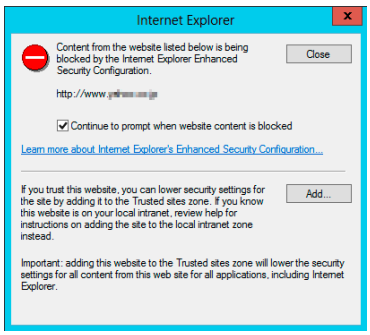
The administrator name and administrator password are set using the Camera Management Tool.

Important

- To ensure system security, register a strong administrator password that cannot be easily guessed by a third party. Do not forget the password.
- Restore factory default settings if you have forgotten the administrator account (P. 185). However, you will become unable to connect to the camera because the administrator account is also initialized. Use the Camera Management Tool to configure the initial settings.
- It is strongly recommended that you clear the [Remember my credentials] checkbox when an authorized user shares a Viewer on the same computer.

Note

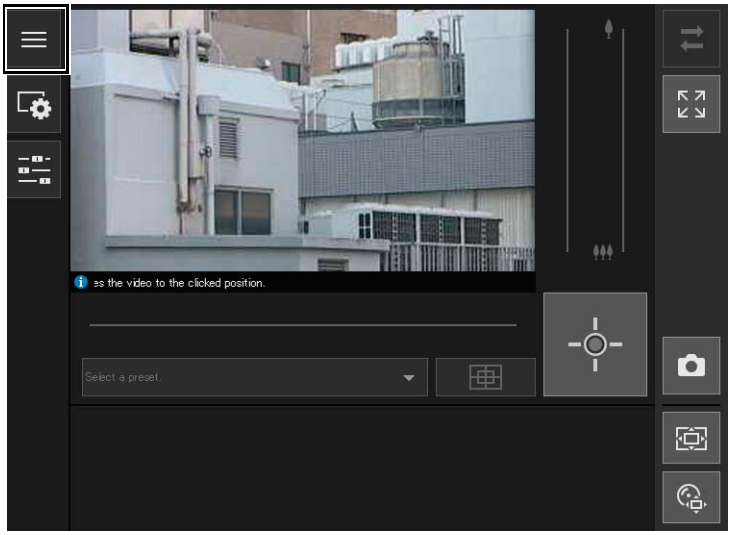
- Only administrators can connect to a camera using the Setting Page.
- When IE ESC (Internet Explorer Enhanced Security Configuration) is enabled in Windows Server, the blocked content dialog box may be displayed when attempting to access the Setting Page or the Viewer. If this happens, please register the camera IP address as a trusted site (P. 24).



Switching to the Administrator or an Authorized User

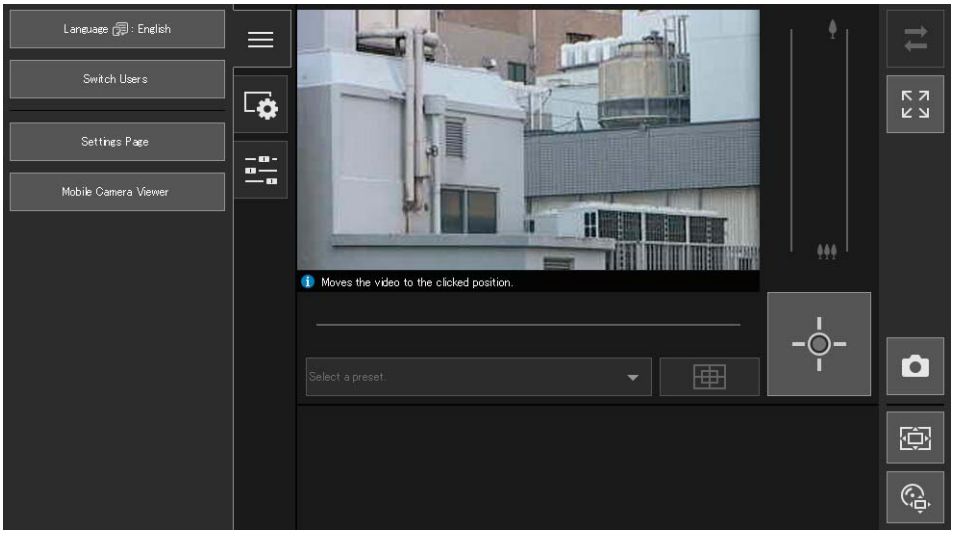
If [Basic] > [Viewer] > [Viewer Settings] > [User Authentication] is set to [Do not authenticate] on the Setting Page, an authentication screen is not displayed when connecting to the Viewer, and you can use the Viewer as a guest user. Guest users cannot perform some operations with the Viewer, but you can also switch the user in order to use the Viewer as an administrator or authorized user.

1 Click the [Main] button.



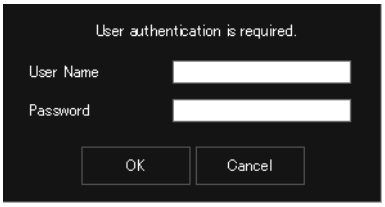
The [Main] menu will be displayed.

2 Click [Switch Users].



The user authentication window is displayed.

3 Enter a user name and password and click [OK].



The Viewer for the user entered for user authentication is displayed.

Camera Viewer Access Restrictions

You can set authorized users, which require user authentication, and guest users, which do not require authentication.
The functions that each user can use in the Camera Viewer depend on the privileges assigned to the user (P. 74).

Administrator:
The user assigned all privileges.
Access the Viewer using the administrator name and password registered for the administrator account.

The administrator can disable all the privileges of an authorized user or a guest user, and completely prohibit authorized users and guest users from accessing the camera.

Authorized user:
An authorized user has higher privileges than a guest user.
It is necessary to register the user name and password (P. 73).

Guest user:
This user can only use a limited set of functions.
Can access the Viewer without performing user authentication.

The four types of privileges for using the Viewers are privileged camera control, camera control, video distribution and audio distribution.
The scope of each privilege and whether it can be granted to a user is shown below.

Privilege	Privileged Camera Control	Camera Control	Video Distribution	Audio Distribution
Scope of Privilege	Can perform the most operations after the administrator.	Can perform some Viewer operations.	View video with the Viewer	Receive audio with the Viewer
Grant to Authorized Users	Yes	Yes	Yes	Yes
Grant to Guest Users	No	Yes	Yes	Yes

If an item in [Privileged Camera Control], [Camera Control], or [Video Distribution] is set to [Enable] in the above table, the items above and to the right of that item are also set to [Enable]. If an item is set to [Disable], the items below and to the left of that item are also set to [Disable].
In the rows, privileges on the left involve privileges on the right. However, audio distribution can be set separately.
In the columns, authorized users have higher privileges than guest users.

Important

- Multiple computers cannot connect to a single camera at the same time using the same administrator account.
  An authorized user or a guest user can connect to the camera from multiple computers at the same time. However, when controlling the camera, the control privileges are given to the authorized user who accessed the camera most recently. On the other hand, guest users are placed in a queue.
- [Basic] > [Viewer] > [General] > [Default Page] must be set to [Display Viewer] to enable authorized users and guest users to connect to the camera.

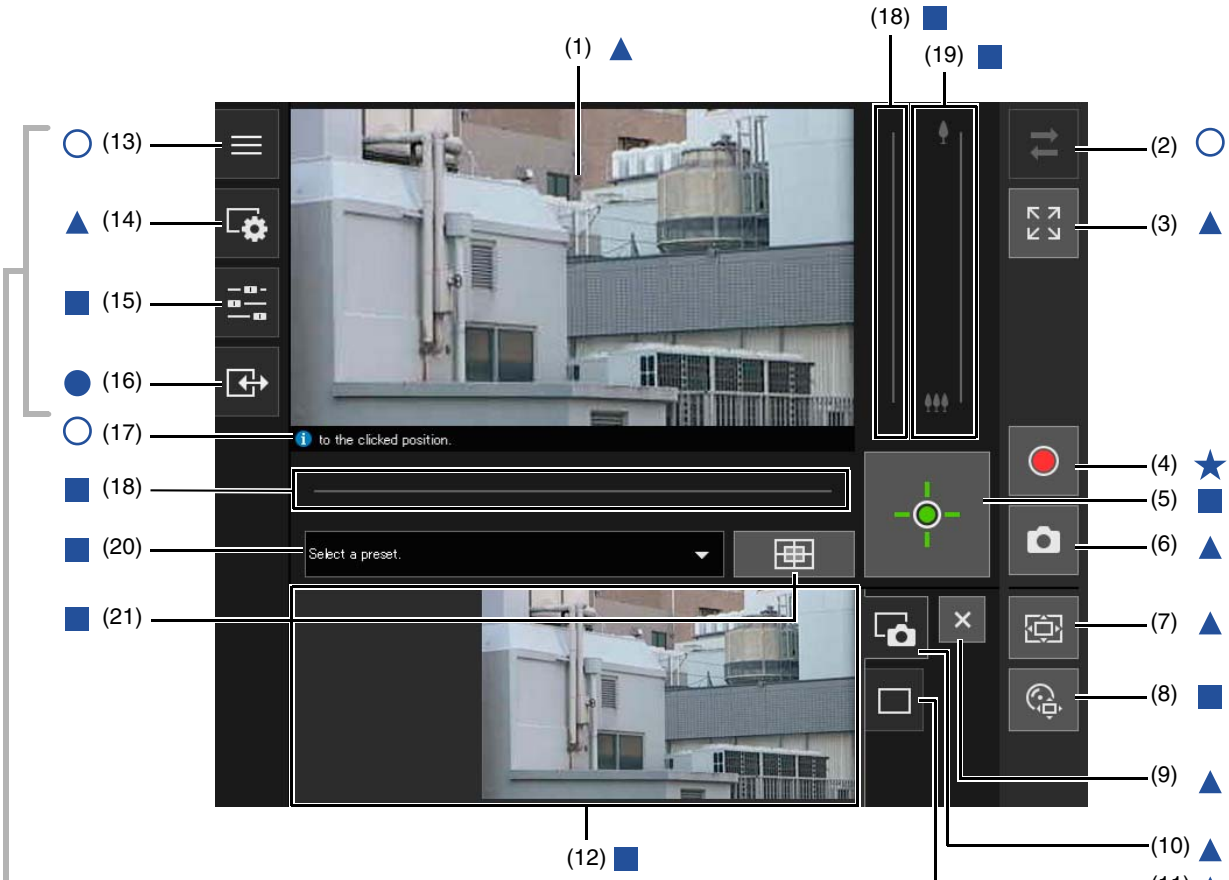
Note

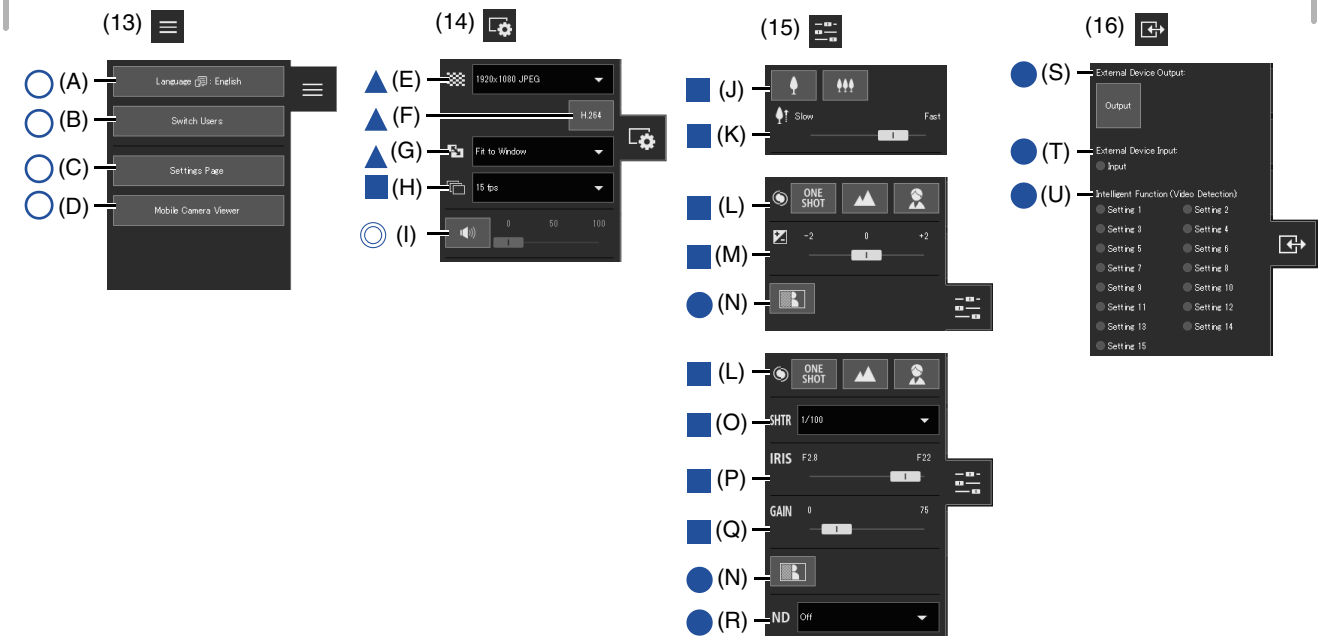
With the factory default settings, authorized users are assigned privileges for camera control.

Camera Viewer Screen

The privileges required for operating the Viewer are indicated with the following symbols.

★	Administrator Privileges	▲	Video Distribution or higher privileges
●	Privileged Camera Control or higher privileges	○	No privileges needed
■	Camera Control or higher privileges	◎	Audio Distribution privileges





(1) Video Display Area
Displays video received from the camera.

(2) [Reconnect] Button
Reconnects to the camera. Can be operated when the Viewer is not connected to the camera.

(3) [Full Screen Mode] Button
Video is displayed in full screen mode (P. 41).

(4) [Memory Card Recording] Button
Start and stop video recording to a memory card (P. 56).

(5) [Obtain/Release Camera Control Privileges] Button
Obtain and release the camera control privileges (P. 45).

(6) [Snapshot] Button
Open the snapshot panel and display a still image of the moment you clicked the button in the control display area (P. 55).

(7) [Viewer PTZ] Button
Starts/stops the Viewer PTZ*. When started, the Viewer PTZ panel is shown in the control display area (P. 51).
*PTZ: pan/tilt/zoom

(8) [Digital PTZ] Button
Starts/stops the Digital PTZ. When started, the Digital PTZ panel is shown in the control display area (P. 52).

(9) [Close] Button
Closes the panels shown in the control display area.

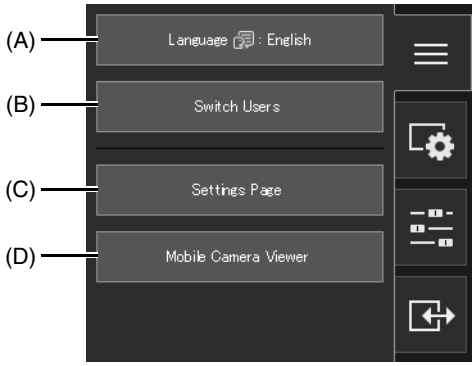
(10) Snapshot Tab
Click this to switch the control display area to the snapshot panel (P. 55).

(11) Viewer PTZ/Digital PTZ Tab
Click this to switch the control display area to the Viewer PTZ/Digital PTZ panel (P. 51).

(12) Control Display Area
Click (10) or (11) to display the snapshot panel or Viewer PTZ/Digital PTZ panel.

(13) [Main] Menu

Switches the language or user, and switches the Setting Page or Mobile Camera Viewer.



(A) [Language] Button

Switches the display language.

(B) [Switch Users]

Use this to log in as an administrator or authorized user (P. 32).

(C) [Settings Page]

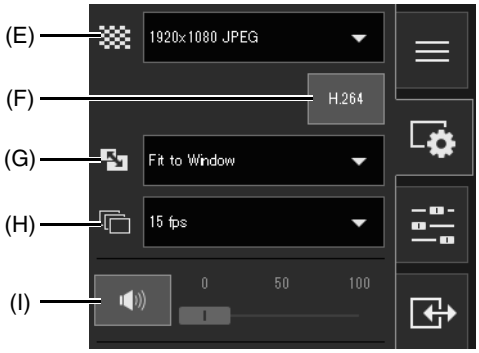
The screen switches to the Setting Page (P. 62).

(D) [Mobile Camera Viewer]

Switches the connection to the Mobile Camera Viewer. For details on Mobile Camera Viewer, please refer to “Mobile Camera Viewer Operation Guide”.

(14) [Video and Audio] Menu

Configures the video display size and audio reception of the Viewer.



(E) Video Size

Select the video reception size and video format from the camera (P. 41).

(F) H.264 Reception

Selects whether to enable or disable H.264 video reception (P. 41).
For guest users, [H.264] is displayed if [Enable] is set in [Basic] > [Viewer] > [Viewer Settings] > [H.264 for Guest Users] on the Setting Page (P. 79).

(G) Display Size

Select the video display size for the screen (P. 41).

(H) Maximum Frame Rate

Select the maximum frame rate for JPEG video (P. 41).

(I) Audio Reception

Start/stop audio reception from the camera and set the volume (P. 57).

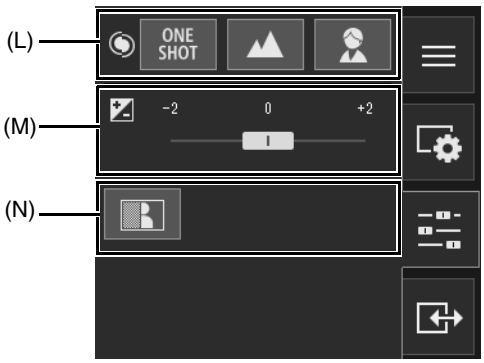
(15) [Camera Operation] Menu

Configure video settings of the camera.

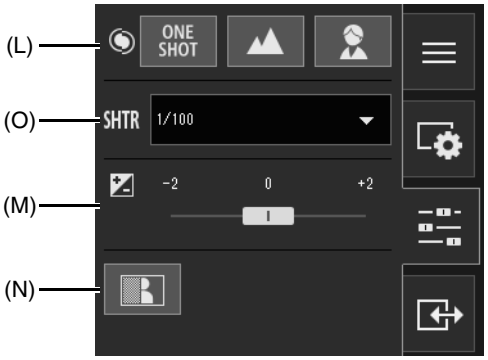
Items to be displayed vary depending on the setting in [Camera] > [Camera Settings] > [Camera Mode] on the Setting Page (P. 84).

With a power zoom lens attached

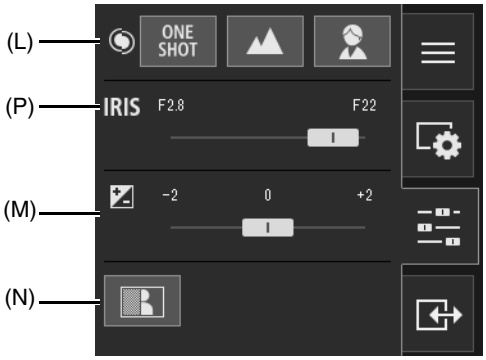
With [Camera Mode] set to [Auto]



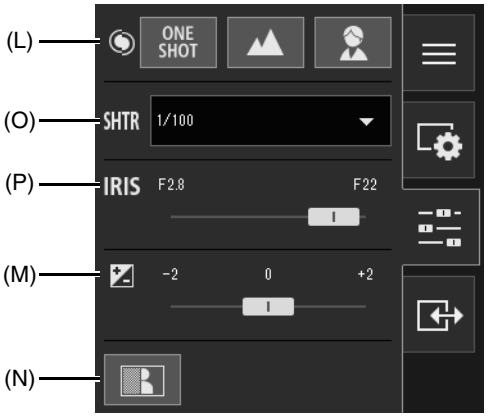
With [Camera Mode] set to [Tv]



With [Camera Mode] set to [Av]



With [Camera Mode] set to [AGC]



With [Camera Mode] set to [Manual]

(J) Zoom

Displayed when a power zoom lens is attached. Operate a button to zoom in and zoom out (P. 47).

(K) Zoom Speed

Displayed when a power zoom lens is attached. Select the operation speed for the zoom button (P. 47)

(L) Focus

Sets the camera to focus on the subject (P. 47).

(M) AE Shift

Corrects the exposure according to the brightness of the subject (P. 47).

(N) Infrared
Select whether to use the infrared mode (P. 48).

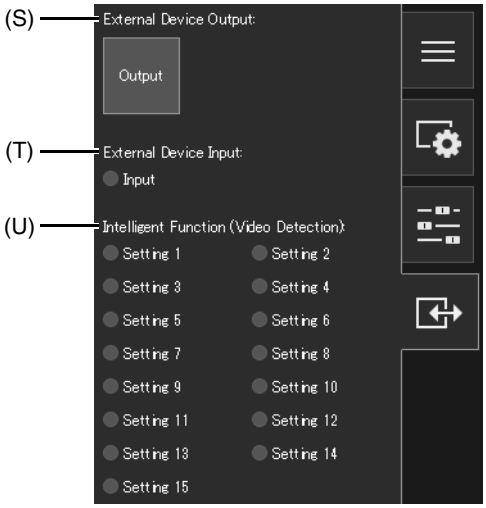
(O) Shutter Speed
Select the shutter speed based on shooting conditions, such as the motion or brightness of the subject (P. 48).

(P) Iris
Specify the iris (aperture) (P. 48).

(Q) Gain
Set the sensitivity to affect brightness (P. 49).

(R) ND Filter
Select for usage of the ND filter (P. 49).

(16) [Event and Input/Output] Menu
Enables you to check the output operations and input status of an external device, as well as to check the detection status of the intelligent function.



(S) External Device Output
Use external device output (P. 58).

(T) External Device Input
Displays the status of the external device input signal (P. 58).

(U) Intelligent Function (Video Detection)
Displays the status of video detection by the intelligent function for each detection setting number (P. 59).

(17) Information Display
Information, warning and error messages are displayed (P. 40).

(18) Pan/Tilt Slider
Drag the sliders to pan (horizontally) or tilt (vertically) the camera (P. 46).
Slider operations are available when using the Viewer PTZ or Digital PTZ.

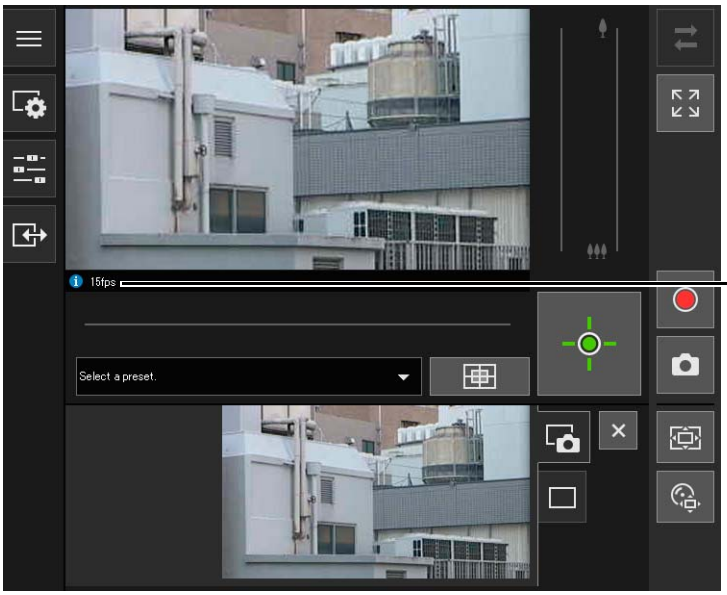
(19) Zoom Slider
Drag the slider to operate the zoom in (telephoto)/zoom out (wide-angle) function of the camera (P. 46).
Slider operations are available when using the Viewer PTZ or Digital PTZ.

(20) Preset Selection Menu
Selects a preset registered in the camera in advance (P. 49).

(21) [Home Position] Button
Move the camera angle to the home position (P. 49).

Checking Information

Information, such as the frame rate, camera pan/tilt/zoom values and descriptions of each function, is shown in the Information Display.
Warning and error messages will also be displayed here if there are problems with camera operations or systems.



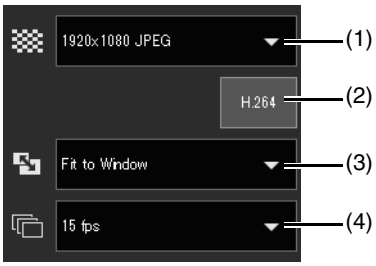
For details on the information displayed, please refer to “List of Viewer Messages” (P. 183).

Changing the Reception Video Size and Display Screen Size

You can set the size and format of the video received from the camera and the size of the display screen on the computer.

Changing the Reception Video Size/Format and Display Screen Size

Open the [Video and Audio] menu and configure the video received from the camera.



(1) Video Size Setting

Select the size and format of video received from the camera.

Selectable Video Size	
JPEG	H.264*
480 x 270 960 x 540 1920 x 1080	• The sizes set with [Video Size] in [Basic] > [Video] > [H.264(1)] or [H.264(2)] on the Setting Page (P. 78), determine the sizes displayed in the menu. • When [H.264(2)] is set to [Enable] in [Basic] > [Video] > [H.264(2)] on the Setting Page (P. 78), both the [H.264(1)] and [H.264(2)] video sizes are displayed in the menu.

* If you enable [H.264] (make it purple), the H.264 video size is added to the menu.

(2) [H.264]

Enable this (make it purple) to receive the H.264 video.

If you click this when it is disabled (gray), the [CANON SOFTWARE LICENSE AGREEMENT] dialog box is displayed. Click [Yes] to accept the terms of the license agreement. The decoder is downloaded from the camera, enabling H.264 video reception. The [CANON SOFTWARE LICENSE AGREEMENT] dialog box is not displayed for a guest user.

(3) Display Size Setting

Select the screen size to display the video.

Selectable Screen Size	Remarks
Actual Pixels 480 x 270 960 x 540 1920 x 1080 Fit to Window	[Actual Pixels] displays the video at the size at which it is being captured. [Fit to Window] displays the video at the maximum size possible in the web browser window.

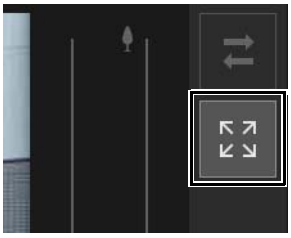
(4) Max. Frame Rate (JPEG)

You can select the maximum frame rate for JPEG video.

The setting is not selectable when displaying H.264 video in the video display area.

Displaying in Full Screen Mode

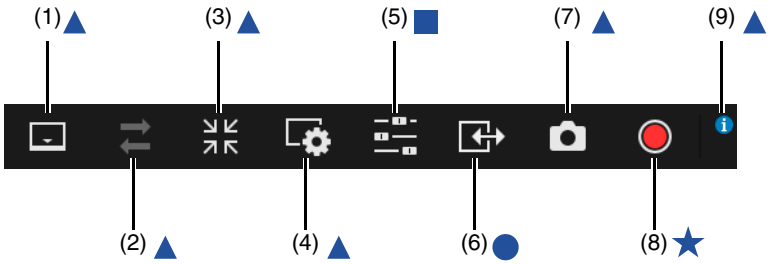
You can display the video display area in full screen mode by clicking the [Full Screen Mode] button in the upper right of the Viewer.



Menus

When the full screen view is used, the menu panels required for controlling the camera are displayed on the bottom of the screen, as with the Camera Viewer screen.
The privileges required for operating the menu panel are indicated with the following symbols.

★	Administrator Privileges
●	Privileged Camera Control or higher privileges
■	Camera Control or higher privileges
▲	Video Distribution or higher privileges
◎	Audio Distribution privileges



(1) Menu Area Display Switch Button
Switches between displaying and hiding the menu bar.

(2) [Reconnect] Button
Reconnects to the camera. Can be operated when the Viewer is not connected to the camera.

(3) Full Screen Mode Switch Button
Returns the video display area to the regular view.

(4) [Video and Audio] Menu
Configures the video display size and audio transmission/reception of the Viewer.

(A) Video Size
Sets the reception video size from the camera (P. 41).

(B) H.264
Selects whether to enable/disable H.264 video reception (P. 41).

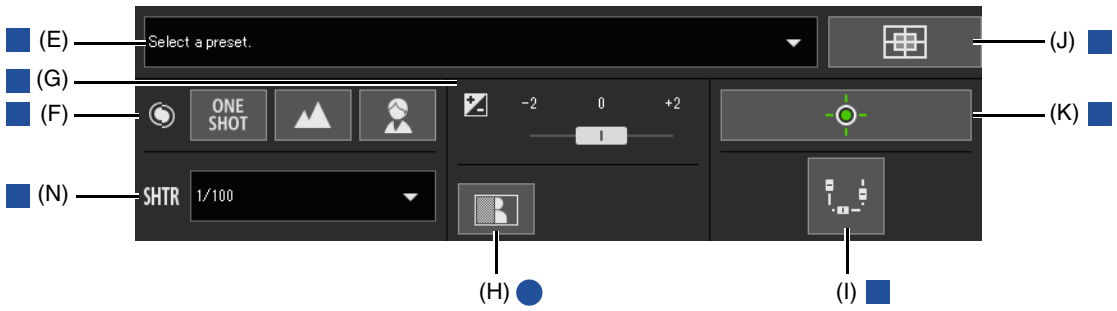
(C) Maximum Frame Rate
Selects the maximum frame rate for JPEG video (P. 41).

(D) Audio Reception
Plays/stops the received audio and sets the volume (P. 57).

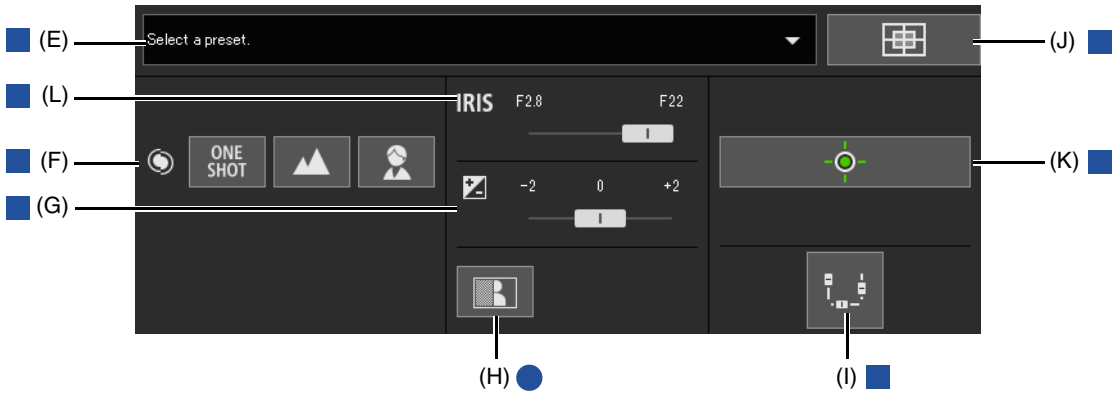
(5) Camera Operation Menu
Performs the basic settings and operations of the camera.

With [Camera] > [Camera Settings] > [Camera Mode] (P. 84) set to [Auto] on the Setting Page

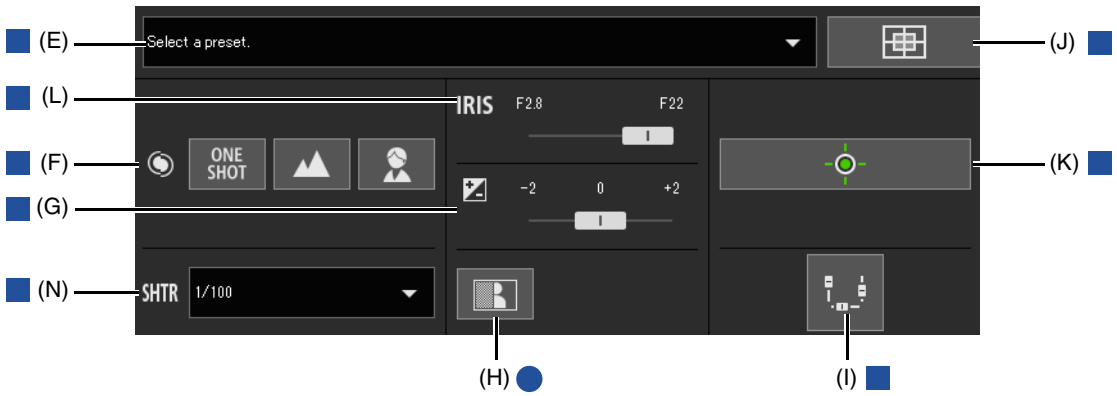
With [Camera] > [Camera Settings] > [Camera Mode] (P. 84) set to [Tv] on the Setting Page



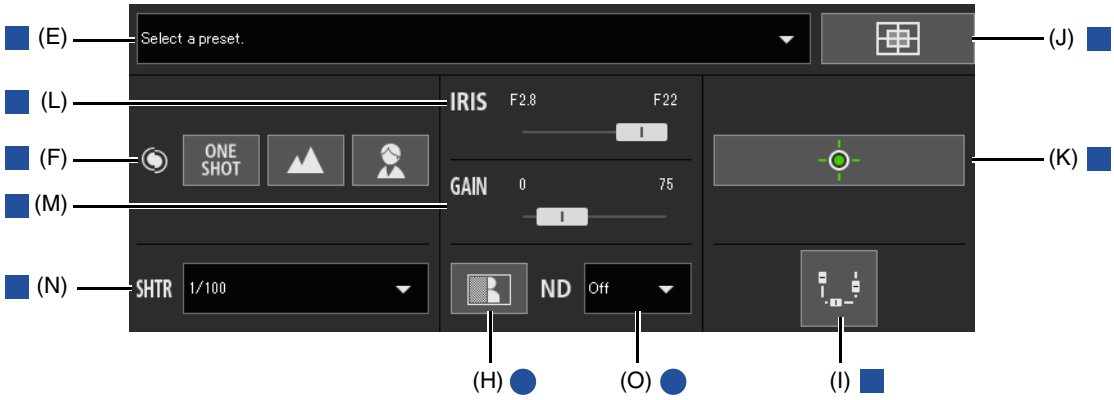
With [Camera] > [Camera Settings] > [Camera Mode] (P. 84) set to [Av] on the Setting Page



With [Camera] > [Camera Settings] > [Camera Mode] (P. 84) set to [AGC] on the Setting Page



With [Camera] > [Camera Settings] > [Camera Mode] (P. 84) set to [Manual] on the Setting Page



(E) Preset
Selects a preset registered in the camera in advance (P. 49).

(F) Focus
Sets the camera to focus on the subject (P. 47).

(G) AE Shift
Adjusts the exposure according to the brightness of the subject (P. 47).

(H) Infrared
Select whether to use the infrared mode (P. 48).

(I) Pan/Tilt/Zoom
If you enable this button (make it purple), the pan/tilt/zoom sliders are displayed on the screen to perform operations.
Slider operations are available when using the Viewer PTZ or Digital PTZ.
The pan slider is displayed on the bottom of the screen, the tilt slider on the left edge of the screen, and the zoom slider on the right edge of the screen.

(J) Home Position
Move the camera angle to the home position (P. 49).

(K) Obtain/Release Camera Control Privileges
Obtain and release the camera control privileges (P. 45).

(L) Iris
Specify the iris (aperture) (P. 48).

(M) Gain
Set the sensitivity to affect brightness (P. 49).

(N) Shutter Speed
Set the shutter speed based on shooting conditions, such as the motion or brightness of the subject (P. 48).

(O) ND Filter
Select for usage of the ND filter (P. 49).

(6) Event and Input/Output Menu
Use external device output (P. 58).

(7) Snapshot
Displays the still image shown when the button was clicked by opening the snapshot panel (P. 55).

(8) Memory Card Recording
Start and stop video recording to a memory card (P. 56).

(9) Information Display
Information, warning and error messages are displayed (P. 40).

Operating the Camera

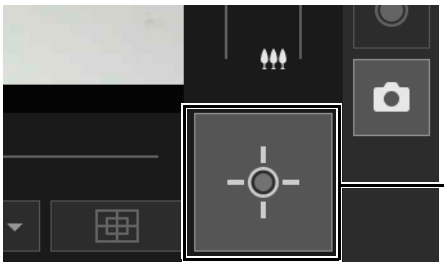
This section describes the operations and configuration required for using the camera, such as obtaining camera control privileges, setting the angle and focus.

Important

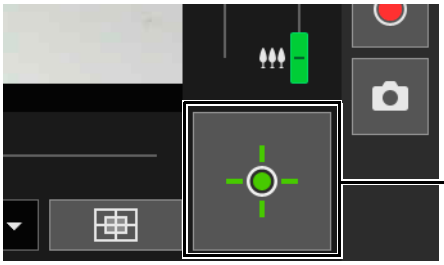
It is necessary to obtain the camera control privileges to perform the operations and configuration as first described in this section.

Obtaining Camera Control Privileges

To use the camera, you must obtain control privileges with the Viewer.
If you have not yet obtained camera control privileges, click the [Obtain/Release Camera Control Privileges] button.



You will obtain control privileges and be able to use the buttons on the Viewer.
The center of the [Obtain/Release Camera Control Privileges] button turns green while you have control privileges.



Camera Control Privilege Status Indicator

Depending on the camera control privilege status, the [Obtain/Release Camera Control Privileges] button appearance changes as follows.

Appearance	Control Privilege Status	Explanation
	Control privileges not obtained	Camera control privileges have not been obtained.
	Waiting for control privileges	When a guest user is waiting to obtain camera control privileges, the remaining time is counted down.
	Control privileges obtained	Camera control privileges have been obtained.
	Control privileges obtained (remaining control time)	After a guest user has obtained camera control privileges, the time that the user can retain control privileges in priority over other guest users is counted down.

Important

- Multiple users cannot obtain control privileges simultaneously.
- The Obtain/Release Camera Control Privileges button is displayed for authorized users and guest users if [Camera Control] is selected in [Basic] > [User Management] > [User Authority] on the Setting Page.
- Administrators can take away camera control privileges from authorized users or guest users. Authorized users can also take away camera control privileges from guest users.
  A user with lower privileges cannot obtain camera control privileges while a user with higher privileges has camera control privileges. Once finished, the administrator should always exit the Viewer or click the [Obtain/Release Camera Control Privileges] button to release the control privileges.

Using Pan/Tilt/Zoom

You can pan, tilt and zoom the camera to set the camera angle.

Note

Camera operations using clicking and dragging, do not offer a high precision control of the camera.

■ Clicking on the Video Display Area or Use the Sliders

Note

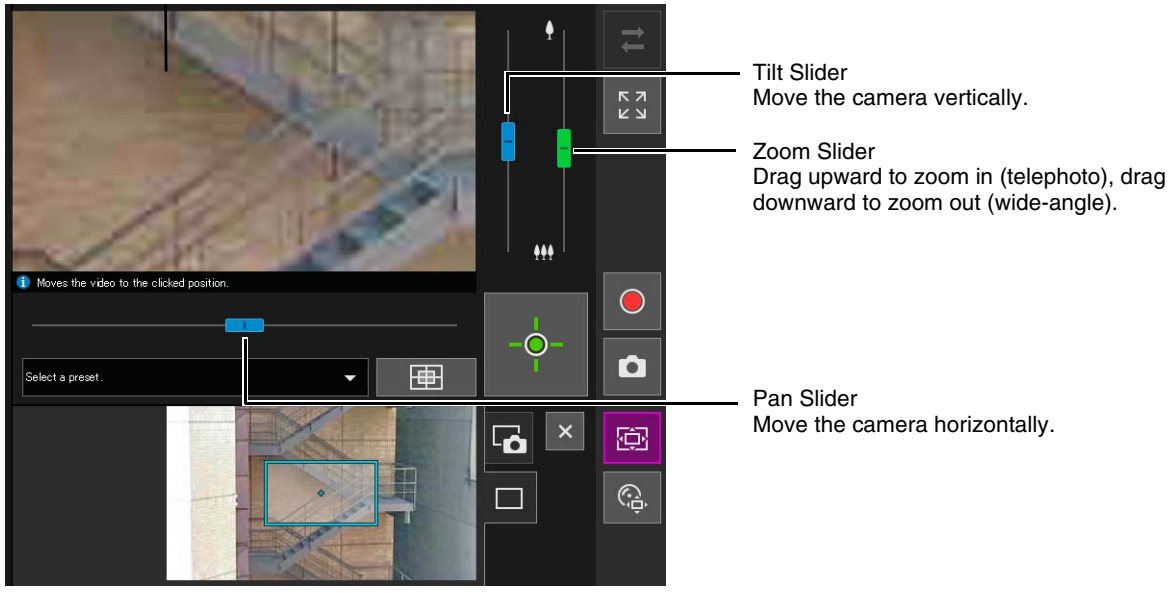
Click operations and slider operations in the video display area become available after starting the Viewer PTZ or Digital PTZ (P. 51).

Moving by Clicking on the Video Display Area

If you click in the video display area, the camera angle will change to center on the mouse pointer location. If the camera angle does not center on the desired location with a single click, repeat the operation.

Moving Using the Sliders

Drag the pan and tilt sliders to pan and tilt the camera.
Drag the zoom slider to zoom the camera.
The slider can also move by clicking directly on the slider bar.



Note

- The zoom ratio (digital zoom ratio) is shown in the information display.

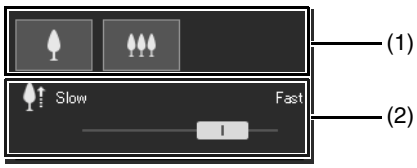
- With digital zoom, image quality is reduced as the zoom ratio increases.

Using [Zoom] in the [Camera Operation] Menu

Note

- The zoom operation screen is displayed only when a power zoom lens is attached.
- When an EF Cinema lens is attached to the camera, set the lens's zoom operation change-over knob to SERVO.

Open the [Camera Operation] menu and perform camera zoom operations.



(1) [Zoom]
Click the (Zoom in) and (Zoom out) buttons. Movement will continue while you hold the button down, and stop when you release it.

(2) [Zoom Speed]
Set the operation speed by the [Zoom] button.

Note

Even if you change the zoom speed setting, the speed of zoom operations on the slider does not change.

Adjusting Video

Open the [Camera Operation] menu to operate for the video of the camera.

Focusing

Focus on the subject.

Clicking (One-shot AF) automatically adjusts the focus once, and then switches to the manual mode.
You can click and hold the (Near) and (Far) buttons to adjust the focus in the near and far directions.
For details on this function, please refer to "Adjusting the Focus" (P. 83).

Important

- If [Camera] > [Camera Settings] > [Camera Mode] (P. 84) is set to [Manual], [Tv], or [AGC], and also [Shutter Speed] is set to [1/7] or slower on the Setting Page, you cannot use the [One-shot AF] button.
- For cautions on using Focus, see the “Important” section on P. 84.

Setting AE Shift

If [Camera] > [Camera Settings] > [Camera Mode] is set to camera modes other than [Manual] on the Setting Page (P. 84), you can adjust the brightness of the video.
Move the slider to a negative value to make the video darker or a positive value to make the video lighter.

Important

Cannot be set when [Camera] > [Camera Settings] > [Camera Mode] is set to [Manual] on the Setting Page (P. 84).

Setting Infrared

Select whether to use the infrared mode according to the brightness of the environment in which the camera is installed. To use the infrared mode, set it to ON (purple).

Infrared ON

Infrared OFF

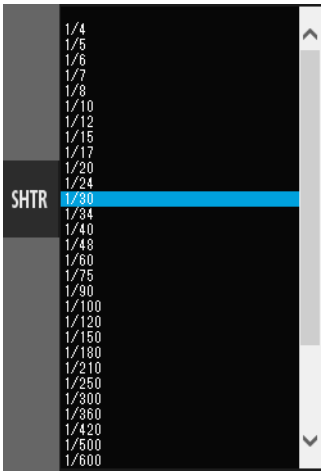
For details on this function, see [Camera] > [Camera Settings] > [Infrared] on the Setting Page (P. 87).

Important

For cautions on using infrared, see the “Important” section on P. 87.

Setting the Shutter Speed

If [Camera] > [Camera Settings] > [Camera Mode] is set to [Manual], [Tv], or [AGC] on the Setting Page (P. 84), you can fix the shutter speed.



For details on this function, see [Camera] > [Camera Settings] > [Shutter Speed] on the Setting Page (P. 85).

Important

For cautions on setting the shutter speed, see the "Important" section on P. 85.

Adjusting the Iris

If [Camera] > [Camera Settings] > [Camera Mode] is set to [Manual], [Av], or [AGC] on the Setting Page (P. 84), you can set a desired iris (aperture).
Moving the slider to the right closes the iris and darkens the image. Moving the slider to the left opens the iris and brightens the image.

For details on this function, see [Camera] > [Camera Settings] > [Iris] on the Setting Page (P. 84).

Important

For cautions on adjusting the iris, see the "Important" section on P. 85.

Adjusting the Gain

If [Camera] > [Camera Settings] > [Camera Mode] is set to [Manual] on the Setting Page (P. 84), you can set the sensitivity to affect brightness.
Moving the slider to the left darkens the video, and moving it to the right brightens video.

Important

For cautions on setting the gain, see the "Important" section on P. 85.

Using the ND Filter

You can select for usage of the ND filter in the following cases:

– [Camera] > [Camera Settings] > [Camera Mode] is set to [Manual] on the Setting Page (P. 84), and the [Infrared] button is OFF in the Camera Viewer (P. 48).
– [Camera] > [Camera Settings] > [ND Mode] is set to [Manual] on the Setting Page (P. 87), and the [Infrared] button is OFF in the Camera Viewer (P. 48).

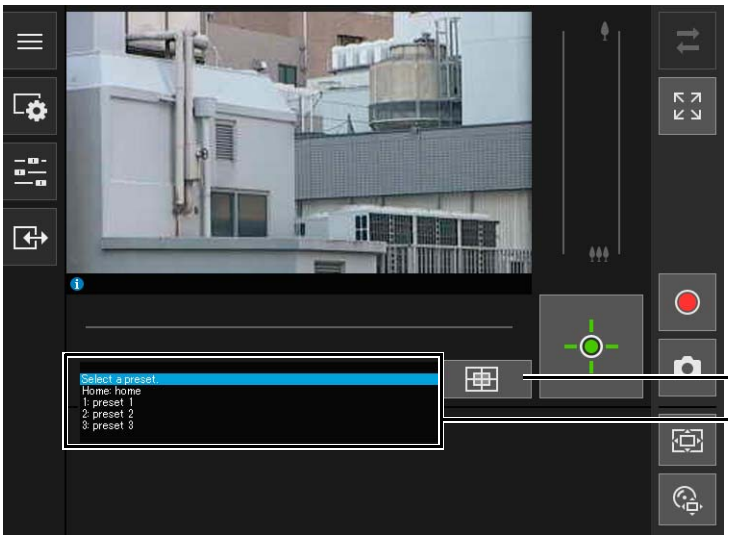
For details on this function, see [Camera] > [Camera Settings] > [ND Filter] on the Setting Page (P. 87).

Important

For cautions on using the ND filter, see the "Important" section on P. 87.

Using Presets or the Home Position

It is possible to control the camera using a preset or home position registered to the camera in advance.
When you click the preset selection menu and select a preset from the list that is displayed, the camera will be set to the registered setting of the selected preset.
Clicking the [Home Position] button will set the camera to the registered setting of the home position.



Note

Register preset/home positions in advance in [Camera] > [Preset] > [Register Preset] (P. 92) on the Setting Page.
The registered preset is displayed in the preset selection menu.

Viewer PTZ and Digital PTZ

Viewer PTZ and Digital PTZ are both functions which allow easy panning, tilting and zooming using the digital zoom.

Viewer PTZ	Digital PTZ
Enlarges the specified part of the video transmitted from the camera and then displays it in the viewer.	Transmits only the cropped part of the entire area that can be captured by the camera.
The size of the received data is large.	The size of the received data is small.
Camera control is not required.	Camera control is required.
PTZ operation can be performed independently for each Viewer.	Independent operation cannot be performed by each Viewer. If multiple Viewers are connected, the same Digital PTZ display is applied to the other Viewers.
Custom trim size	Five levels of trim size

Magnifying and Display Part of Video (Viewer PTZ)

You can use the Viewer PTZ to magnify part of a video (using digital zoom) without moving the camera.
This feature does not use the camera's pan, tilt, or zoom features, making it useful for situations like the use of the intelligent function, where you do not want to change the camera position.

Note

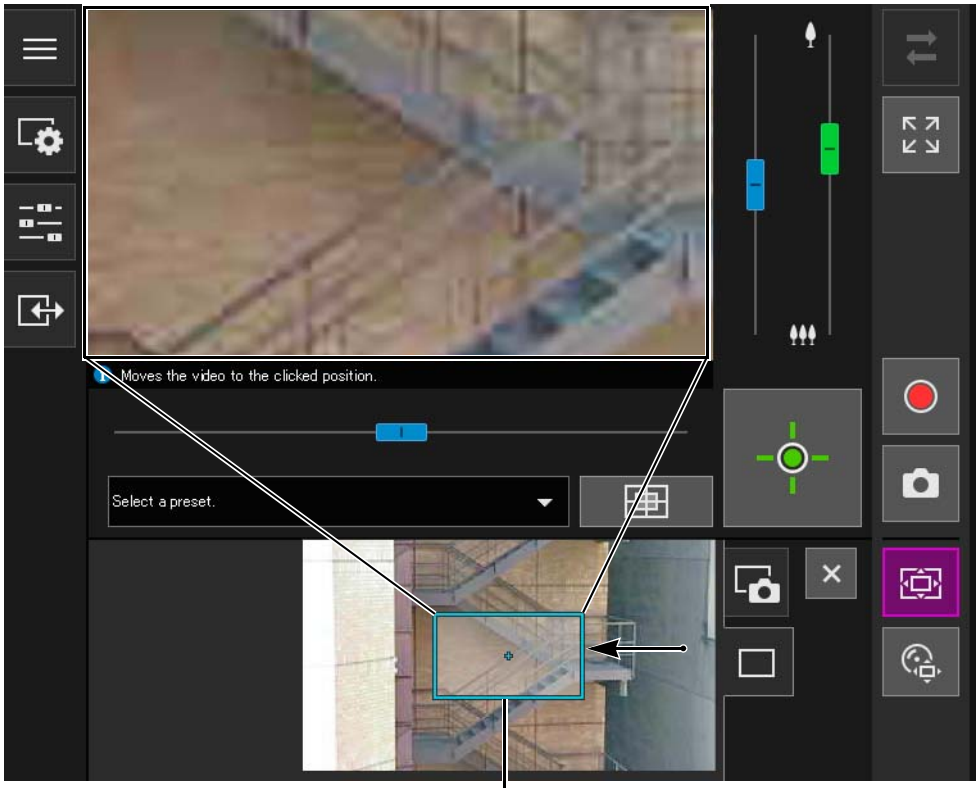
- You cannot record the video magnified with the Viewer PTZ.
- You can display the magnified video in full screen mode when using the Viewer PTZ.

1 Click the [Viewer PTZ] button.

The [Viewer PTZ] button changes active (purple), and the Viewer PTZ panel is shown in the control display area. Initially, the preview frame (light blue) surrounds the entire video.

2 In the Viewer PTZ panel, drag an edge of the preview frame to make it smaller.

The video of the area inside the preview frame is magnified to fill the video display area.



3 Move the frame to the area you would like to magnify and resize the frame as desired.

Move or Resize by Dragging

Press the mouse button inside the frame and drag it to move the preview frame.
If you press the mouse button and drag outside the frame, a new preview frame will be drawn.
You can resize the preview frame by dragging an edge of the frame.

Move by Clicking

If you click outside the frame, the preview frame will move and center on that point.

Move Using the Sliders/Resize

You can use the pan and tilt sliders in the video display area to move the preview frame. You can use the zoom slider to resize the image within preview frame.

Note

The Viewer PTZ uses digital zoom, so the higher the digital zoom ratio, the lower the quality of the video.

Exiting Viewer PTZ

The Viewer PTZ exits if you perform one of the following operations.

- Click the [Viewer PTZ] button to disable it.
- Click the [Digital PTZ] button to start the Digital PTZ.

Note

You can also perform the following operations to retain the zoomed view of the video display area without exiting the Viewer PTZ while the [Viewer PTZ] button is active (purple).

- Click the [Close] button on the control display area to close the Viewer PTZ panel.
- Click the snapshot tab to switch the panel in the control display area.

Cropping and Displaying Part of an Image (Digital PTZ)

You can use the Digital PTZ panel to crop and display part of a camera image in the image display area.

Note

If you enable Digital PTZ while receiving H.264 video, the received video is switched to JPEG.

Cropping Video With Digital PTZ Panel

1 Click the [Digital PTZ] button.

The [Digital PTZ] button changes active (purple), and the Digital PTZ panel is shown in the control display area.

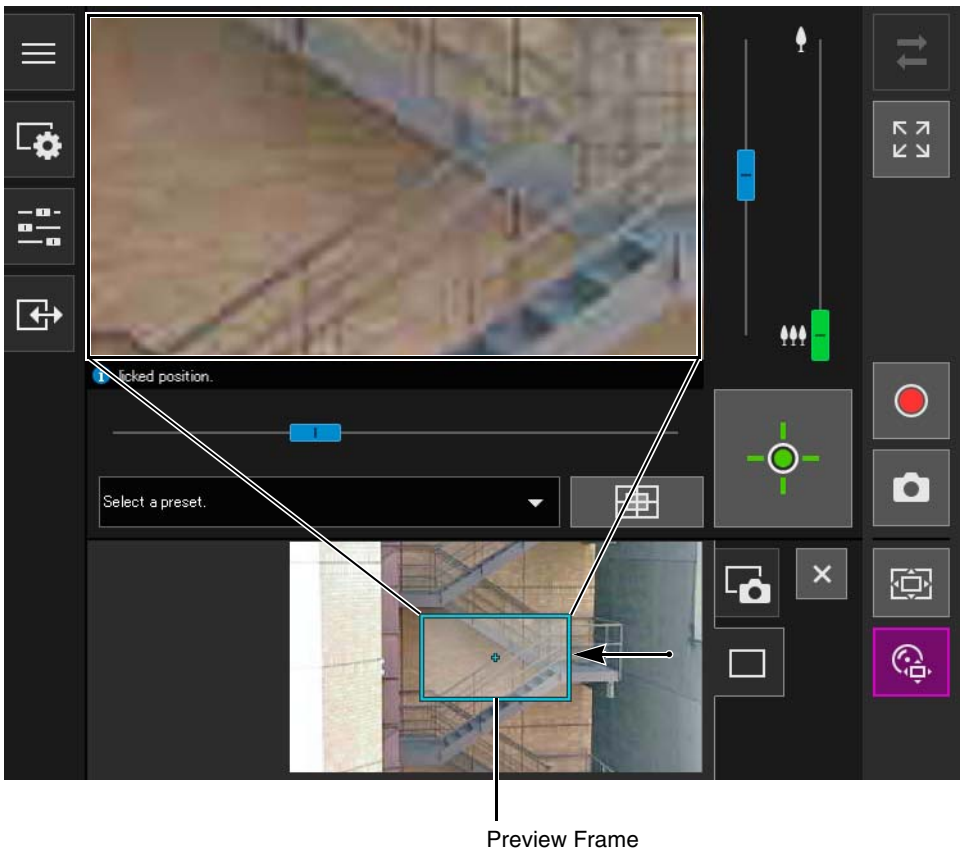
2 In the Digital PTZ panel, move and resize the preview frame.

The preview frame operations are the same as with the Viewer PTZ (P. 51).
The preview frame size can be set to one of the following five sizes: 640 x 360, 512 x 288, 384 x 216, 256 x 144, and 128 x 72.

Note

The preview frame will move in steps. Fine-tuned movement is not possible.

The video of the area inside the manipulated preview frame is magnified to fill the video display area.



Note

The Digital PTZ uses digital zoom, so the higher the digital zoom ratio, the lower the video quality.

Using Presets or the Home Position

You can use a registered preset or home position to specify the range for Digital PTZ.
If you select a preset, the preview frame on the Digital PTZ panel moves to the preset position, and the video inside the frame is shown in the video display area.

Note

Register presets in advance in [Camera] > [Preset] > [Register Preset] on the Setting Page (P. 92).

Exiting Digital PTZ

The Digital PTZ exits if you perform one of the following operations.

- Click the [Digital PTZ] button to disable it.
- Click the [Viewer PTZ] button to start the Viewer PTZ.

Note

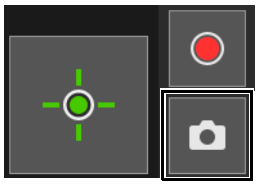
You can perform the following operations to continue Digital PTZ while the [Digital PTZ] button is active (purple).

- Click the [Close] button on the control display area to close the Digital PTZ panel.
- Click the snapshot tab to switch the panel in the control display area.

Saving Snapshots

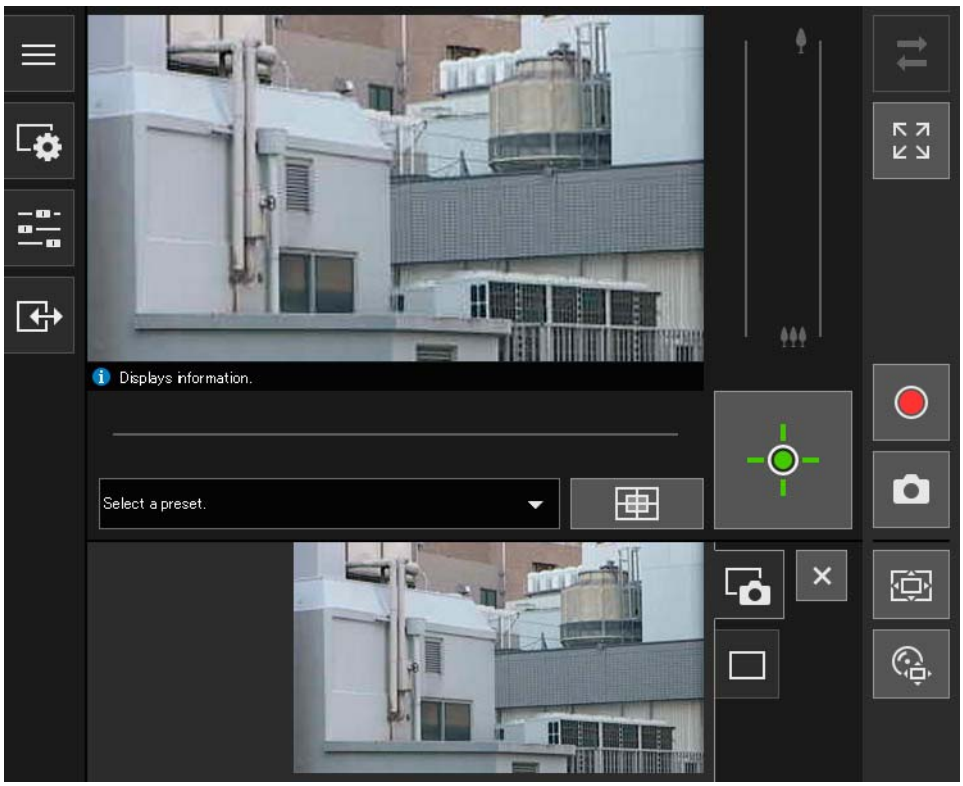
You can take snapshots while checking the video in the video display area.

1 Click the [Snapshot] button at the moment you want to capture a still image.



The snapshot panel is opened in the control display area and the still image from the instant that the button was clicked is displayed.
If you click the [Snapshot] button again, the image displayed in the Snapshot panel will be updated.

2 To save the snapshot, right-click on the Snapshot panel.



3 Click [Save picture as] in the menu that is displayed.

4 Enter the desired file name and save the snapshot.

Note

- The saving format of the snapshot depends on the web browser being used.
- The saved snapshots are the same size as the reception video size.

Recording Video to a Memory Card

Manually record video being shown in the video display area to a memory card inserted in the camera.

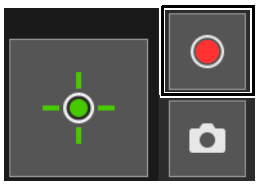
Note

- You can manually record video if the following conditions have been met.
  - The memory card inserted in the camera is mounted.
  - [Operation Settings] is set to [Save Logs and Videos] in [Memory Card] > [Memory Card Operations] (P. 155) on the Setting Page.
- The format and size of the video recorded to a memory card depends on the settings configured on the Setting Page.
  - Video format: [Memory Card] > [Memory Card Operations] > [Video Format] (P. 156)
  - Video size: JPEG [Basic] > [Video] > [JPEG] > [Video Size: Upload / Memory card]
    H.264 [Basic] > [Video] > [H.264(1)] or [H.264(2)] > [Video Size]

Recording Videos Manually

1 If you have not obtained camera control privileges, click the [Obtain/Release Camera Control Privileges] button to obtain the privileges.

2 Click the [Memory Card Recording] button.



The display of the [Memory Card Recording] button will change during video recording.


Recording


Recording (while camera control privileges are not obtained)


Not recording (while camera control privileges are obtained)


Not recording (while camera control privileges are not obtained, or when no memory card is mounted to the camera)

3 To stop video recording, click the [Memory Card Recording] button again.

Important

- Video manually recorded to the memory card will automatically be terminated after 300 seconds of recording.
- When recording manually, do not change the settings in the [Settings Page]. Doing so may result in the termination of the manual recording.
- While manually recording to the memory card, you can continue to record even if you release camera control privileges or disconnect the camera.

Confirming Recorded Video

Use the Recorded Video Utility to confirm and play back the video manually recorded to a memory card.
For details, please refer to “Recorded Video Utility User Manual”.

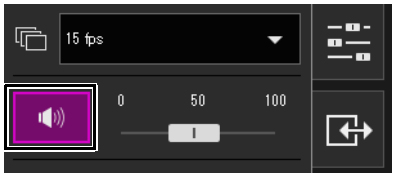
Receiving Audio

Open the [Video and Audio] menu to set the audio reception from the camera.

Receiving Audio

Receive audio from the microphone connected to the camera and play it back in the Viewer.

1 In the [Video and Audio] menu, click the [Audio Reception] button.



Audio reception starts.
The [Audio Reception] button icon will change to active (purple) while receiving audio.

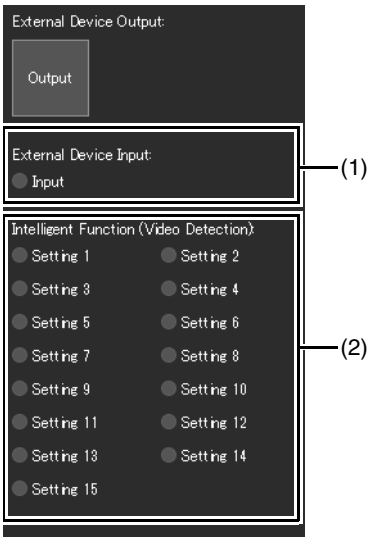
2 In [Output Volume], adjust the volume to an appropriate level using the slider.

Note

- To receive audio, you must connect the microphone to the camera and specify the type of the microphone from [Video and Audio] > [Audio] > [MIC Power] (P. 102) and set [Server] > [Audio Server] > [Audio Transmission from the Camera] to [Enable] (P. 107) on the Setting Page.
- While the icon is active (purple), audio is constantly received even if you close the [Video and Audio] menu.

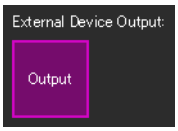
Checking the Status of Event Detection

In the [Event and Input/Output] menu, you can operate the output of an external device and check the status of input of the external device, and detection of intelligent functions.



Operating External Device Output

You can operate output for the external device set in [Event] > [External Device] (P. 116) on the Setting Page.
Click the icon to switch between the active (purple)/inactive (gray) status.
Example:



Output: Output active

Note

To operate [External Device Output] output, it is necessary to obtain camera control privileges.

Checking the Status of Event Detection

(1) **[External Device Input]**

Displays the input status of the external device set in [Event] > [External Device] (P. 117) on the Setting Page.
When a contact input signal is received from an external device, input will be activated and the icon becomes green.
Example:

Input: Input active

(2) [Intelligent Function (Video Detection)]

The status of video detection set in [Event] > [Intelligent Function] > [Video Detection] (P. 124) is displayed for each detection setting number. When the detection settings configured in Intelligent Function (Moving Object Detection, Abandoned Object Detection, Removed Object Detection, Camera Tampering Detection, Passing Detection, or Intrusion Detection) are triggered, the corresponding icon will turn green.

If a name is entered in [Detection Settings Name] in [Event] > [Intelligent Function] on the Setting Page (P. 128), that name is displayed in [Setting 1] - [Setting 15].

Example:

Setting 1: Video Detection status ON

Other settings: Video Detection status OFF

Note

The icon indicating the detection status will be displayed for a maximum of five minutes (except for Moving Object Detection).

Chapter 4

Setting Page

The Setting Page enables you to configure all the settings required for using the camera. Please configure the settings on the Setting page according to how the camera will be used, before you use the camera.
The Setting Page also provides menus for when the camera is in operation; for example, camera maintenance.

How to Use the Setting Page

This section explains operations up to displaying the Setting Page, and common Setting Page operations.

Note

- The Setting Page can only be operated by administrators.
- Use the Camera Management Tool in advance to configure the administrator account and network settings.

Accessing the Setting Page

Directly enter the IP address set in the Camera Management Tool into a web browser to display the Setting Page of the camera.

Note

You can also access the Setting Page from the Camera Management Tool. For details, please refer to “Camera Management Tool User Manual”.

1 Launch the web browser.

2 Enter the IP address, and press the Enter key.

The user authentication window is displayed.

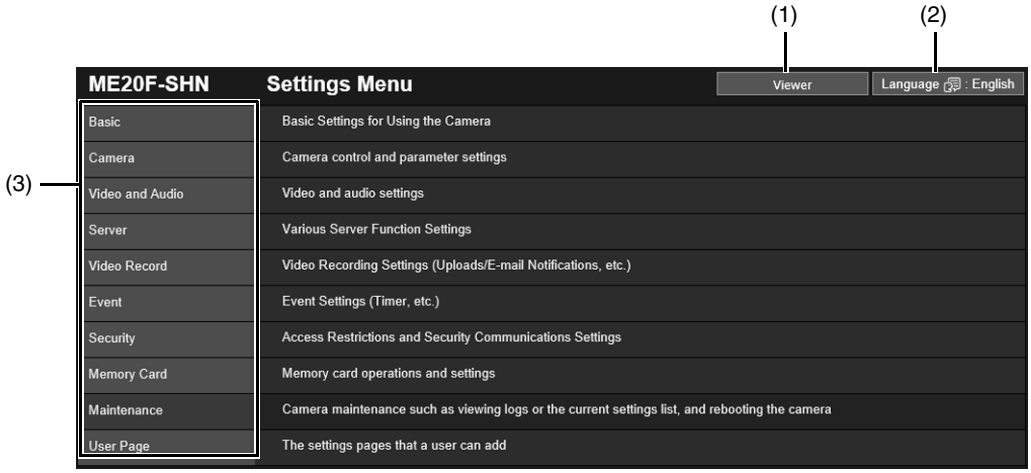
3 Enter the Administrator Name and Administrator Password and click [OK].

The Setting Page is displayed.

Note

The Viewer is displayed when [Basic] > [Viewer] > [General] > [Default Page] is set to [Display Viewer] in the setting menu (P. 79).

Settings Menu



(1) [Viewer] Button
Start the Camera Viewer (P. 31).

(2) Language Switch Button
Set the language to display on the screen.

(3) Setting Menus
If you click one of these items, its submenu (P. 66) will be displayed (excluding the [Memory Card] and [User Page] menus). Click a submenu to navigate to its Setting Page.

Important

- If you open another window or tab to access the camera while an authenticated web page is displayed, the authentication information of the displayed web page may be discarded. In this case, enter the authentication information again.
- To ensure security, exit the web browser after completing settings on the Setting Page and after using the Camera Viewer.
- Do not open multiple Setting Pages at one time and try to change the settings of a single camera.

Common Setting Page Operations

This section explains basic Setting Page operations, and operations common to all Setting Pages.

Note

If you have enabled settings in your web browser to not display dialog boxes, you may be unable to perform operations on the Setting Page. If this happens, exit your web browser and launch it again.

Applying Changes to Settings

If you change a setting on the Setting Page, the [Apply] and [Clear] buttons on the upper right or lower right of the screen is no longer grayed out and can be clicked.

Click [Apply] in this state to apply the changed settings.
Click [Clear] to revert to the previous settings.

Note

Changes in [Camera] > [Camera] will be applied immediately since there are no [Apply] or [Clear] buttons.

Setting Changes Requiring Rebooting

Items that require the camera to be rebooted in order to apply the changed settings are indicated with an orange symbol to their right.

When any item indicated with an orange symbol is changed, [Apply] displayed at the upper right and lower right of each Setting Page changes to [Apply and reboot].

Click [Apply and reboot] to apply the changed settings and reboot the camera.
Click [Clear] to revert to the previous settings.

Important

Setting changes will be lost if you navigate to another Setting Page without clicking [Apply] or [Apply and reboot]. Be sure to click [Apply] or [Apply and reboot] to apply the changed settings.

Return to the Settings Menu

Click [Settings Menu] at the upper right of each Setting Page to return to the setting menu.

Important

Do not use the [Back] or [Forward] buttons in the web browser to navigate Setting Pages. The changed settings may revert to the original settings or unwanted setting changes may be applied.

Help

Click [Help] at the beginning of any setting item to display a detailed explanation of that setting item.

Setting Ranges and Character Limits

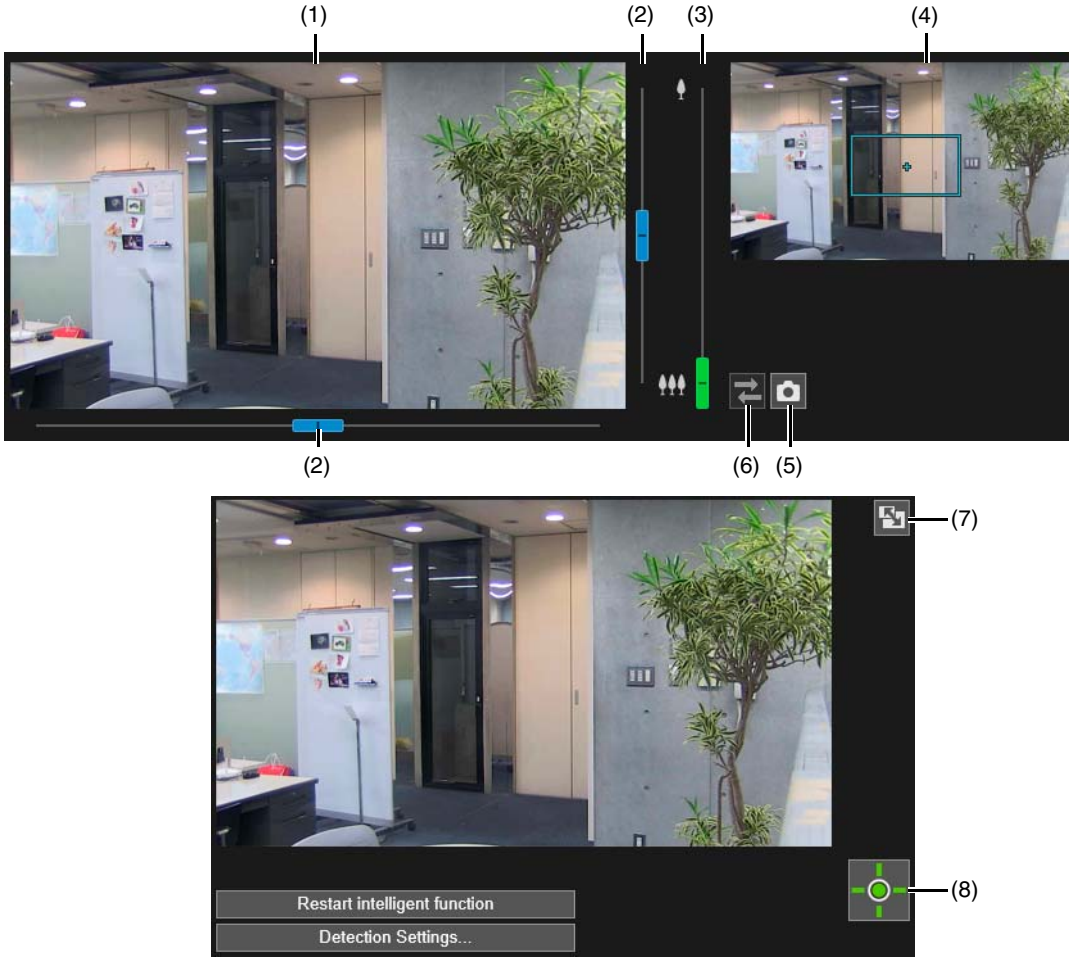
For settings where you must enter numerical values or characters, the setting range or limits on the number of characters will be displayed.
Please enter the settings within the displayed limits.

Operating the Video Display Area

Some Setting Pages such as [Camera], [Preset] and [Intelligent Function] can be configured using the video display area.

Note

- The displayed items will change depending on the Setting Page.
- Other users cannot access the Viewer while video is being displayed on the Setting Page. Also, video cannot be displayed or configured while the administrator is connected to the Viewer or color bars are being output (refer to "Setup Guide").



(1) Video Display Area
Camera video is displayed here. Use the mouse to set the areas, etc. The operations on the video display area are the same as in the Viewer (P. 46).

(2) Pan/Tilt Slider
Pan and tilt operations are the same as in the Viewer (P. 46).

(3) Zoom Slider
Zoom operations are the same as in the Viewer (P. 46).

(4) Full-View Screen
Displays the full range of motion of the camera. You can set areas, etc. using mouse operations on the full-view screen for some Setting Pages.

(5) [Snapshot] Button
Open the snapshot window and display a still image of the moment you clicked the button (P. 55).

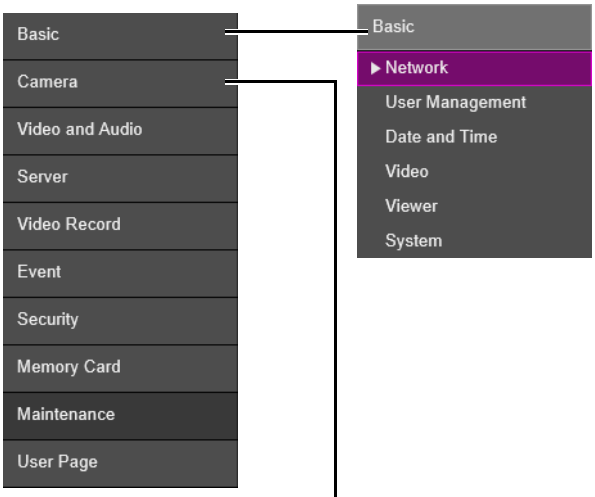
(6) [Reconnect] Button
Reconnects to the camera. You can use this when not connecting to the camera.

(7) [Screen Resize] Button
The size of the video display area is switched each time this button is clicked.

(8) [Obtain/Release Camera Control Privileges] Button
Click this to obtain and release the camera control privileges (P. 45).

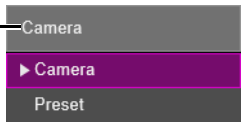
About Each Setting Page

This section will give an overview of each item in the Settings Menu and each submenu.
Each of the [Basic], [Video and Audio], and [Video Record] menus has a [Video] submenu, but the functions are all common. The functions can be set in any of the menus and the settings will be reflected in all of the [Video] submenus.



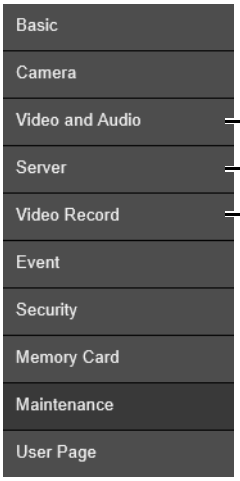
Basic

- Network (P. 69)
  Network settings for connecting to the camera.
- User Management (P. 73)
  Use this to change administrator account information, add/delete authorized users and set privileges for users.
  The settings of this item are the same as those in [Security] > [User Management]. Settings configured on one page are also reflected on the other.
- Date and Time (P. 75)
  Camera date and time settings.
- Video (P. 77)
  General video settings, such as the size and quality of video transmitted from the camera.
- Viewer (P. 79)
  Configure the startup, authorization, and view of the Viewer.
- System (P. 80)
  Specify the camera name and external input/output devices, and configure the system and installation of the camera.

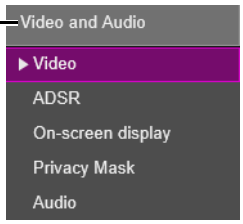


Camera

- Camera (P. 83)
  Select the camera mode for settings such as video quality compensation.
- Preset (P. 92)
  Register a series of settings as a preset.

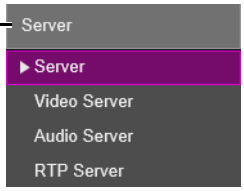


Video and Audio



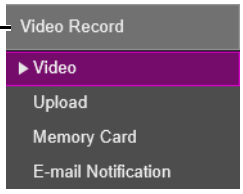
- Video (P. 77)
- ADSR (P. 95)
  ADSR is an abbreviation for Area-specific Data Size Reduction.
  Reduces the data size of transmitted H.264 video by reducing the video quality of unspecified area.
- On-screen display (P. 97)
  Displays the date and time, camera name and other text on the Video.
- Privacy Mask (P. 99)
  Configure a mask for the areas of the camera video you want to mask.
- Audio (P. 102)
  Settings for the power of the microphone connected to the camera.

Server

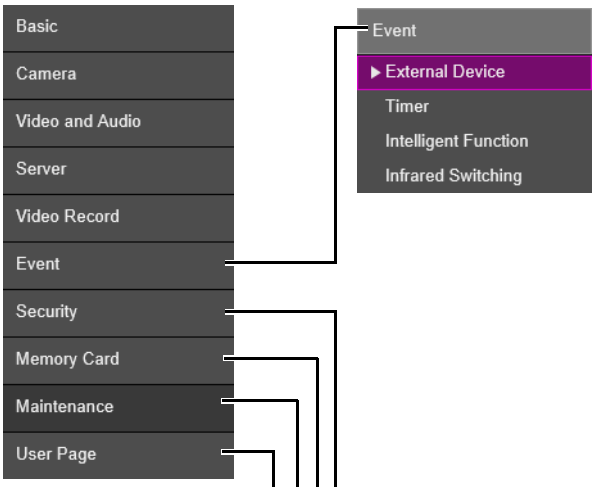


- Server (P. 103)
  Settings for HTTP server, SNMP server, FTP server usage or WS-Security time checks.
- Video Server (P. 106)
  Settings for clients that can be connected to a video server.
- Audio Server (P. 107)
  Settings for audio transmission from the camera to the computer.
- RTP Server (P. 108)
  Settings for RTP streaming.

Video Record



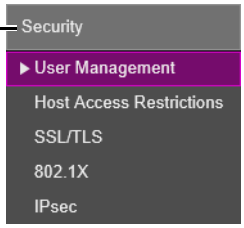
- Video (P. 77)
- Upload (P. 110)
  Settings for uploading video via HTTP or FTP when an event is triggered.
- Memory Card (P. 155)
  Perform memory card operations or configure settings. The settings of this item are the same as those of the [Memory Card] menu. Settings configured on one page are also reflected on the other.
- E-mail Notification (P. 114)
  Settings for sending an e-mail notification to a specified recipient when an event is triggered.



Event

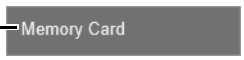
- External Device (P. 116)
  Operation settings for external device output and for external device input triggered events.
- Timer (P. 118)
  The timer function can generate events that can trigger operations, such as video recording, and e-mail notification at regular intervals.
- Intelligent Function (P. 120)
  Configure the intelligent functions such as moving object detection, camera tampering detection, and intrusion detection.
- Infrared Switching (P. 143)
  The camera angle can be moved to preset positions when

Security



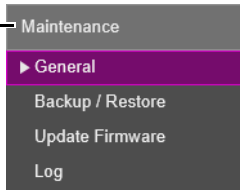
- User Management (P. 73)
  The settings of this item are the same as those of the [User Management] in [Basic] menu. Settings configured on one page are also reflected on the other.
- Host Access Restrictions (P. 144)
  Separate access control from IPv4 and IPv6 addresses can be set.
- SSL/TLS (P. 146)
  Certificate creation and management, and encrypted communication settings.
- 802.1X (P. 149)
  Settings for 802.1X authentication and authentication status display, and for certificate management.
- IPsec (P. 151)
  Settings for using IPsec.

Memory Card (P. 155)



Settings for recording video to a memory card when an event is triggered.
The settings of this item are the same as those in [Video Record] > [Memory Card]. Settings configured on one page are also reflected on the other.

Maintenance



- General (P. 158)
  Check the device information/settings, and licenses, and reboot and initialize the device, etc.
- Backup / Restore (P. 160)
  Perform backup and restoration.
- Update Firmware (P. 161)
  Perform firmware updates.
- Log (P. 162)
  Display logs and configure log notification.

User Page

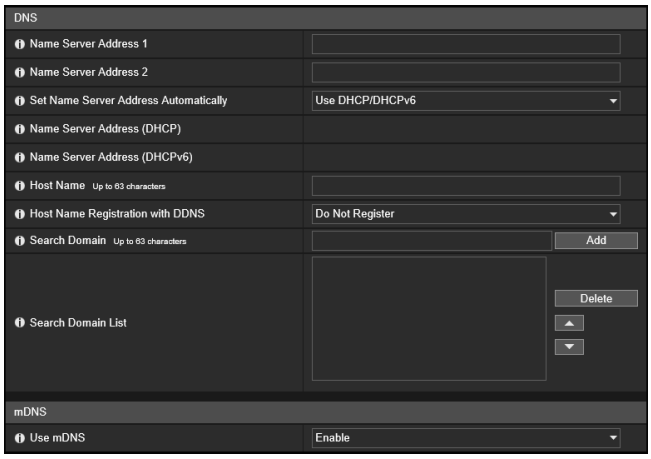
Link to web page customized by the user.
For information on the User Page, contact a Canon Customer Service Center.

[Basic] > [Network]
Configuring Network Settings

Network settings for connecting to the camera.

The following settings can be configured here.

- LAN
- IPv4
- IPv6
- DNS
- mDNS



Important

If any network settings are changed, the camera may become inaccessible from the active web browser. In this case, a confirmation dialog box will be displayed when you click [Apply] or [Apply and reboot]. Click [OK] to apply the new settings.
If you reboot the camera after changing settings and cannot connect to the camera from the web browser, any available URI for connecting to the camera will be displayed in a message. If you cannot connect to the camera through the displayed URI, contact your system administrator.

LAN

Set the LAN communication method and size of video transmitted from the camera.

[LAN Interface]
Select the interface suited to the device for connecting to the camera. Generally use [Auto].

[Maximum Packet Size]
Enter the maximum packet size to be transmitted by the camera. Normally there is no need to change the default setting of 1500.
A setting of 1280 or greater is necessary when using IPv6.
When using ADSL, setting a slightly lower value may increase transmission efficiency.

IPv4

Settings for using IPv4 to connect to the camera. The IPv4 address can be assigned by the DHCP server automatically or set manually.

Important

- Contact your System Administrator for the [IPv4 Address], [Subnet Mask] and [IPv4 Default Gateway Address] if you set the IPv4 address manually.
- If any of the [IPv4 Address], [Subnet Mask] or [IPv4 Default Gateway Address] settings are wrong, the camera may become inaccessible via the network. If this occurs, use the Camera Management Tool to reset the address.

[IPv4 Address Settings Method]
Select the method for setting the IPv4 address.
For [Manual], enter a fixed IPv4 address into [IPv4 Address].
For [Auto (DHCP)], the settings acquired from the DHCP server will be automatically entered in [IPv4 Address], [Subnet Mask] and [IPv4 Default Gateway Address].

Important

If [Auto (DHCP)] is selected as the IPv4 address setting method, the IPv4 address may not be assigned correctly in certain environments, such as when a router is present between the DHCP server and the camera. If this occurs, select [Manual] and enter a fixed IPv4 address.

[IPv4 Address]
When [IPv4 Address Settings Method] is set to [Manual], enter a fixed IPv4 address.

[Subnet Mask]
When [IPv4 Address Settings Method] is set to [Manual], enter the designated subnet mask values for each network.

[IPv4 Default Gateway Address]
When [IPv4 Address Settings Method] is set to [Manual], enter a default gateway IP address. Be sure to set this when connecting the camera to a different subnet from that of the Viewer.

[AutoIP]
Select this to enable or disable AutoIP.

[IPv4 Address (AutoIP)]
When [AutoIP] is set to [Enable], an automatically set IPv4 address is displayed.

IPv6

Settings for using IPv6 to connect to the camera. The IPv6 address can be assigned by the RA or DHCPv6 server automatically or set manually.

Important

Contact your System Administrator for the [IPv6 Address (Manual)], [Prefix Length] and [IPv6 Default Gateway Address] if you set the IPv6 address manually.

[IPv6]
Select this to enable or disable IPv6.

[Auto (RA)]
Select [Enable] to set an address automatically using RA (Router Advertisement, network information automatically transmitted from a router).

[Auto (DHCPv6)]
Select [Enable] to use DHCPv6 to set an address automatically.

[IPv6 Address (Manual)]
Enter a fixed IPv6 address if you set the address manually.

[Prefix Length]
Enter a prefix length if [Disable] is specified in [Auto (RA)].

[IPv6 Default Gateway Address]
Enter a default gateway address if [Disable] is specified in [Auto (RA)]. Be sure to set this when connecting the camera to a different subnet from that of the Viewer.

[IPv6 Address (Auto)]
If [Enable] is specified in [IPv6] and [Enable] is specified in [Auto (RA)] and [Auto (DHCPv6)], then the automatically acquired address will be displayed.

Note

In an environment where IPv6 cannot be used, and IPv6/Auto is set to [Enable], then only the link-local address will be displayed in the [IPv6 Address (Auto)] field.

DNS

Set the DNS server address. The DNS server address can be set manually or automatically assigned by a DHCP/DHCPv6 server.

[Name Server Address 1], [Name Server Address 2]
Enter the name server address you want to register. To register only one address, keep the [Name Server Address 2] field blank.

Note

If [Name Server Address 1] is unavailable, [Name Server Address 2] will be accessed. However, [Name Server Address 2] must be set in advance.

[Set Name Server Address Automatically]
Select the server to use for automatically setting the name server address.
To set [Use DHCP], select [Auto (DHCP)] in [IPv4 Address Settings Method] (P. 70).
To set [Use DHCPv6], select [Enable] in [IPv6], then select [Enable] in [Auto (DHCPv6)] (P. 70).

[Name Server Address (DHCP)]
Select [Use DHCP] or [Use DHCP/DHCPv6] in [Set Name Server Address Automatically] to display the name server address acquired from the DHCP server.

[Name Server Address (DHCPv6)]
Select [Use DHCPv6] or [Use DHCP/DHCPv6] in [Set Name Server Address Automatically] to display the name server address acquired from the DHCPv6 server.

[Host Name]
You can register the camera host name in the name server using alphanumeric characters.
Do not use "_" (underscore) in the host name in Internet Explorer 9/10/11.

[Host Name Registration with DDNS]
When you enter a name into [Host Name] and select [Register], the host name will be registered in the name server. Registering the host name to DDNS is useful when operating with [IPv4 Address Settings Method] set to [Auto (DHCP)] (P. 70). DNS server registration settings must be set in advance. Contact your system administrator for the DNS server settings.

[Search Domain]
Enter a domain name and click [Add] to add the domain name to the Search Domain List.
Specify the host name without specifying a domain name for a server, such as the upload server, to search domains in the form "host name + domain name", when the domain names are specified in the Search Domain List.
Do not use "_" (underscore) in the domain name in Internet Explorer 9/10/11.

[Search Domain List]
A list of domain names added using [Search Domain].
The function queries the DNS server for each domain name starting from the top of the list.
Use the ▲▼ buttons on the right to change the order of the domain names.
To delete a domain name, select one from the list and then click [Delete].

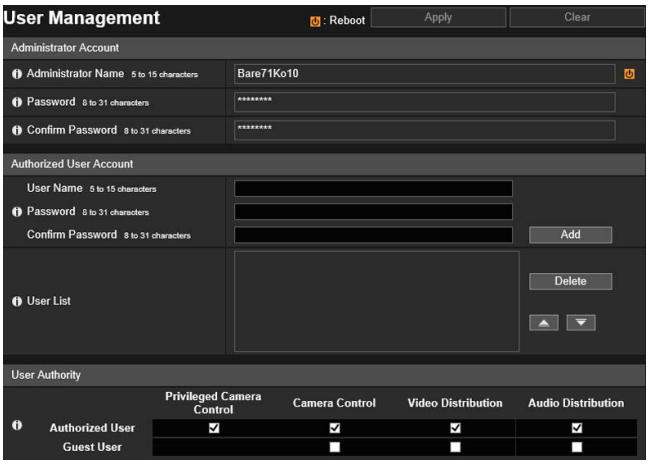
mDNS

This will configure settings for using multicast DNS. If you use mDNS, the IP address and host name of the camera will be broadcast to other hosts on the network.

[Use mDNS]
Select this to enable or disable mDNS.

[Basic] > [User Management]
Configuring Accounts and Privileges

You can change the administrator account, add new authorized users, and set the privileges for authorized users and guest users.
For details on user privileges, please refer to “Camera Viewer Access Restrictions” (P. 33).
[User Management] is the same as [Security] > [User Management]. Settings configured on one [User Management] page are also reflected on the other.



The following settings can be configured here.
- Administrator Account
- Authorized User Account
- User Authority

Administrator Account

Set this when changing the account information for the administrator.

Important

- To ensure system security, register a strong administrator password that cannot be easily guessed by a third party. Do not forget the password.
- If you forget the administrator password, restore the factory default settings (P. 185). Note, however, that this will reset all camera settings to factory default settings including the administrator account, the network information, date and time.

[Administrator Name]
Enter the administrator name using alphanumeric characters, hyphens "-", and underscores "_". However, "-" and "_" characters are unable to be used at the beginning of the sentence.

[Password]
Enter the administrator password.
If the Camera Viewer, etc., are connected, terminate the connection before changing the password.

[Confirm Password]
Enter the same password as above for confirmation.

Authorized User Account

Add authorized users.

[User Name], [Password], [Confirm Password]
To add the authorized user, enter the user name and password, then click [Add].
Enter the user name using alphanumeric characters, hyphens "-", and underscores "_".
Up to 50 authorized users can be added.

[User List]
Displays a list of added authorized users.
The order of the list can be changed with the ▲▼ buttons on the right.
To delete an authorized user from the list, select the user and click [Delete].

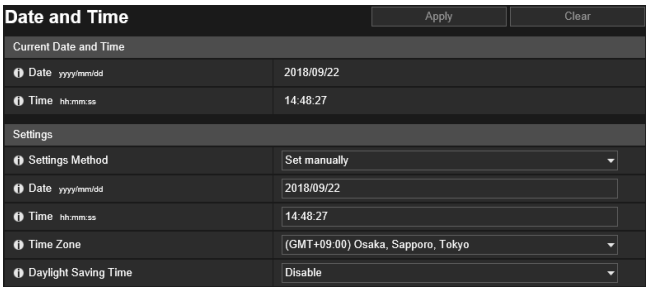
User Authority

Set the privileges for authorized users and guest users. This setting enables you to set access restrictions for the Camera Viewer (P. 33).

[Privileged Camera Control], [Camera Control], [Video Distribution], [Audio Distribution]
Select the items for granting users privileges.
An authorized user has higher privileges than a guest user.

[Basic] > [Date and Time]
Setting the Date/Time

Camera date and time settings.



The following settings can be configured here.
- Current Date and Time
- Settings

Current Date and Time

The date and time set in the camera are displayed.

Settings

Set the date and time setting method, time zone and daylight saving time for the camera.

[Settings Method]
Select the date and time setting method.

[Set manually]
Set the desired date and time in [Date] and [Time].
Set the time in 24-hour format in <hour:minute:second> order.

[Synchronize with NTP server]
Synchronize with the time of NTP server specified in the displayed [Set NTP Server Settings Automatically].

[Set NTP Server Settings Automatically]
Select one of the following setting methods.

[Disable]
Enter the IP address or host name of the NTP server in [NTP Server].

[Use DHCP]
The camera time is synchronized with the time of the NTP server at the address acquired from the DHCP server.
The acquired NTP server address is displayed in [NTP Server (DHCP)].
In order to set [Use DHCP], you must change [Network] > [IPv4] > [IPv4 Address Settings Method] to [Auto (DHCP)] (P. 70).

[Use DHCPv6]
The camera time is synchronized with the time of the NTP server at the address acquired from the DHCPv6 server.
The acquired NTP server address is displayed in [NTP Server (DHCPv6)].
In order to set [Use DHCPv6], you must change [Network] > [IPv6] > [IPv6] to [Enable], then set [Auto (DHCPv6)] to [Enable] (P. 70).

[Use DHCP/DHCPv6]
The camera time is synchronized with the time of the NTP server at the address acquired from the DHCP server or DHCPv6 server.
If the NTP server address can be acquired from both the DHCP server (IPv4) and DHCPv6 server, the NTP server address acquired from the DHCP server (IPv4) will be used.

[Synchronization Interval (minutes)]
Enter the synchronization interval for the specified NTP server.

[Last Sync Time]
The time last synchronized with the specified NTP server will be displayed.

[Synchronize with computer time]
The date and time will be synchronized with that of the computer currently accessing the camera. After clicking [Apply], [Settings Method] will change to [Set manually].
[Time Zone] is not automatically selected, so set it if necessary.

Note

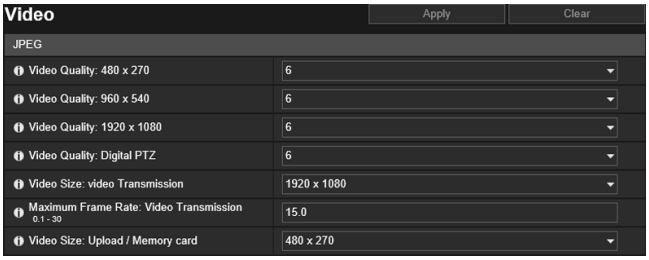
If the NTP server IP address is incorrect or a connection with the NTP server cannot otherwise be established, [Last Sync Time] will not be updated, or will be blank.

[Time Zone]
Select the appropriate time zone.
When the time zone is changed and [Apply] is selected, the date and time will be automatically changed based on the selected time zone.

[Daylight Saving Time]
Select whether to automatically adjust for daylight saving time to suit the time zone.

[Basic] > [Video]
Setting Video Size and Quality

General video settings, such as the size and quality of JPEG and H.264 video transmitted from the camera.
[Video] is common with [Video] found in [Video and Audio] and [Video Record]. A setting configured in any of the [Video] submenus will be reflected in the other [Video] submenus as well.



The following settings can be configured here.
- JPEG
- H.264(1)
- H.264(2)

Important

- The following may occur if video size, video quality and target bit rate are set higher, as this increases network load and data size per frame.
  - JPEG: The frame rate may drop
  - H.264: Video may be temporarily disrupted
- In case of H.264 video, block noise may become noticeable if a large video size and low target bit rate are set.
- The data size may increase depending on the type or movement of the subject. If the frame rate remains low or other undesirable conditions continue for a prolonged period, lower the video size or quality setting.

JPEG

You can configure settings for the quality and size of JPEG video transmitted from the camera, as well as, the video size when recording the camera video.

[Video Quality]
Select the video quality transmitted from the camera for each video size.
Greater values have higher quality.

[Video Quality: Digital PTZ]
Select the video quality for digital PTZ.

[Video Size: video Transmission]
Select the default video size transmitted from the camera when no video size has been specified by the Viewer.

[Maximum Frame Rate: Video Transmission]
Limit the maximum frame rate per second transmitted to reduce the viewer load. Up to 30 frames per second can be set.

[Video Size: Upload / Memory card]
Select the size of video when using the upload function (P. 110) or when recording to a memory card (P. 155).
Set whether to upload a video or record it to a memory card with [Video Record] > [Upload] or [Memory Card] > [Video Record Action] (P. 110).

H.264(1)

Settings for H.264(1) video transmitted from the camera.

[Video Size]
Select the size of the video transmitted from the camera.

[Bit Rate Control]
Set the video bit rate.
If you select [Use bit rate control (constant bit rate)], please set [Target Bit Rate (kbps)]. If you select [Do not use bit rate control (variable bit rate)], please set [Video Quality].

[Target Bit Rate (kbps)]
You can select the target bit rate if [Bit Rate Control] is set to [Use bit rate control (constant bit rate)].

[Video Quality]
You can select the video quality if [Bit Rate Control] is set to [Do not use bit rate control (variable bit rate)].
Greater values have higher quality.

[Frame Rate (fps)]
Select the video frame rate.

[I Frame Interval (sec)]
Select the I frame interval (sec) for H.264 video.

Important

- When [H.264(1)] or [H.264(2)] video is used for memory card recording and upload, the following restrictions apply to the setting.
  - [Bit Rate Control]: [Use bit rate control (constant bit rate)] only
  - [Target Bit Rate (kbps)]: [3072] or less
  - [I Frame Interval (sec)]: either [0.5], [1], or [1.5]
- When dual streaming H.264 videos, setting the video size for H.264(1) and H.264(2) to the following combinations restricts the frame rate to a maximum of 15 fps. For all other combinations, a frame rate of up to 30 fps can be selected.

H.264(1)	H.264(2)
1920 x 1080	All sizes
All sizes	1920 x 1080

H.264(2)

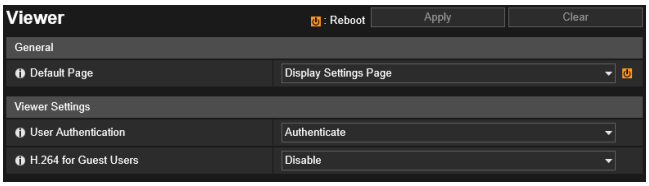
Settings for H.264(2) video transmitted from the camera.

[H.264(2)]
Select [Enable] to dual stream H.264 video.

[Video Size], [Bit Rate Control], [Target Bit Rate (kbps)], [Video Quality], [Frame Rate (fps)], [I Frame Interval (sec)]
Please refer to each setting in “H.264(1)”.

[Basic] > [Viewer]
Configuring the Viewer

Configure the startup, authorization, and view of the Viewer.



The following settings can be configured here.
- General
- Viewer Settings

General

[Default Page]
Sets the Setting Page or the Viewer as the first page to display when the camera is connected.
If users other than the administrator use the Viewer, set [Default Page] to [Display Viewer].

Viewer Settings

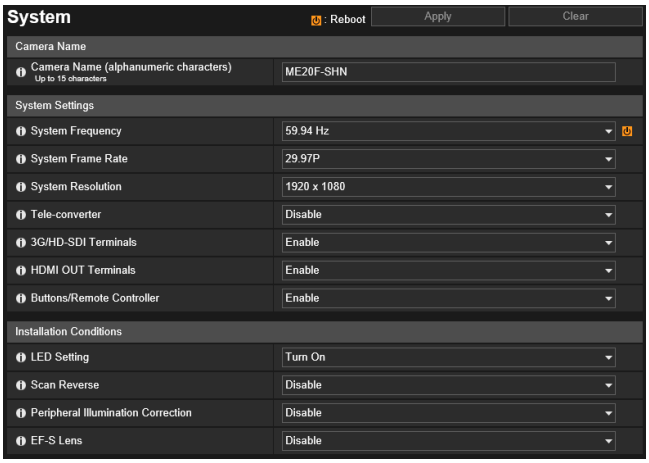
[User Authentication]
Displays the user authentication screen when the camera is connected to the Viewer (P. 31). If you select [Authenticate], only the administrator or an authorized user (P. 73) can connect.

[H.264 for Guest Users]
Set whether guest users may receive H.264 video. If you select [Enable], the [H.264] button will be displayed even when a guest user connects to the viewer (P. 37).
If you select [Enable], the [CANON SOFTWARE LICENSE AGREEMENT] dialog box is displayed. Click [Yes] to accept the terms of the license agreement.

Important
Additional H.264 licenses are required to receive H.264 video on multiple computers (P. 14). Select [Disable] for environments in which license management cannot be performed, such as environments in which multiple unspecified users access the camera.

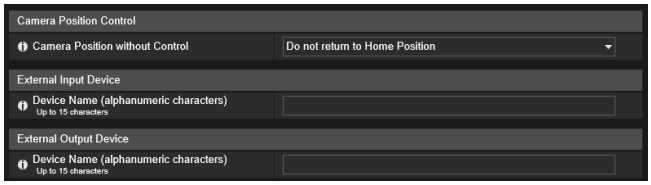
[Basic] > [System]
Setting General Camera Controls

Specify the camera name and external input/output devices, and configure the system and installation of the camera.



The following settings can be configured here.

- Camera Name
- System Settings
- Installation Conditions
- Camera Position Control
- External Input Device
- External Output Device



Camera Name

Set the camera name.

[Camera Name]
Enter any camera name. Be sure to enter a name in [Camera Name].

Note

The camera name to be specified here is different from that to be entered using buttons on the back of the camera.

System Settings

Select the video signal format, tele-converter settings, and whether to use video and audio output terminals, buttons on the back of the camera, and a remote controller.

Important

The combination of the video signal format that can be used as network-distributed video is as follows.
[System Frequency]: [59.94 Hz]
[System Frame Rate]: [29.97P]
[System Resolution]: [1920 x 1080]

For combinations other than the above, the network-distributed video will be black images.

Note

Depending on the setting value of [System Frequency] or [System Frame Rate], nothing may be displayed on the external monitor. Please refer to "Troubleshooting" of "Button Operation Guide" and change the settings.

[System Frequency]
Select [59.94 Hz] for the network-distributed video.
When you change [System Frequency], [System Frame Rate] is automatically updated.

[System Frame Rate]
Select [29.97P] for the network-distributed video.
Available setting options vary depending on the value of [System Frequency].

[System Resolution]
Select [1920 x 1080] for the network-distributed video.

[Tele-converter]
Select the digital zoom ratio. Note that the image is digitally processed so the image will deteriorate.

[3G/HD-SDI Terminals]
Select whether to enable or disable video and audio output from the 3G/HD-SDI terminal.
If you select [Disable], video and audio will not be output to an external monitor or recorder connected to the 3G/HD-SDI terminal.

[HDMI OUT Terminals]
Select whether to enable or disable video and audio output from the HDMI OUT terminal.
If you select [Disable], video and audio will not be output to an external monitor or recorder connected to the HDMI OUT terminal.

[Buttons/Remote Controller]
Select whether to enable or disable button operations on the back of the camera and the operation via a remote controller.
If you select [Disable], camera button and remote controller operations will be unavailable.

Note

- Even if [Buttons/Remote Controller] is set to [Disable], the RESET and REBOOT switches on the back of the camera will not be disabled.
- Even if [Buttons/Remote Controller] is set to [Disable], the following dials/buttons on the optional RC-V100 Remote Controller will not be disabled.

CAMERA POWER button
BLACK GAMMA LEVEL dial
WHITE BALANCE B dial
ZOOM dial
MASTER PEDESTAL dial
KNEE POINT dial
SHARPNESS LEVEL dial
MASTER BLACK R dial
FOCUS dial
IRIS dial
KNEE SLOPE dial
WHITE BALANCE R dial
MASTER BLACK B dial
ACTIVE button

Installation Conditions

Configure settings for camera use suitable for the location the camera will be installed.

[LED Setting]
Select whether to turn on the LED indicating the camera operation status.
If you select [Turn On], the LED will light up when turning the power on, rebooting, and during normal use.
When [Turn Off] is selected, the LED will light for several seconds during startup and then turn off.
Regardless of the setting, the LED will flash when initializing the settings.

[Scan Reverse]
Select the reversing direction of the video.
Select the setting suited to the camera installation method, such as ceiling mounting or placing on a desk.

[Peripheral Illumination Correction]
Select whether to use the peripheral illumination correction.
Specifying [Enable] corrects darkened image corners caused by lens characteristics.
Note that depending on the shooting conditions, noise may appear in the periphery of the image as a result of the correction.

[EF-S Lens]
When using an EF-S lens or EF Cinema lens with this camera, the peripheral illumination fall-off or vignetting may occur. In such a case, use this setting to change the segmenting range of the sensor.
Specifying [Enable] digitally enlarges the image by a factor of approximately 1.55, so the image will deteriorate.

Camera Position Control

Settings for camera use when there are no camera control restrictions for users or requests for camera control privileges.

[Camera Position without Control]
Select the camera operation when there are no users with camera control privileges.

If [Return to Home Position] has been selected, the home position of the camera must be set in advance with [Camera] > [Preset] > [Register Preset] (P. 92).

External Input Device

Enter each device name in order to identify the corresponding external input device being connected.

[Device Name]
Enter the name of the device connected to the external input device terminal.

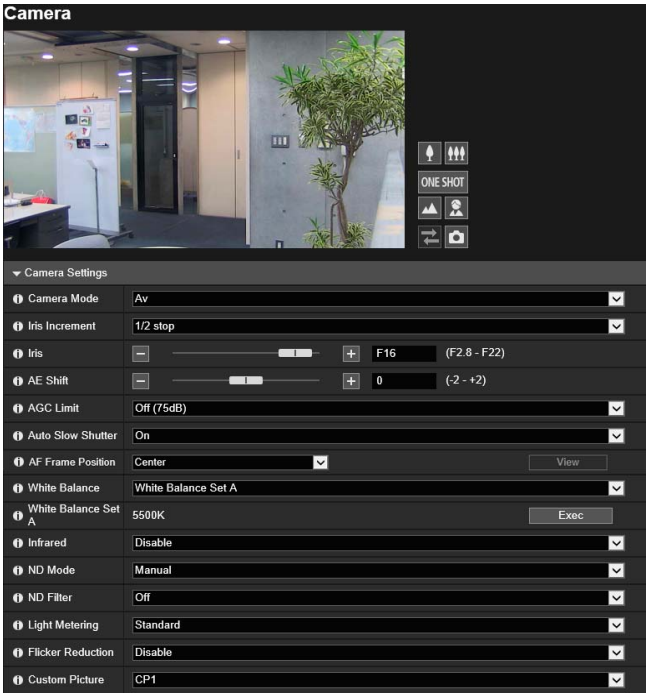
External Output Device

Enter each device name in order to identify the corresponding external output device being connected.

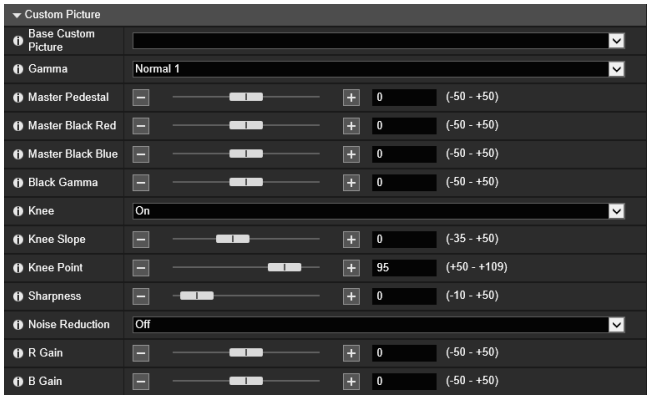
[Device Name]
Enter the name of the device connected to the external output device terminal.

[Camera] > [Camera]
Configuring Video Settings

Configure settings such as video quality compensation. If you change settings, the changes are immediately reflected in the video display area and Viewer.



The following settings can be configured here.
- Adjusting the Focus
- Camera Settings
- Custom Picture



Note

When a power zoom lens is attached, (Zoom in) / (Zoom out) buttons are displayed. For information on the button operation, please refer to P. 47.

Adjusting the Focus

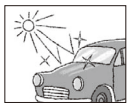
The camera offers two focusing methods: one-shot AF and manual focus.
Clicking ONE SHOT (One-shot AF) on the side of video display automatically adjusts the focus once, and then switches to the manual mode.
You can click and hold the (Near) and (Far) buttons to adjust the focus in the near and far directions.

The following procedure enables you to adjust the focus appropriately.

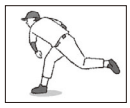
1. Select [Av] in [Camera Mode], and move the iris slider to the left limit to fully open the aperture. The depth of field becomes shallow, and you can adjust the focus appropriately.
2. Adjust focus by manual focus or one-shot AF.
   Manual Focus: [Adjust Focus] > continue pressing [Near] or [Far] button.
   One-shot AF: Select [Center] or [Selectable] in the [AF Frame Position] and click [One-shot AF] button (for details on [AF Frame Position], refer to P. 85).
3. When you have finished adjusting the focus, change [Camera Mode] to an appropriate setting.

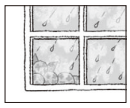
Set the focus mode switch on the attached lens to AF or SERVO in advance.

Difficult to Focus with One-shot AF


Reflective surfaces


Subjects with low contrast or without vertical lines


Fast moving subjects


Through dirty or wet windows


Low-light scenes

Important

- If [Shutter Speed] is set to 1/4, 1/5, or 1/6, one-shot AF is not available.
- Be aware of the following when adjusting the focus:
  - If you operate the zoom after focusing, the focus on the subject may be lost.
  - When adjusting the focus, be careful not to touch the front of the lens or moving parts on the lens except for the focus ring.
- When adjusting the focus with one-shot AF, also be aware of the following:
  - Autofocus may not work well when high [Gain] levels are set.
  - Autofocus may not work well when [Gamma] is set to [Wide DR] or [Canon Log] in [Custom Picture].
  - The point where the camera focuses may change slightly depending on shooting conditions, such as subject, brightness and zoom position. Check the focus before resuming shooting.
- With some EF lenses, the camera may take longer to focus automatically or may not be able to focus correctly. Visit your local Canon website for the latest information.
- When attached with a lens which does not support one-shot AF, focusing can only be performed manually. For information on lenses, please refer to "Setup Guide".
- The focus position may shift in an environment with large temperature changes. Set the focus again and check whether the focus is correct.

Camera Settings

Sets the camera settings.

[Camera Mode]
The camera offers five camera modes.

[Auto]
The camera controls the exposure by automatically adjusting the iris, gain and shutter speed.

[Tv] (shutter priority AE)
Set [Shutter Speed] to match low light conditions or fast moving subjects. The camera will then automatically set the appropriate aperture and gain to obtain the best exposure.

[Av] (aperture priority AE)
Set [Iris] (aperture) to control the depth of field. The camera will then automatically set the appropriate gain and shutter speed to obtain the best exposure.

[AGC] (automatic gain control)
You can set [Shutter Speed] and [Iris] (aperture). The camera will then automatically adjust the gain (the sensor's sensitivity) depending on the brightness of the subject.

[Manual]
You can adjust [Shutter Speed], [Iris] (aperture), and [Gain].

Note

When the camera mode is set to a mode other than [Manual] and the brightness changes, exposure adjustment may not be smooth.

[Iris Increment]
When the camera mode is set to [Av], [AGC] or [Manual], you can determine the aperture value increment used in adjusting the aperture from [1/2 stop], [1/3 stop], and [Fine]. If you select [Fine], the actual increments will be smaller than 1/3 stop.

[Iris]
When the camera mode is set to [Av], [AGC] or [Manual], you can adjust the aperture value.

Moving the slider to the right narrows the iris, making the video darker. Moving the slider to the left opens the iris, making the video brighter. Available aperture values will vary depending on the lens attached.
When using an EF Cinema lens supporting to adjust the iris from the camera, the iris setting of the lens needs to be set to Auto. Required settings vary depending on the lens. For details, please refer to the instruction manual of the lens used.

Lens	Part used on the lens	Setting for automatic adjustment
CN7x17 KAS S/E1 CN20x50 IAS H/E1	Iris operation change-over switch	A
CN-E18-80mm T4.4 L IS KAS S CN-E70-200mm T4.4 L IS KAS S	Iris auto/manual change-over switch	A

Important

- When using a compatible EF Cinema lens
  - When you change the aperture value from a position of fully open or fully closed iris, multiple adjustment operations may be required to change the iris.
  - When using the extender, enable the lens' iris correction function and adjust the F-number.
- The aperture values set and displayed on the Setting Page are approximate. Use them only as a reference.

[AE Shift]
You can compensate the exposure obtained during automatic exposure (camera modes other than [Manual]), in order to darken or lighten the image. You can select a level from -2 EV to +2 EV (in 0.25-EV increments).

[Shutter Speed]
If [Camera Mode] is set to [Tv], [AGC], or [Manual], you can fix the shutter speed.
Set the shutter speed based on shooting conditions. For example, you may want to set slower shutter speeds for darker environments.
Setting values available for 59.94 Hz/29.97P are as follows:
1/4, 1/5, 1/6, 1/7, 1/8, 1/10, 1/12, 1/15, 1/17, 1/20, 1/24, 1/30, 1/34, 1/40, 1/48, 1/60, 1/75, 1/90, 1/100, 1/120, 1/150, 1/180, 1/210, 1/250, 1/300, 1/360, 1/420, 1/500, 1/600, 1/720, 1/840, 1/1000, 1/1200, 1/1400, 1/1700, 1/2000

Important

- When shooting under artificial light sources such as fluorescent, mercury or halogen lamps, the image may flicker depending on the shutter speed. In such case, set [Flicker Reduction] to [Enable] to have the camera automatically detect and correct* flicker (P. 88).
  * Depending on the shooting conditions, the camera may not be able to reduce the flicker.
- Alternatively, you may be able to avoid flicker by setting the shutter speed to a value matching the frequency of the local electrical system: 1/100 for 50 Hz systems, 1/60 or 1/120 for 60 Hz systems.

[Auto Slow Shutter]
Determines the shutter speed used when the camera mode is set to [Auto] or [Av]. When this setting is set to [Off], the camera will not use shutter speeds slower than the frame rate currently used.
This will reduce blur on moving subjects in dark scenes.

[Gain]
When the camera mode is set to [Manual], you can manually adjust the gain to change the brightness of the image.
You can select a value in the range from 0 to +75 dB (in 3-dB increments).

Important

- When high gain levels are set, the picture may flicker slightly.
- When high gain levels are set, bright red, green or blue dots may appear on the screen. In such case, use a faster shutter speed or select a lower gain value.

[AGC Limit]
In camera modes other than [Manual], the camera will automatically adjust the gain. In such case, you can set an automatic gain control (AGC) limit to prevent the camera from using gain values above the preset limit.
You can select [Off (75dB)] for no limit (maximum gain as given in the parenthesis); or a maximum gain level from 36 dB to 75 dB, in 3-dB increments.

[AF Frame Position]
There are two options to choose from for the one-shot AF to focus on the area.

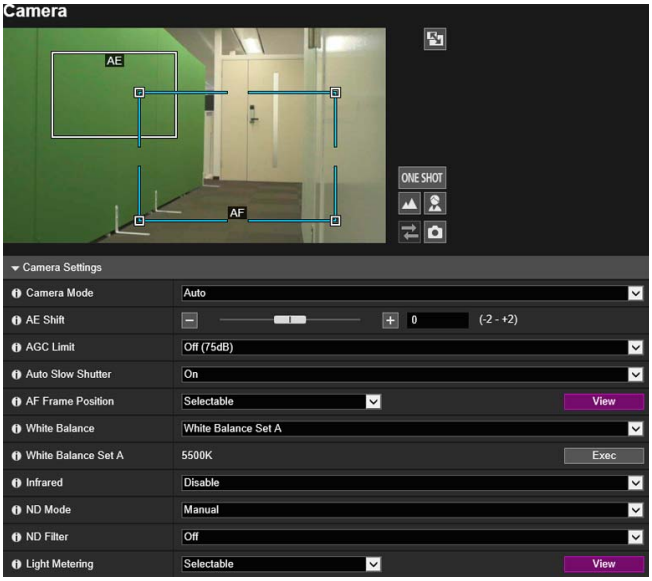
[Center]
Set the area in the center.

[Selectable]
Able to set the position and size of the AF frame to any area in the video display area.
Operate following the steps below:

1.When selecting [Selectable] from the [AF Frame Position], the AF frame will be displayed in the video display area.
2.Set the AF frame to any area.
- Move the frame by dragging within the lines.
- Adjust the size of the frame by dragging any of the four squares.

3.After setting the area, click the [One-shot AF] on the side of the video display area.

If the AF frame is not displayed, click [View].



Note

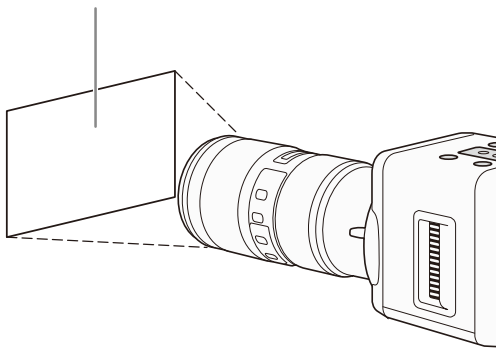
- AF frame and AE frame can be displayed simultaneously (for details on the AE frame, please refer to [Camera] > [Camera Settings] > [Light Metering] (P. 87)).
- Frame selected will be displayed in light blue.
- In order to select a frame, click on the frame, where it is not overlapping another frame or on the mark (for AF frame AF, for AE frame AE).

[White Balance]
The camera uses an electronic white balance process to calibrate the picture and produce accurate colors under different lighting conditions. There are six methods of setting the white balance.

[Auto]
The camera constantly adjusts the white balance automatically to achieve an optimal level. The camera will adjust the white balance if the light source changes.

[White Balance Set A], [White Balance Set B]
Obtain a reference white using the same lighting conditions you plan to use when shooting.
Place a white object (e.g. white paper) under the light source, point the camera at the white object so that it fills the whole screen, and click [Exec].
You can save two custom white balance settings, [White Balance Set A] and [White Balance Set B].

A gray card or white object



[Daylight] (approx. 5500 K)
Select this when capturing under the sunlight. It can be further fine-tuned within a range of -9 to +9 in [White Balance Fine Adjustment].

[Tungsten] (approx. 3000 K)
Select this when capturing under a light bulb (indoor). It can be further fine-tuned within a range of -9 to +9 in [White Balance Fine Adjustment].

[Color Temperature]
In the color temperature setting, you can select a color temperature between +2000 K and +15000 K in 100 K increments.

Important

- The white balance settings in the custom picture file ([R Gain], [B Gain]) take precedence over the white balance set with these procedures.
- If [Infrared] is set to [Enable], [White Balance] cannot be set.
- The color temperatures set and displayed on the Setting Page are approximate. Use them only as a reference.
- Custom white balance may provide better results in the following cases:
  - Changing lighting conditions
  - Close-ups
  - Subjects in a single color (sky, sea or forest)
  - Under mercury lamps and certain types of fluorescent and LED lights
- Readjust the custom white balance if the light source or ND filter setting changes.

[Infrared]
You can select [Infrared] to be enabled/disabled. Using the infrared mode, the camera becomes more sensitive to infrared light, allowing you to shoot in dark locations.

Important

Depending on the light source, autofocus may not work well during infrared mode.

[ND Mode]
Select [Auto] or [Manual] for how the ND filter is adjusted.
Using the ND filter allows you to open up the aperture to obtain a shallower depth of field even when shooting in bright surroundings.

Important

- If [Camera Mode] is set to [Manual], [ND Mode] is fixed to [Manual] and will not be displayed.
- If [Infrared] is set to [Enable], [ND Mode] cannot be set.

[Auto]
Automatically sets the ND filter.

[Manual]
You can select a setting value for [ND Filter].

[ND Filter]
If [ND Mode] is set to [Manual], you can select a setting value.
There are two options for the ND filter: [1/8] (3 stops) and [1/64] (6 stops).

Important

Depending on the scene, the color may change when turning the ND filter on/off. Setting a custom white balance may be effective in such case (P. 86).

[Light Metering]
Select the light metering mode from four options to match the shooting conditions. Using the appropriate setting will produce a suitable exposure level during automatic exposure (with [Infrared] set to [Disable]).

[Standard]
Averages the light metered from the entire screen, giving more weight to the subject in the center.

[Backlight]

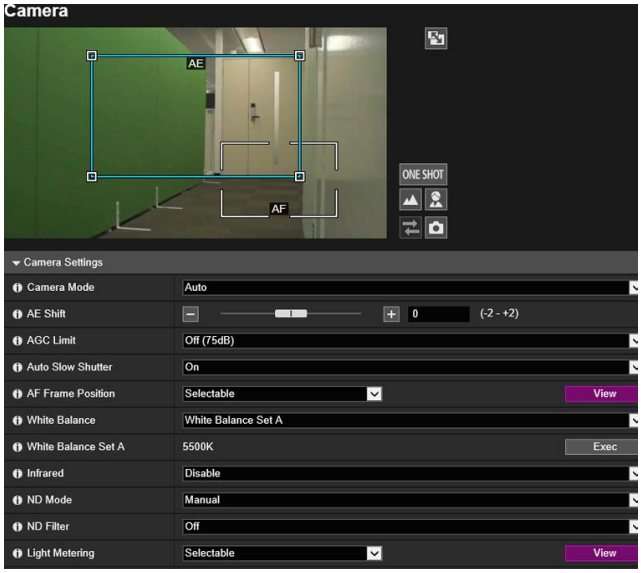
Suitable when shooting backlit scenes.

[Spotlight]
Use this option when shooting a scene in which only a certain part of the picture is lit, for example, when the subject is lit by a spotlight.

[Selectable]
Controls the specified area to be at optimal brightness.
Able to set the position and size of the AE frame to any area in the video display area.
Operate following the steps below:

1.When selecting [Selectable] from the [Light Metering], the AE frame will be displayed in the video display area.
2.Set the AE frame to any area.
- Move the frame by dragging within the lines.
- Adjust the size of the frame by dragging any of the four squares.

If the AE frame is not displayed, click [View].



Note
- AE frame and AF frame can be displayed simultaneously (for details on the AF frame, please refer to [Camera] > [Camera Settings] > [AF Frame Position] (P. 85)).
- Frame selected will be displayed in light blue.
- In order to select a frame, click on the frame, where it is not overlapping another frame or on the mark (for AF frame AF, for AE frame AE).

Important
When the camera mode is set to [Manual], changing the light metering mode will not affect the exposure. Adjust the exposure to a suitable level.

[Flicker Reduction]
Allows the camera to automatically detect and correct flicker caused by artificial light sources. When set to [Enable], it may be possible to automatically detect and compensate for the flicker.

[Custom Picture]
The camera lets you change several setting that control various aspects of the image produced. As a set, all these settings are treated as a single custom picture file. After adjusting the desired settings to your preference, you can save up to four custom picture files in the camera and load them later to apply exactly the same settings. Alternatively, you can use one of the preset custom picture files.
The following preset custom picture files are protected and cannot be edited.

Preset Name	Gamma	Feature
EOS Std.	EOS Std.	Reproduces the image quality and look (vivid, sharp and crisp) of an EOS digital SLR camera with its picture style set to [Standard].
Wide DR	Wide DR	Applies a gamma curve with a very wide dynamic range and an appropriate color matrix that nevertheless do not require post-production processing.
Canon Log	Canon Log	Uses the Canon Log gamma and color matrix for an outstanding dynamic range and an image suitable for processing in post-production.

Preset Name	Gamma	Feature
Crisp Img	Crisp Img	Under sufficient light conditions, video becomes clear with high sharpness applied. Under low-light conditions, the data size can be reduced by setting the noise reduction to a high level. Setting suitable for transmitting the video over the network.
Blue Scr	Normal 1	Displayed only when [Blue Scr] is specified for a custom picture file using the buttons on the back of the camera. A setting that optimizes the color correction for chroma key systems (blue screen) that use LED lights and retroreflective backdrops. It can also be used for chroma key shooting with common blue backdrops.
Green Scr	Normal 1	Displayed only when [Green Scr] is specified for a custom picture file using the buttons on the back of the camera. A setting that optimizes the color correction for chroma key systems (green screen) that use LED lights and retroreflective backdrops. It can also be used for chroma key shooting with common green backdrops.

Selecting [CP1] - [CP4], you can register the specified image quality settings as a custom picture file, so that the desired adjustment values can be loaded by simply selecting it from the list. For details, please refer to the following "Custom Picture".

Custom Picture

After adjusting the desired settings to your preference, you can save them as custom picture files in [Custom Picture] > [CP1] - [CP4] and load them later to apply exactly the same settings.

Functional classification	Function/Setting item	Ref.
Group related to light gradation	Gamma	P. 89
	Master Pedestal	P. 90
	Master Black Red	P. 90
	Master Black Blue	P. 90
	Black Gamma	P. 90
	Knee	P. 90
Group related to outline and noise	Sharpness	P. 91
	Noise Reduction	P. 91
Group related to direction, strength, and conversion of colors	White Balance	P. 91

[Base Custom Picture]
You can configure setting items based on presets provided in advance.
[Linear] is a setting suitable for data processing of luminance input/output characteristics in research applications. For information on [EOS Std.], [Wide DR], [Canon Log], and [Crisp Img], please refer to the table on P. 88. Selecting [Neutral] returns to the initial settings.
When the selection is blank, it will allow the user to set each item based on the current camera settings. Alternatively, you can select a blank space to start with current camera settings.

[Gamma]
Select the gamma curve.

[EOS Std.]
This gamma curve approximates the look of an EOS digital SLR camera when the picture style is set to [Standard]. Produces higher contrast than with the [Normal 1] setting.

[Wide DR]
Gamma curve with a very wide dynamic range compared to the [Normal 1] setting. Optimized for playback on TV monitors.

[Canon Log]
Logarithmic gamma curve that obtains an impressive dynamic range and makes the most of the image sensor characteristics. Requires image processing in post-production.

[Linear]

Does not apply a gamma curve. Creates a linear relationship between the luminance input and output. Used when processing the input and output data for research and other purposes.

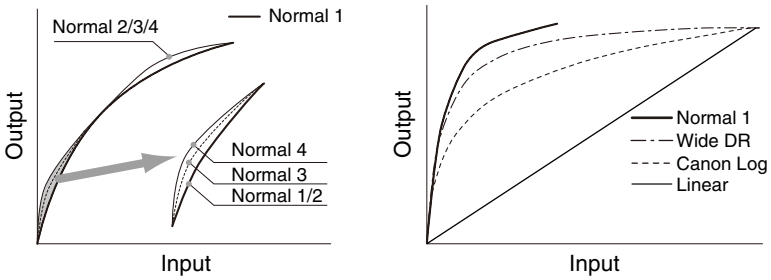
[Crisp Img]
Increases the contrast and saturation to achieve high visibility and color reproduction close to the appearance.

[Normal 1]
Standard picture for playback on TV monitors. The default setting is [Normal 1].

[Normal 2]
Setting suitable for playback on TV monitors. Produces brighter highlights (bright areas of the image) than with the [Normal 1] setting.

[Normal 3]
Setting suitable for playback on TV monitors. Produces a more faithful black gradation in the shadows (dark areas of the image) than with the [Normal 2] setting.

[Normal 4]
Setting suitable for playback on TV monitors. Produces even better black gradation in the shadows (dark areas of the image) than with the [Normal 3] setting.

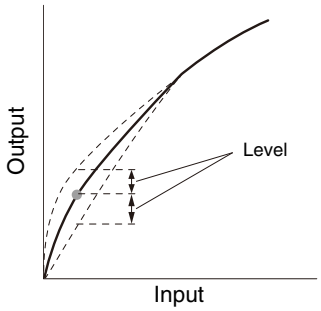


[Master Pedestal]
Increases or decreases the black level. Moving the slider to the left makes black areas darker, and moving it to the right makes black areas brighter.
This setting can be adjusted from -50 to +50. (Default: ±0)

[Master Black Red]
Corrects the R value for the black color cast.
This setting can be adjusted from -50 to +50. (Default: ±0)

[Master Black Blue]
Corrects the B value for the black color cast.
This setting can be adjusted from -50 to +50. (Default: ±0)

[Black Gamma]
Raises or lowers the lower part of the gamma curve (dark areas of the image). Changing the value adjusts the gamma curve on the black side within the range of the figure.
This setting can be adjusted from -50 to +50. (Default: ±0)



Note

When [Gamma] is set to [Wide DR], [Canon Log], or [Linear], [Black Gamma] is not available.

[Knee]
By compressing the highlights, you can prevent parts of the image from being overexposed.

Note

The [Knee] setting is available only when [Gamma] is set to [Normal 1] - [Normal 4].

[Knee Slope]

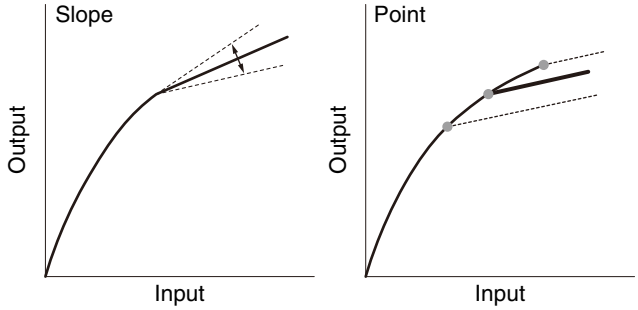
Determines the slope of the gamma curve above the knee point.

This setting can be adjusted from -35 to +50. (Default: ±0)

[Knee Point]

Sets the knee point of the gamma curve.

This setting can be adjusted from 50 to 109. (Default: 95)



[Sharpness]

Select a sharpness level.

The video becomes sharper with a higher level selected, and becomes softer with a lower level selected.

The video file size becomes larger as the level becomes higher.

This setting can be adjusted from -10 to +50. (Default: ±0)

[Noise Reduction]

Select a noise filter that reduces the amount of noise that appears in the image. The larger the value, the stronger the noise reduction effect is. This setting is generally more effective in low-light conditions.

When a higher level is selected, the noise reduction effect is increased, but residual images are more likely to appear.

When a lower level is selected, the noise reduction effect is decreased and resolution is increased, but the video file size becomes larger.

Select a level from 1 (lowest level) to 12 (highest level), or select [Off] to turn the noise reduction off. (Default: [Off])

[R Gain]

Adjust the intensity of red tones in white balance.

This setting can be adjusted from -50 to +50. (Default: ±0)

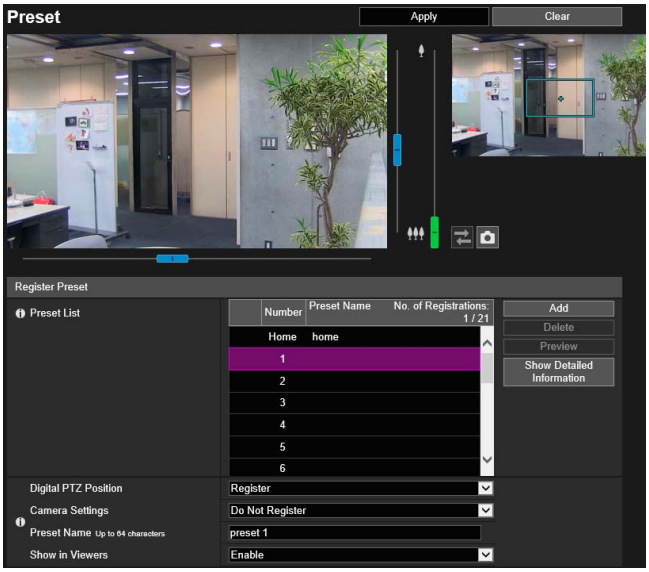
[B Gain]

Adjust the intensity of blue tones in white balance.

This setting can be adjusted from -50 to +50. (Default: ±0)

[Camera] > [Preset]
Registering Presets

By registering settings as presets, such as camera angles and camera settings (e.g. exposure), the presets can be easily called up by Viewers to apply the settings.



The following settings can be configured here.
- Register Preset

Important
- Reconfigure the presets if you change the [Basic] > [System] > [Installation Conditions] > [Scan Reverse] (P. 81) settings.
- Reconfigure the presets if you change the zoom position.

Using Presets

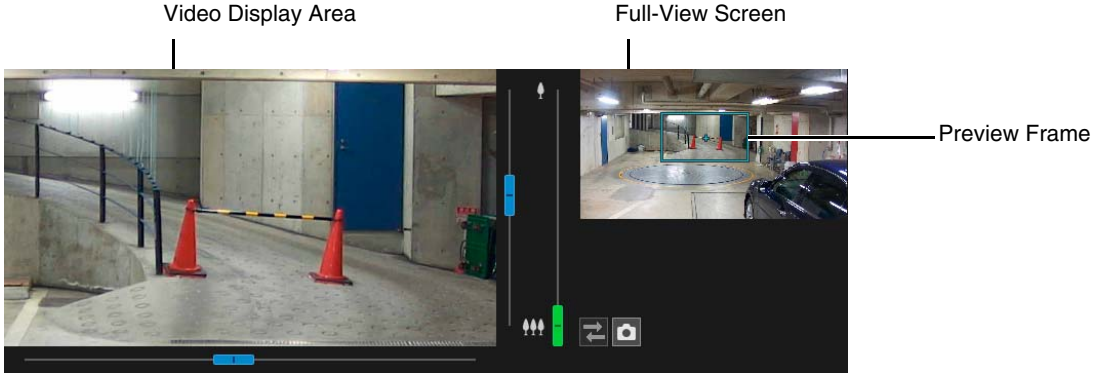
In addition to immediate execution of registered camera angles and the camera settings such as exposure when operating the viewer, you can execute the presets during switches between the normal capture and infrared modes (P. 143) or at the start time of the timer event (P. 118).

Registering a Preset

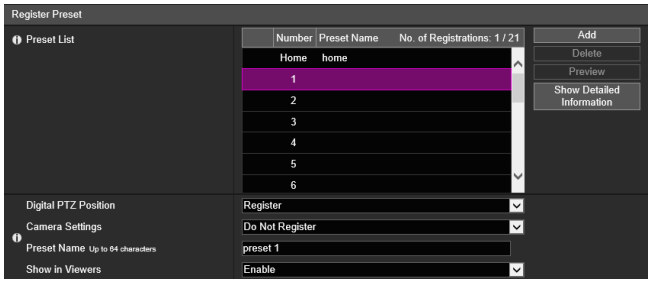
The camera angle and camera settings can be registered as a preset.
The number of presets you can register are 21 at maximum (including the home position).

1 **Operate the video display area and full-view screen to set the angle you want to register as the preset.**

The preview frame (blue) indicates the position currently cropped into the video display area.



2 Set the items of preset registration.



[Digital PTZ Position]
Select [Register] to register the current camera angle as a preset.

Note

If you selected [Home] (home position) in the preset list, [Digital PTZ Position] is always registered.

[Camera Settings]
Select [Register] to register the current settings in [Camera] > [Camera Settings] as a preset.

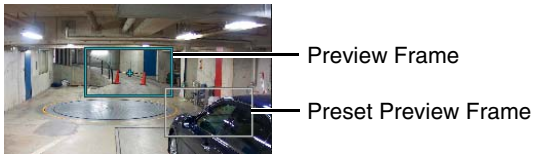
[Preset Name]
Enter a preset name. Be sure to enter a preset name in [Preset Name].

[Show in Viewers]
Select [Enable] to allow the Camera Viewers to use the preset.

3 Click [Add].

4 To register multiple presets, repeat steps 1 – 3.

When you select the added preset, the registered position is displayed as a preset preview frame (white frame) in the full-view screen.



If you click [Preview], the preset currently selected is also displayed in the video display area.

5 Click [Apply].

The preset is saved in the camera.

Note

Click [Clear] to discard the settings and restore the settings saved in the camera. However, note that presets only registered to the preset list by clicking [Add] are all discarded.

Deleting a Preset

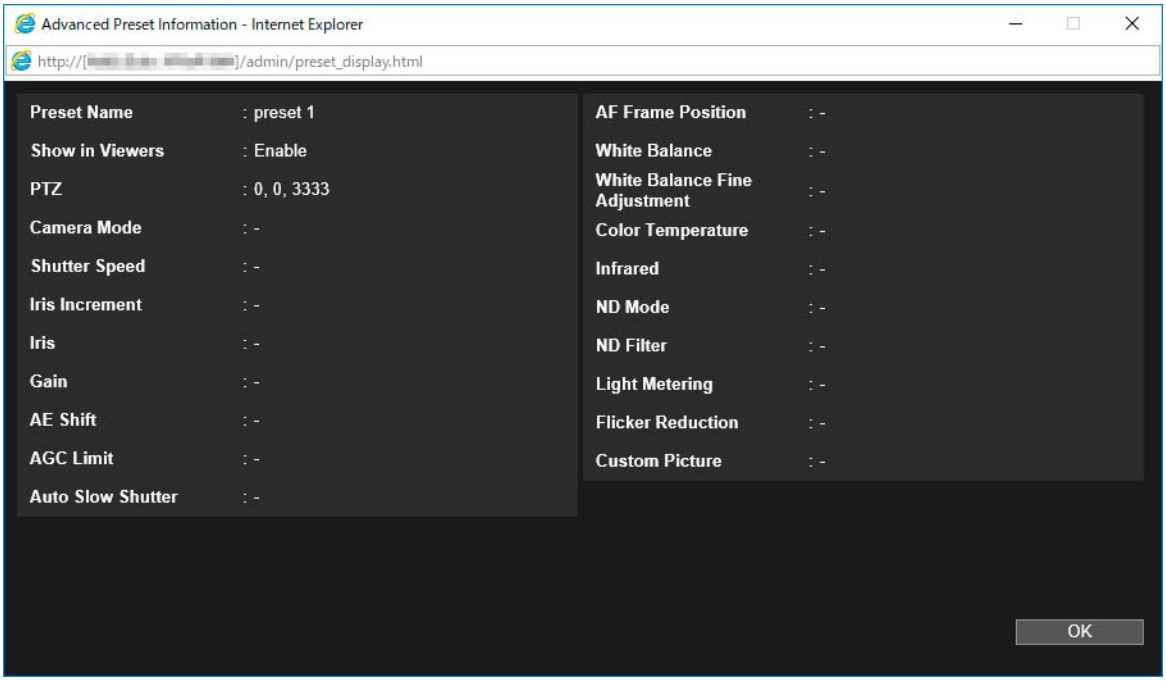
Select the preset to delete in the preset list, and click [Delete]. Click [Apply] to delete the preset from the camera. [Home] (home position) cannot be deleted.

Previewing a Preset

Select a preset in the preset list, and click [Preview]. The preset settings are shown in the video display area.

Checking Advanced Preset Information

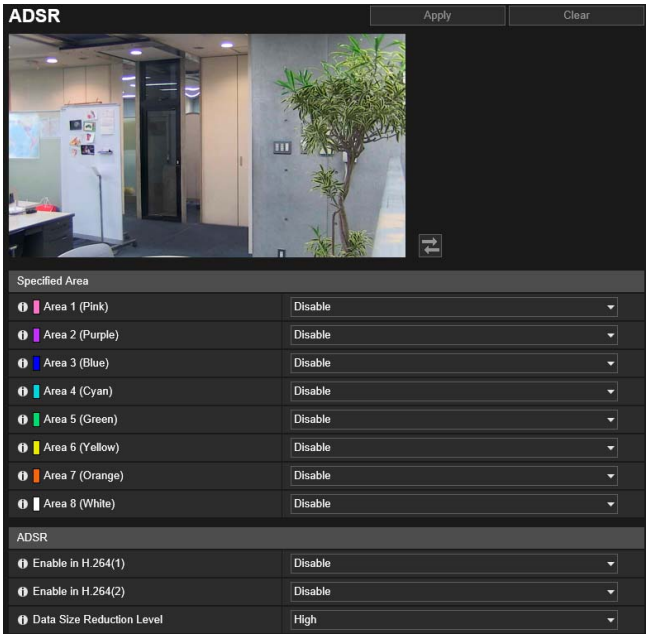
Displays the information of the presets registered in the camera.
Select the preset to check the advanced information from the preset list, and click [Show Detailed Information].



Check the detailed information, and click [OK].

[Video and Audio] > [ADSR] Reducing Data Size by Lowering Video Quality in Specific Areas

Reduces the size of transmitted H.264 video by reducing the video quality of non-target areas, such as ceilings and the sky. ADSR is an abbreviation for Area-specific Data Size Reduction.



The following settings can be configured here.
- Specified Area
- ADSR

Important

Some image scenes and settings for selected areas may not be able to reduce data size using ADSR. Please test the ADSR feature in the environment before use.

Note

- The image quality of the specified area depends on the [Bit Rate Control] setting in [Video] > [H.264(1)] or [H.264(2)].
  - When [Use bit rate control (constant bit rate)] is set: The image quality is adjusted according to the situation to match the target bit rate.
  - When [Do not use bit rate control (variable bit rate)] is set: The setting in [Video] > [H.264(1)] or [H.264(2)] is retained.
- The image quality for areas outside the specified area will be reduced according to [Data Size Reduction Level].

Specified Area

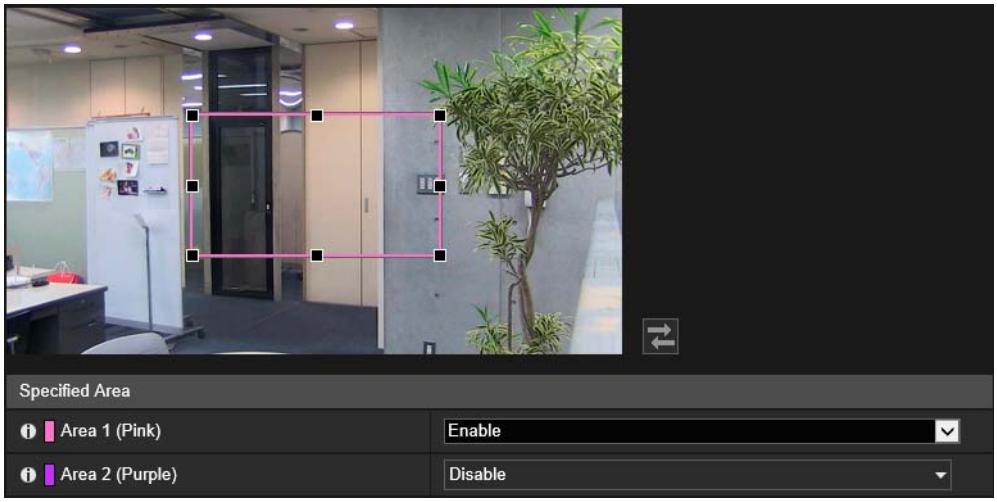
Specify the area where video quality is not to be lowered.
You can specify up to eight areas with different colored frames.

Important

- If you change the [Scan Reverse] setting in [Basic] > [System] > [Installation Conditions], review the specified area settings.
- If you change the zoom position, review the specified area settings.

1 Select [Enable] for the area with the frame color to use for the specified area.

The frame for the specified area is displayed on the video display area.



2 Set the specified area.

Set the specified area as follows within the display area.

- Drag out a frame and move it to the area you want to specify.
- Change the size of the frame by dragging any of the eight handles (■).

3 Click [Apply].

The settings are saved to the camera.

Note

You can use the Camera Viewer to check video with ADSR settings applied. Video outside the specified area will deteriorate according to the amount of applied data reduction.

ADSR

Set the data size reduction of outside areas set with [Specified Area].

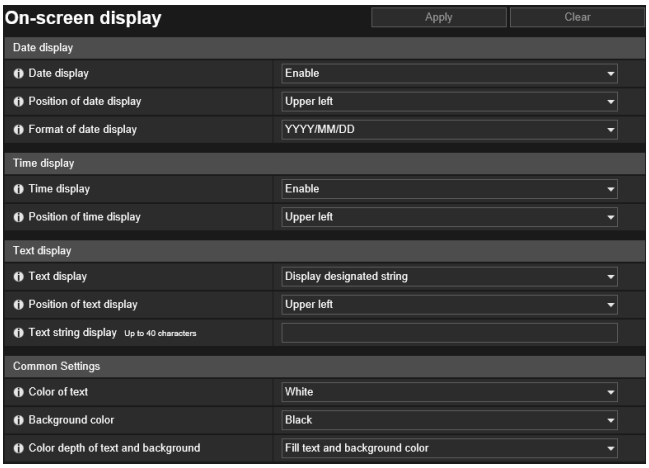
[Enable in H.264(1)]
Select [Enable] to lower video quality of outside areas set with [Specified Area] in H.264(1) video.

[Enable in H.264(2)]
Select [Enable] to lower video quality of outside areas set with [Specified Area] in H.264(2) video.

[Data Size Reduction Level]
Set the data size reduction level for the outside area of [Specified Area]. If you select [Low], the data size reduction effect is lower. If you select [High], the data size reduction effect is higher.

[Video and Audio] > [On-screen display]
Displaying Date, Time and Text on the Video

Displays the date and time, camera name and other text on the Video.



The following settings can be configured here.

- Date display
- Time display
- Text display
- Common Settings

Important

The on-screen time display is not suitable for usage where high reliability is required. Only use it as reference information on systems where utmost and constant reliability is required for surveillance.

Note

- Depending on video quality settings, the on-screen display may become difficult to decipher. Set it after confirming appearance on actual video.
- When using digital PTZ, on-screen display will not be shown if the cropped video has a horizontal size of 384 pixels or less.
- Setting the [Text display], [Date display], and [Time display] to the same position may result in not displaying all of the information. In such case, items set with [Upper right] or [Lower right] for [Position of text display] are prioritized for display.
- All of the texts may not be displayed depending on the video size, text length, and text position. Check the display after changing the video size and on-screen display settings.
- On-screen display settings are not displayed in the video output to the external monitor that is connected using the 3G/HD-SDI terminal or HDMI OUT terminal.

Date display

[Date display]
Select whether to display the date on the Video.

[Position of date display]
Select position for date display on the Video.

[Format of date display]
Select the year, month and day display order.

Time display

[Time display]
Select whether to display the time on the Video.

[Position of time display]
Select position for time display on the Video.

Text display

[Text display]
Select the text strings to display on the Video.

[Display designated string]
Displays the text string entered in [Text string display] below.

[Display camera name]
Displays the camera name entered in [Camera Name] (P. 80).

[Position of text display]
Select position for text display on the Video.

[Text string display]
If [Text display] is set to [Display designated string], enter the text string to be displayed in alphanumeric characters.

Common Settings

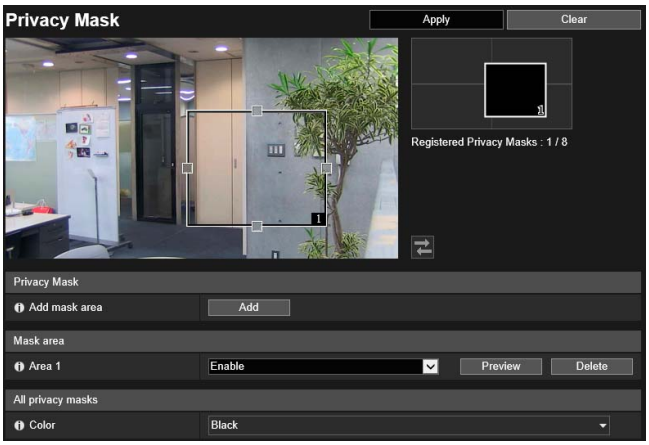
[Color of text]
Select from eight colors for the text color.

[Background color]
Select from eight colors for the background color.

[Color depth of text and background]
Select a color depth combination (Filling, Transparence, Translucence) for the text and background color.

[Video and Audio] > [Privacy Mask]
Setting Privacy Mask

Mask any areas of the camera video. You can check the camera video and set up to eight privacy masks.



The following settings can be configured here.

- Privacy Mask
- Mask area
- All privacy masks

Important

- Privacy masks are applied to all video transmitted from the camera (live video, uploaded video, recorded video and video recorded to a memory card).
- Privacy masks are not available in the following situation.
  - When the camera is launched immediately after being turned on
- Intelligent Function detection also works in the privacy mask areas. The [Intelligent Function] Setting Page displays the profile line of detected objects, etc., so you may be able to tell the movement of subjects even if a mask is applied.

Note

Privacy masks are not displayed in the video on the external monitor that is connected using the 3G/HD-SDI terminal or HDMI OUT terminal.

Registering Privacy Masks

Use the mouse to position and size the privacy mask areas, then save the settings to the camera.

1 In [Add mask area], click [Add].

The preview frame attached with the area number is shown on the video display area. The privacy mask area for the corresponding number is also displayed on the privacy mask registration area.

2 Set the size and position for the preview frame in the video display area.

Drag the preview frame shown in the video display area to the position you want to mask.
Change the size of the preview frame by dragging the handles (☐) positioned on its four sides.

3 Set [Mask area] to [Enable].

The settings for the privacy mask area is enabled.
Set [Mask area] to [Disable] to temporarily disable a privacy mask area without deleting it. The disabled privacy mask area of the registration area will be displayed with a crossed out frame.

4 Change the color for the privacy mask area with [Color] as necessary.

The color selected here is reflected to all the preview frames and privacy mask areas.

5 To add privacy mask areas, repeat steps 1 to 4.

You can save up to eight privacy masks.

6 Click [Apply].

The privacy mask area is saved to the camera.
Saved privacy mask areas are shown in the video display area and the privacy mask registration area.

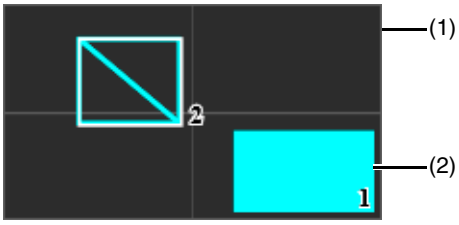
Important

- You will need to set the position of the privacy mask again if you change the [Scan Reverse] setting in [Basic] > [System] > [Installation Conditions].
- You will need to set the position of the privacy mask again if you change the zoom position.

Changing/Deleting a Privacy Mask

Privacy Mask Registration Area

This shows the positions of privacy mask areas in the entire area that can be captured by the camera.



(1) Entire Area That Camera Can Capture
This shows the area that can physically be captured.

(2) Privacy Mask Areas
Privacy mask areas with [Mask area] set to [Enable] (P. 100) are filled in.
Privacy mask areas with [Mask area] set to [Disable] (P. 100) have diagonal lines displayed in them.

Changing Mask Position and Size

How to Select a Privacy Mask

The following methods are available for selecting the privacy mask area.

- Click the privacy mask area you want to change in the privacy mask registration area.
- Click [Preview] in the mask area you want to display.
- Click the privacy mark area shown in the video display area.

1 Select the privacy mask area you want to change.

2 Change the position and size of the privacy mask area.

Move the preview frame by dragging it and change its size by dragging the handles (☐) positioned on its four sides.

Note

To discard changes and restore settings saved to the camera, click [Clear]. However, note that mask area settings that have not been saved in the camera by clicking [Apply] are all discarded.

3 Click [Apply].

The changed privacy mask area is saved to the camera.

Deleting a Privacy Mask from the Camera

Click [Delete] for [Mask area] in the privacy mask that you want to delete, then click [Apply].
The selected privacy mask area is deleted from the camera.

[Video and Audio] > [Audio]
Setting for the Power of Microphone

Set for the power of the microphone connected to the camera.

The following settings can be configured here.
- General Audio

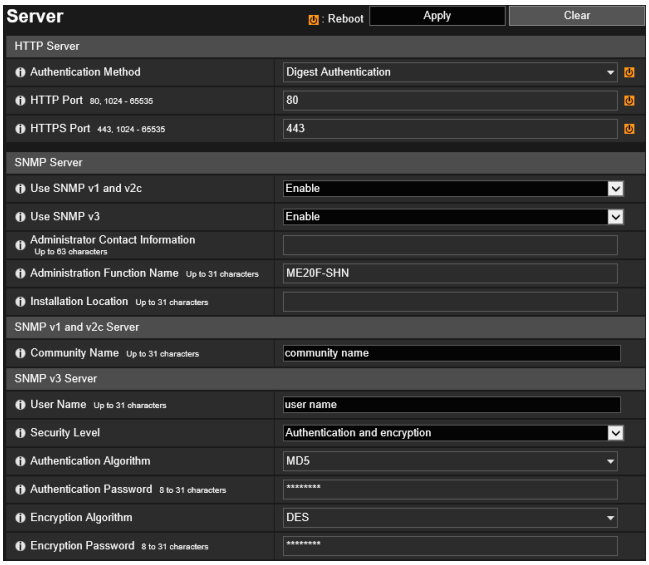
General Audio

[MIC Power]
Select [Enable] for a commercially available microphone that requires external power (a microphone with plug-in power functionality).

Caution
When using a microphone, change the [MIC Power] setting to suit the specifications of the microphone. Selecting [Enable (condenser microphone)] for a microphone without plug-in power functionality may damage the camera and/or microphone. Be sure to configure the setting correctly.

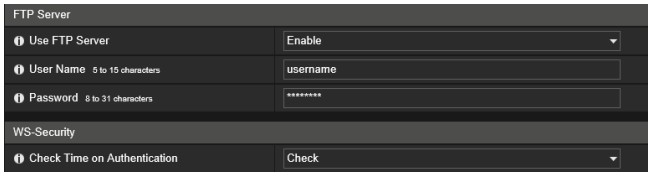
[Server] > [Server]
HTTP, SNMP and FTP Server Settings

Settings for HTTP server, SNMP server, FTP server usage or WS-Security time checks.



The following settings can be configured here.

- HTTP Server
- SNMP Server
- SNMP v1 and v2c Server
- SNMP v3 Server
- FTP Server
- WS-Security



HTTP Server

Set the authentication method and HTTP port number.

Important

If the setting of [HTTP Port] or [HTTPS Port] is changed and the camera may become inaccessible from the active web browser, a confirmation dialog box will be displayed. Click [OK] to apply the new setting.
If you reboot the camera and cannot connect to the camera from the web browser, any available URI for connecting to the camera will be displayed in a message.
If you cannot connect to the camera through the displayed URI, contact your system administrator.

[Authentication Method]
Select an authentication method for use by the HTTP server.

[HTTP Port]
Enter an HTTP port number.
Normally use [80] (factory default setting).

[HTTPS Port]
Enter an HTTPS port number.
Normally use [443] (factory default setting).

SNMP Server

Configure the necessary settings to use SNMP.

Note

- The camera information referenced from the SNMP manager is read-only.
- Use an SNMP Manager that supports SNMP MIB2 (supporting RFC1213).

[Use SNMP v1 and v2c]
If you select [Enable], you can use SNMP v1 and v2c to browse the camera information from an SNMP manager.

[Use SNMP v3]
If you select [Enable], you can use SNMP v3 to browse the camera information from an SNMP manager.

[Administrator Contact Information]
Enter contact information (e-mail address, etc.) for the administrator of the camera. Setting information can be referenced by the SNMP manager.

[Administration Function Name]
Enter the camera name used for administration. Setting information can be referenced by the SNMP manager.
If left blank, the camera model name will be used.

[Installation Location]
Enter information regarding the installation location of this camera. Setting information can be referenced by the SNMP manager.

SNMP v1 and v2c Server

[Community Name]
If you select [Enable] for [Use SNMP v1 and v2c], enter the community name to use for SNMPv1 and v2c. The factory default setting is blank.

SNMP v3 Server

[User Name]
If you selected [Enable] for [Use SNMP v3], set the user name to use with SNMP v3.

[Security Level]
Select the security level to use for SNMP v3.

[Authentication Algorithm]
If you selected [Authentication but no encryption] or [Authentication and encryption] for [Security Level], select the authentication algorithm.

[Authentication Password]
If you selected [Authentication but no encryption] or [Authentication and encryption] for [Security Level], set the authentication password.

[Encryption Algorithm]
If you selected [Authentication and encryption] for [Security Level], select the encryption algorithm.

[Encryption Password]
If you selected [Authentication and encryption] for [Security Level], set the encryption password.

FTP Server

[Use FTP Server]
The settings for using an FTP server.

[User Name]
Set the name of the user to allow FTP connections for.

[Password]
Set the password of the user to allow FTP connections for.

Important

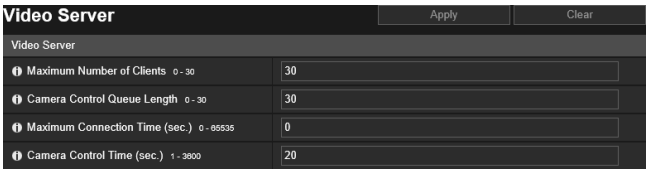
- Canon will assume no liability for any accident or damage resulting from use of FTP software.
- When changing the user name, make sure to also change the password.
- If you set the same user name as a user name used in the system, the message “User name is invalid.” is displayed. In this case, set another user name.

WS-Security

[Check Time on Authentication]
Select whether to check the time information of data transmitted by the client.

[Server] > [Video Server]
Video Transmission Settings

Settings for clients that can connect to a video server.



The following settings can be configured here.
- Video Server

Video Server

[Maximum Number of Clients]
Enter the maximum number of clients that can be connected to the camera at the same time.
If set to [0], only administrators will be able to connect.

Important
When there are many clients or they are connected to the camera over an SSL/TLS connection, the video frame rate may slow down and the sound may drop out if audio reception from the camera is enabled.

[Camera Control Queue Length]
Enter the maximum queue length for clients requesting camera control privileges from the Camera Viewer.
If set to [0], only administrators can queue for camera control.

[Maximum Connection Time (sec.)]
Enter the maximum time in seconds during which an individual client can connect to the camera.
If set to [0], the connection time is unlimited.

[Camera Control Time (sec.)]
Enter the maximum time Camera Viewer can retain camera control privileges.

[Server] > [Audio Server]
Audio Transmission Setting

Set the audio input from the microphone connected to the camera.

The following settings can be configured here.
- Audio Server

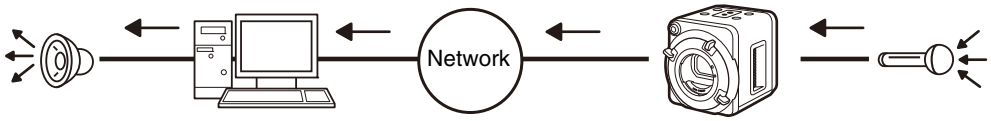
Important

- Video and audio can be distributed to up to 30 clients. However, when there are many clients or they are connected to the camera over an SSL/TLS connection, the video frame rate may slow down and the sound may drop out if audio reception from the camera is enabled.
- The video and audio may not be synchronized.
- The audio may be temporarily interrupted, depending on the performance of the computer and the network environment.
- The audio may be interrupted if anti-virus software is enabled.
- Communication may be temporarily interrupted, cutting off the audio, if the LAN cable is unplugged and plugged in again. If this occurs, reconnect from the Viewer.
- The volume, sound quality, etc., may change depending on the characteristics of the microphone used.

Audio Server

Set audio transmission from the microphone.

[Audio Transmission from the Camera]
Select [Enable] to transmit audio from the microphone connected to the camera to the Viewer.



[Voice Activity Detection]
Select whether to detect when there is no sound coming from the microphone.
When set to [Enable], audio data transmission will pause while there is no sound input from the camera. This can reduce the load on the network used.

[Server] > [RTP Server]
RTP Settings

Set the video and audio transmission using RTP.

The following settings can be configured here.
- RTP Server
- Audio Multicast
- RTP Stream 1 to 5

RTP Server

Enable RTP, and set the RTSP authentication method and port number.

[RTP]
Select this to enable or disable RTP.

[RTSP Authentication Method]
Select an authentication method for RTSP. Since the RTSP authentication method is configured independently of the HTTP authentication method, you need to configure each authentication method.

[RTSP Port]
Enter the RTSP port number.
Normally use [554] (factory default setting).

Audio Multicast

Set multicast for audio transmission.

[Multicast Address]
Enter the multicast address for audio transmission as follows.
IPv4: Range from 224.0.0.0 to 239.255.255.255.
IPv6: Address starting with ff00::/8
Set IPv4 to [0.0.0.0] and IPv6 to [::0 (::)] to disable multicast.

[Multicast Port]
Enter the multicast port number for audio transmission.
If set to [0], multicast is disabled.

[Multicast TTL]
Enter the effective range for multicast transmission.
If set to [0], multicast is disabled.
The TTL (Time To Live), representing the effective range for multicast transmission, is decremented each time the signal passes through a router. When the value reaches 0, the signal can no longer pass through the router and be transmitted. For example, if TTL is set to [1], multicast transmission is confined to the local segment only and cannot pass through the router to be transmitted.

RTP Stream 1 to 5

You can set each stream for RTP stream transmission in an RTP Stream 1 to RTP Stream 5 session.

[Video Size]
Select the video format (JPEG or H.264) and video size for the RTP stream.
The video sizes for H.264 will be determined according to the [H.264(1)] and [H.264(2)] settings in [Video] (P. 78).
In addition, [H.264(2)] cannot be set for multiple RTP streams.

[Frame Rate]
Enter the frame rate if the RTP stream is JPEG video.
This cannot be set for H.264 video. The [Frame Rate] setting in [Video] > [H.264(1)] or [H.264(2)] will be used.

[Multicast Address]
Enter the multicast address for RTP streaming as follows.
IPv4: Range from 224.0.0.0 to 239.255.255.255.
IPv6: Address starting with ff00::/8
Enter [0.0.0.0] for IPv4 and [::0(::)] for IPv6 to disable multicast.

[Multicast Port]
Enter the multicast port number for RTP streaming.
If set to [0], multicast is disabled.

[Multicast TTL]
Enter the effective range for multicast transmission of RTP streams.
If set to [0], multicast is disabled.
The TTL (Time To Live), representing the effective range for multicast transmission, is decremented each time the signal passes through a router. When the value reaches 0, the signal can no longer pass through the router and be transmitted. For example, if TTL is set to [1], multicast transmission is confined to the local segment only and cannot pass through the router to be transmitted.

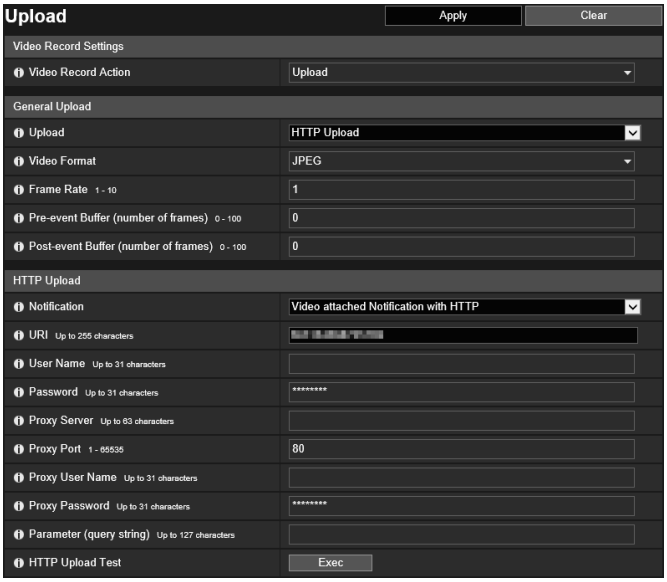
[Audio Transmission]
Select whether to use audio transmission for RTP streaming.

Note

- RTP Streaming URL
  rtsp://IP Address:Port Number/rtpstream/config1(to 5)=r|u|m
  [=r|u|m] is optional and can be omitted. If specified, specify only one option.
  r: Requests RTP over TCP
  u: Requests RTP over UDP
  m: Requests multicast
  Example: RTP Stream 1 request using RTP over TCP
  rtsp://192.168.100.1:554/rtpstream/config1=r
  Caution: Note that the actual operation is dependent on the RTP client application, so the URL does not necessarily specify the method used for transmission.
- When H.264 is selected, bit rate control and video quality are each set with [Video] (P. 78).
- The [Video Distribution] and [Audio Distribution] settings in [Basic] > [User Management] > [User Authority] are not used for RTP.
- RTP streaming video may not be viewable on systems using a proxy server or firewall. If this occurs, contact your system administrator.
- If Host Access Restrictions are applied to a client while it is streaming using RTP over UDP, it may take from a few to tens of seconds until streaming ceases.
- Regardless of the [Server] > [Audio Server] > [Audio Transmission from the Camera] setting, RTP streaming audio will be used.

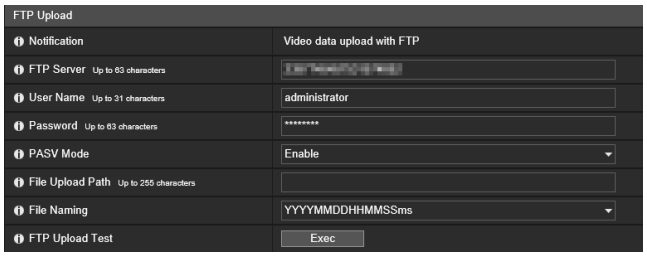
[Video Record] > [Upload]
HTTP and FTP Upload Settings

Settings for uploading video via HTTP or FTP when an event is triggered.
Use [Server] > [Server] (P. 103) to configure HTTP server and FTP server settings for uploading.



The following settings can be configured here.

- Video Record Settings
- General Upload
- HTTP Upload
- FTP Upload



Important

- When using the upload function or recording to a memory card, the following settings are required according to each event.
  - [Video Record] settings configured with [Event] > [Timer].
  - [Video Record] settings configured with each of the [Event] > [External Device].
  - The setting in the [Event] tab of the Intelligent Function (P. 141).
- When using the upload function, or recording to the memory card, do not change the settings in the [Settings Page]. Doing so may result in the upload function or the recording to memory card to stop.
- If you are using either HTTP or FTP upload together with e-mail notification by text and video, set [Video] > [JPEG] > [Video Size: Upload / Memory card] (P. 77) to a small size.
- HTTP upload does not support SSL/TLS.
- If the camera is set to upload or send e-mail notification continuously, not all video or e-mails may be sent depending on the video size and the network condition to the server. If this occurs, a message is written to the log (P. 162).

Video Record Settings

When an event is triggered, you can set whether to upload camera video with HTTP or FTP or to record the video to a memory card.
This item can also be set with the [Memory Card] submenu (P. 155) and will be reflected in [Video Record Settings] here.

[Video Record Action]
Select [Upload] to upload video.

General Upload

Set the upload method and video format for upload.

[Upload]
Select whether to upload with HTTP or FTP.

[Video Format]
Select the video format for upload.

Video size and quality of the uploaded video follow the settings in [Video] (P. 77).

Important

- For H.264(1) or H.264(2), the following settings must be configured in [Video] > [H.264(1)] (P. 78) or [H.264(2)] (P. 78).
  - [Bit Rate Control]: [Use bit rate control (constant bit rate)]
  - [Target Bit Rate (kbps)]: [3072] or less
  - [I Frame Interval (sec)]: [0.5], [1] or [1.5]
- You cannot select a different H.264 format from that in [Memory Card] > [Memory Card Operations] > [Video Format] (P. 156).

[Frame Rate]
Enter the maximum frame rate of video to be uploaded when [Video Format] is set to [JPEG].

[Pre-event Buffer (number of frames)] (JPEG)/[Pre-event Buffer (sec)] (H.264)
Enter the number of frames or seconds of video to be buffered before the event.
Enter the maximum number of frames for [JPEG] or the maximum number of seconds for [H.264(1)] or [H.264(2)] in [Video Format].

[Post-event Buffer (number of frames)] (JPEG)/[Post-event Buffer (sec)] (H.264)
Enter the number of frames or seconds of video to be buffered after the event.
Enter the maximum number of frames for [JPEG] or the maximum number of seconds for [H.264(1)] or [H.264(2)] in [Video Format].

Important

The maximum video buffer size capacity is approx. 56 MB. If a large video size is set, the Frame Rate, Pre-event Buffer and Post-event Buffer may not be achieved as specified.
If buffering cannot be achieved as specified, a message is written to the log (P. 162). Confirm that no messages are displayed in the log.

Note

If the server or network load increases due to the upload settings, the video frame rate may drop. If this occurs, reconfigure the following settings to reduce the size and frequency of uploaded data.

- Set a lower value for [Video Size: Upload / Memory card] for [JPEG] (P. 77).
- Reduce the number of frames or seconds in [Pre-event Buffer] or [Post-event Buffer].
- From the Intelligent Function [Event] tab, disable [ON Event Operation], [OFF Event Operation] or [Detected mode Operation] (P. 141).
- If [External Device Input Event] is enabled, disable [Active Event Operation], [Inactive Event Operation] or [Ongoing Active Event Operation] (P. 117).
- If [Timer Event] is enabled, increase the value in [Repeat Interval] (P. 118).

HTTP Upload

Settings for the HTTP upload function when [Upload] is set to [HTTP Upload].
The HTTP upload function sends notifications via HTTP or via HTTP with attached images, depending on the network camera event.
For information about the HTTP upload function and settings, contact your nearest Canon Customer Service Center.

[Notification]
Select whether to send event information notifications only or notifications with attached videos when using HTTP upload.

[URI]
Enter the HTTP server URI to which to upload.

[User Name], [Password]
Enter the user name and password required for authentication.
Digest authentication is not supported.

[Proxy Server]
If using a proxy server, enter the host name or IP address of the proxy server.

[Proxy Port]
If using a proxy server, enter the port number of the proxy server.

[Proxy User Name], [Proxy Password]
Enter to use a user name and password for the proxy server.

Digest authentication is not supported.

[Parameter (query string)]
Enter the request parameters.
Parameters can be specified using the “%” character (P. 166).

[HTTP Upload Test]
Clicking [Exec] initiates an upload test based on the settings currently entered.
Only a single JPEG image will be uploaded, but it is not necessary to click [Apply] at that time. After entering a password, first click [Exec], then click [Apply].

Important

Enter [Proxy Server], [Proxy Port], [Proxy User Name] and [Proxy Password] if connecting via a proxy server.

FTP Upload

Settings for the FTP upload function when [Upload] is set to [FTP Upload].

[Notification]
This is set to [Video data upload with FTP].

[FTP Server]
Enter the host name or IP address of FTP server.

[User Name], [Password]
Enter the user name and password required for authentication.

[PASV Mode]
Select whether to use PASV mode when connecting to an FTP server.

[File Upload Path]
Enter a remote path (directory name) for video files to be uploaded to.

[File Naming]
Select a file naming rule for the upload file.

[YYYYMMDDHHMMSSms]
Video is uploaded according to the file name format of “{year}{month}{day}{hour}{minute}{second}{ms}.jpg”.
(Example: 20160123112122000.jpg)

[YYYYMMDD Directory/HHMMSSms]
A subdirectory named “{year}{month}{day}” is created first, and then the video is uploaded using the file name “{hour}{minute}{second}{ms}.jpg”.
(Example: 20160123/112122000.jpg)

[Loop]
Video is loaded with a file name numbered in sequence from 0000 up to the value set in [Maximum Number of Loops].
(Example: 0000.jpg, 0001.jpg) The number will return to 0000 when the maximum number of loops is reached.
Since the way FTP servers manage the upload of files with existing file names differs as follows, be sure to check the FTP server specifications before configuring this setting.

- Overwrite the existing file name
- Automatically save the file with a different name
- Generate an error

[Maximum Number of Loops]
If [Loop] is set under [File Naming], enter the maximum number of loops.

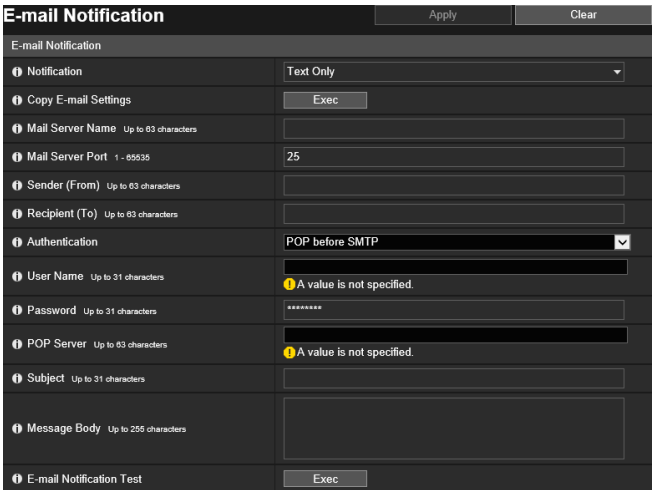
[User Settings]
Video is uploaded according to the file naming method specified in [Subdirectory Name to Create] and [File Name to Create].

[Subdirectory Name to Create], [File Name to Create]
If [File Naming] is set to [User Settings], enter the subdirectory name to be created as well as the name of the created file.
Parameters can be specified in the entry with the “%” character (P. 166).

[FTP Upload Test]
Clicking [Exec] initiates an upload test based on the settings currently entered.
Only a single JPEG will be uploaded, but it is not necessary to click [Apply] at that time. After entering a password, first click [Exec], then click [Apply].

[Video Record] > [E-mail Notification]
Setting E-mail Notification

Settings for sending an e-mail notification to a specified recipient when an event is triggered.



The following settings can be configured here.
- E-mail Notification

E-mail Notification

Set the mail server to be used for e-mail notifications and the content of the e-mail to be sent.

[Notification]
[Subject] and [Message Body] are text.
If you set [Text with Video], an image (JPEG format) captured immediately before the event will be attached.

[Copy E-mail Settings]
Copy the e-mail settings used in [Maintenance] > [Log] > [Log Notifications] (P. 162). However, the password is not copied.

[Mail Server Name]
Enter the host name or IP address of the SMTP server.

[Mail Server Port]
Enter the port number for the SMTP server.

[Sender (From)]
Enter the e-mail address of the sender.

[Recipient (To)]
Enter the e-mail address of the recipient.

[Authentication]
Select an authentication method suited to the destination SMTP server.

[User Name], [Password], [POP Server]
Enter the user name and password needed for authentication, and the POP server host name or IP address when e-mail authentication is set to [POP before SMTP].

[User Name], [Password]
Enter the user name and password needed for authentication when e-mail authentication is set to [SMTP-AUTH].

[Subject]
Enter the subject of the e-mail in alphanumeric characters.

[Message Body]
Enter the message body (text) of the e-mail in alphanumeric characters.
Parameters can be specified in the text using the “%” character (P. 166).

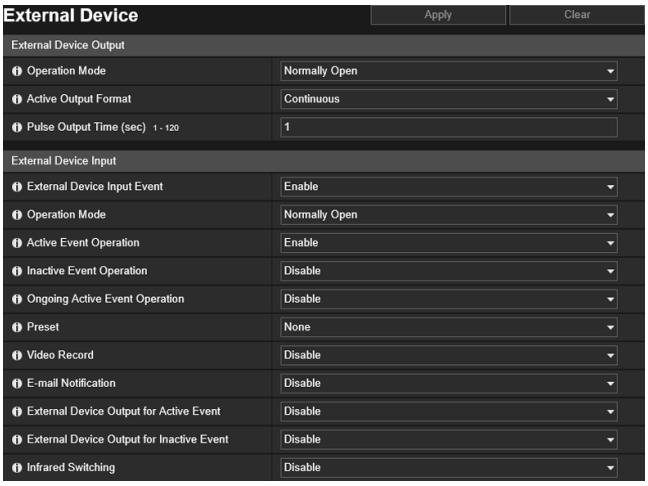
[E-mail Notification Test]

Clicking [Exec] initiates an e-mail notification test based on the settings currently entered.

It is not necessary to click [Apply]. After entering a password, first click [Exec], then click [Apply].

[Event] > [External Device]
External Device Input Triggered Operation Settings

Operation settings for external device output and for external device input triggered events.



The following settings can be configured here.
- External Device Output
- External Device Input

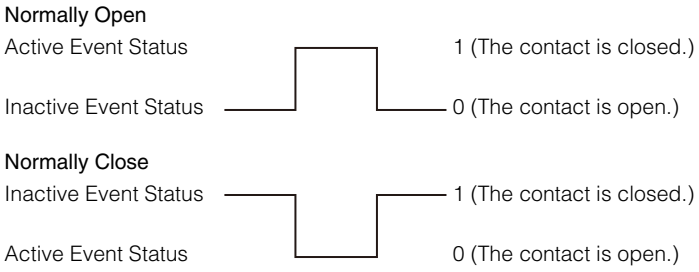
External Device Output

Set the operation for output to the external device.

Note

The output for an external device can be switched between active and inactive with [External Device Output] of the Camera Viewer (P. 58).

[Operation Mode]
Select whether the output terminals are normally open or closed.
If you set [Normally Open], an active event occurs when the output terminal connection closes, and an inactive event occurs when the output terminal connection opens.
If you set [Normally Close], an active event occurs when the output terminal connection opens, and an inactive event occurs when the output terminal connection closes.



[Active Output Format]
Select the output format when the external device output is active.

[Pulse Output Time (sec)]
Enter the output duration time (sec.) when [Active Output Format] is set to [Pulse].

Important

When [Active Output Format] is set to [Pulse] and a timer is used (P. 118), contact output is controlled only once when the timer starts.

External Device Input

You can set the operation to be performed when an event is triggered by input from an external device.

Note

An icon in the [Event and Input/Output] menu of the Camera Viewer will indicate when there is an external device input event (P. 58).

[External Device Input Event]
Select whether to use the input from an external device, such as a connected sensor, as an event.

[Operation Mode]
Select the circuit condition to suit the signal input from the connected external device.
When [Normally Open] is set, an active event occurs when the terminals of the external device close, and an inactive event occurs when the terminals open.
When [Normally Close] is set, an active event occurs when the terminals of the external device open, and an inactive event occurs when the terminals close.

[Active Event Operation]
Select the operation to be performed when an active event is triggered.
If [Enable] is set, [Preset], [Video Record] and [E-mail Notification] will be executed according to their settings when an active event is triggered.

[Inactive Event Operation]
Select the operation to be performed when an inactive event is triggered.
If [Enable] is set, [Preset], [Video Record] and [E-mail Notification] will be executed according to their settings when an inactive event is completed.

[Ongoing Active Event Operation]
Select the operation to be performed during an active event. This can only be set when [Active Event Operation] is set to [Enable].
If [Enable] is set, [Video Record] and [E-mail Notification] will be executed according to their settings during the active event.

[Preset]
If you specify a preset, the camera angle will automatically move to the preset location when an external device input event is triggered.
It is necessary to set presets beforehand with [Camera] > [Preset] (P. 92).

[Video Record]
Select whether to record video depending on the event.
If you select [Enable] and an external device input event is triggered, video will be transmitted to the recording destination specified in [Video Record] > [Upload] > [Video Record Action] (P. 110).

[E-mail Notification]
Select whether to send an e-mail notification depending on the event.
If [Enable] is selected, e-mail notification will be performed when an external device input event is triggered.
To use e-mail notification, you must set [Video Record] > [E-mail Notification] (P. 155) beforehand.

[External Device Output for Active Event]
Select the actions of external device output when an active event is triggered.

[External Device Output for Inactive Event]
Select the actions of external device output when an inactive event is triggered.

[Infrared Switching]
Select the infrared switching behavior when an external device input event is triggered.
When [Switch to Normal Capture] is set, switches to normal capture when an active event is triggered, and switches to the infrared mode when an inactive event is triggered.
When [Switch to Infrared] is set, switches to the infrared mode when an active event is triggered, and switches to normal capture when an inactive event is triggered.

Important

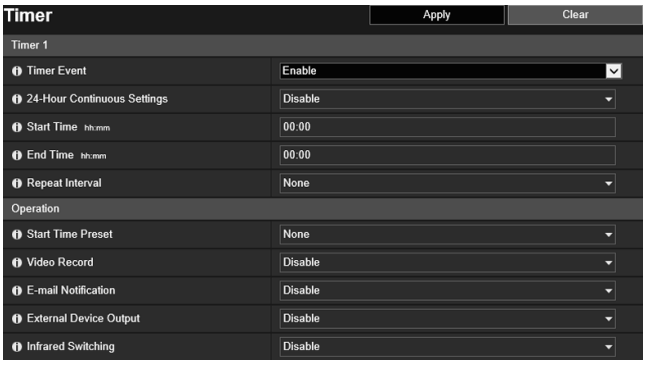
When the [Infrared Switching] setting switches the modes between normal capture and infrared, camera control privileges are released, even if the user has obtained those camera control privileges using the Camera Viewer or other camera control applications.

[Event] > [Timer]
Timer Triggered Operation Settings

The timer function can generate events that can trigger operations, such as video recording and e-mail notifications at regular intervals.
You can set the following two types of timers.

- 24 hours continuous from specified time
- Within specified time only

Either type can be set to trigger timer events at regular intervals.



The following settings can be configured here.

- Timer 1 to 4
- Operation

Timer 1 to 4

You can register up to four timer events.

[Timer Event]
Select whether to use a timer event.

[24-Hour Continuous Settings]
When set to [Enable], and [Repeat Interval] is set to an option other than [None], the timer event will be repeated at the interval specified in [Repeat Interval], irrespective of the [Start Time] setting. If [Repeat Interval] is set to [None], the timer event will be triggered only at the time set in [Start Time].
Note that when set to [Enable], only [Video Record] operations can be performed.

[Start Time]
Enter the start time of the timer event in 24-hour format. The timer event will be triggered at the start time.

[End Time]
When [24-Hour Continuous Settings] is set to [Disable], enter the end time of the timer event in the 24-hour format.

[Repeat Interval]
Select a repeat interval for timer events. The timer event will be triggered at the selected intervals.

Operation

Set the operations to be performed when timer events are triggered.

[Start Time Preset]
When [24-Hour Continuous Settings] is set to [Disable] and you specify a preset, the camera angle will automatically move to the preset location at the time set in [Start Time].
It is necessary to set presets beforehand with [Camera] > [Preset] (P. 92).

Important

When the camera is moved to a preset position specified in the [Start Time Preset] settings, camera control privileges are released, even if the user has obtained those camera control privileges using the Camera Viewer or other camera control applications.

[Video Record]
Select whether to record video depending on the timer event.
If you select [Enable] and a timer event is triggered, video will be transmitted to the recording destination specified in [Video Record] > [Upload] > [Video Record Action] (P. 110).

[E-mail Notification]
When [24-Hour Continuous Settings] is set to [Disable], select whether to send an e-mail notification depending on the timer event.
If [Enable] is selected, e-mail notification is performed when a timer event is triggered.
To use e-mail notification, you must set [Video Record] > [E-mail Notification] (P. 114) beforehand.

[External Device Output]
When [24-Hour Continuous Settings] is set to [Disable], select the actions of the external device output at [Start Time] and [End Time] of a timer.
[Repeat Interval] is not supported.

[Infrared Switching]
When [24-Hour Continuous Settings] is set to [Disable], select the infrared switching behavior when a timer event is triggered. This can only be set with [Timer 1].
Select [Switch to Normal Capture] to switch to normal capture at the start time, and to the infrared mode at the end time.
Select [Switch to Infrared] to switch to the infrared mode at the start time, and to normal capture at the end time.
[Repeat Interval] is not supported.

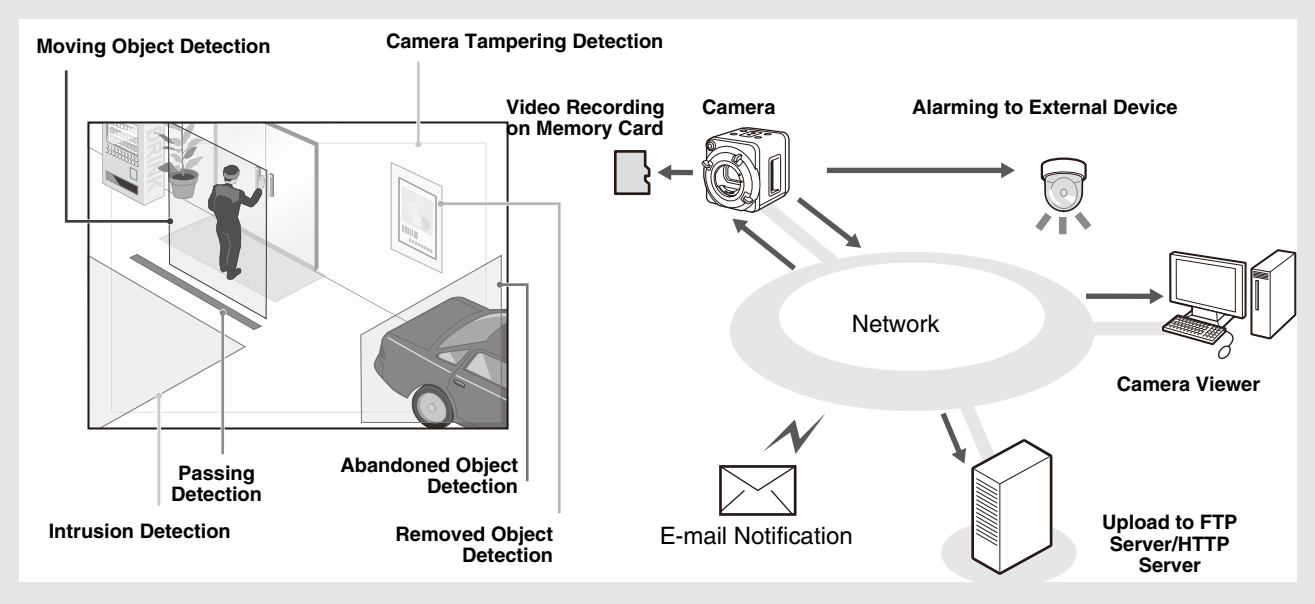
Important

- If you set [Start Time] and [End Time] and select a preset with [Start Time Preset], the infrared setting of [Infrared] (P. 87) registered in [Camera] > [Preset] is given priority. Therefore, even if you set [Infrared Switching] to [Switch to Normal Capture] or [Switch to Infrared], the [Infrared Switching] setting will be disabled if the opposite setting has been configured in [Preset] > [Camera Settings].
- When the [Infrared Switching] setting switches the modes between normal capture and infrared, camera control privileges are released, even if the user has obtained those camera control privileges using the Camera Viewer or other camera control applications.

[Event] > [Intelligent Function]
- Overview -

Intelligent Function

The Intelligent Function records video, outputs to an external device, and starts other operations when it detects changes in the video due to subject movement.



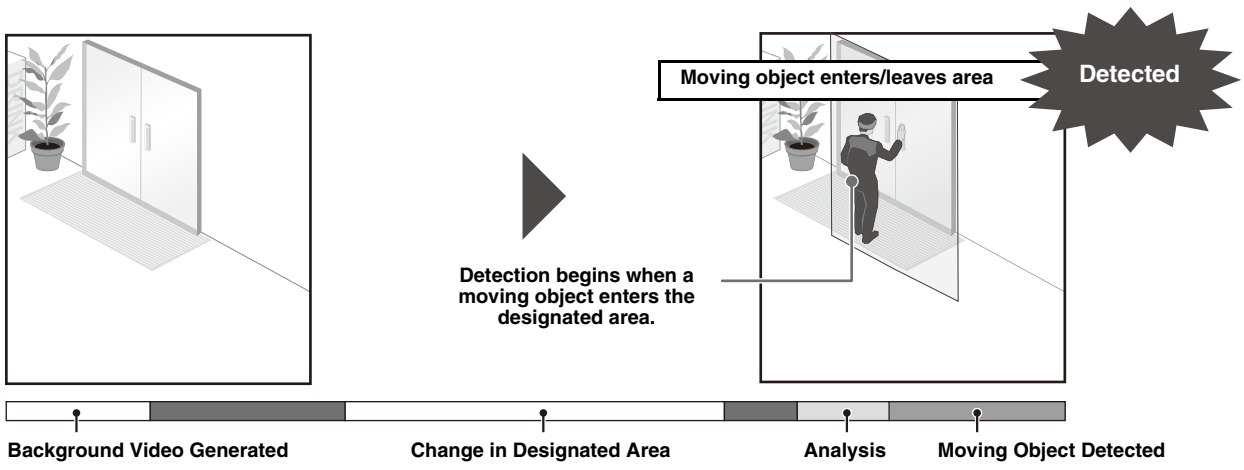
Notes on Use of This Camera
The Intelligent Function is not suitable for applications where high reliability is required. If constant and maximum reliability is required for surveillance it is not recommended that you use this function. Canon shall assume no liability for any accident, loss or other undesirable outcomes resulting from Intelligent Function operations.

■ Video Detection

Detects changes to video in a specified area. There are six types of detection to suit your needs.

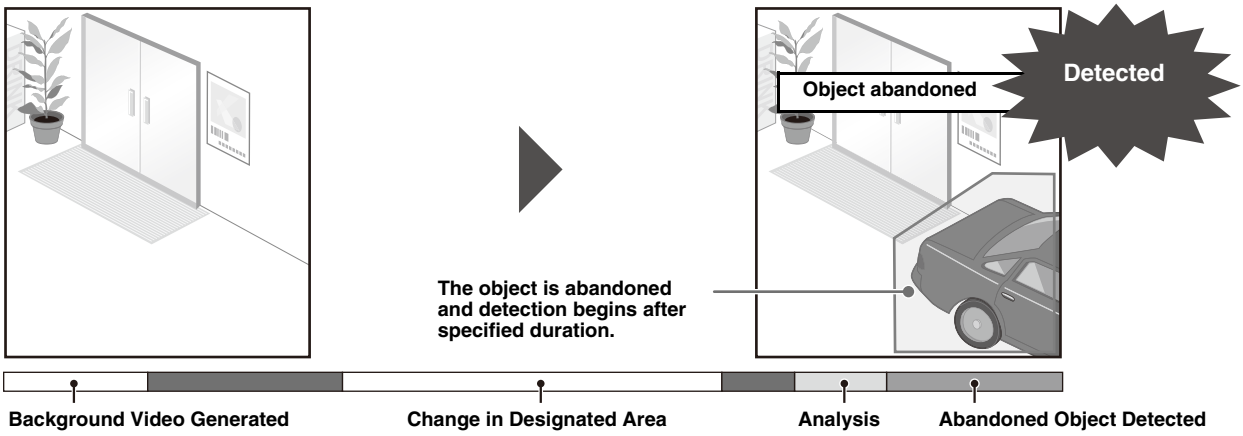
Moving Object Detection

Detects moving objects. This function can be used to detect visitors or suspicious individuals.
Moving object detection is triggered while moving objects are inside the detection area.



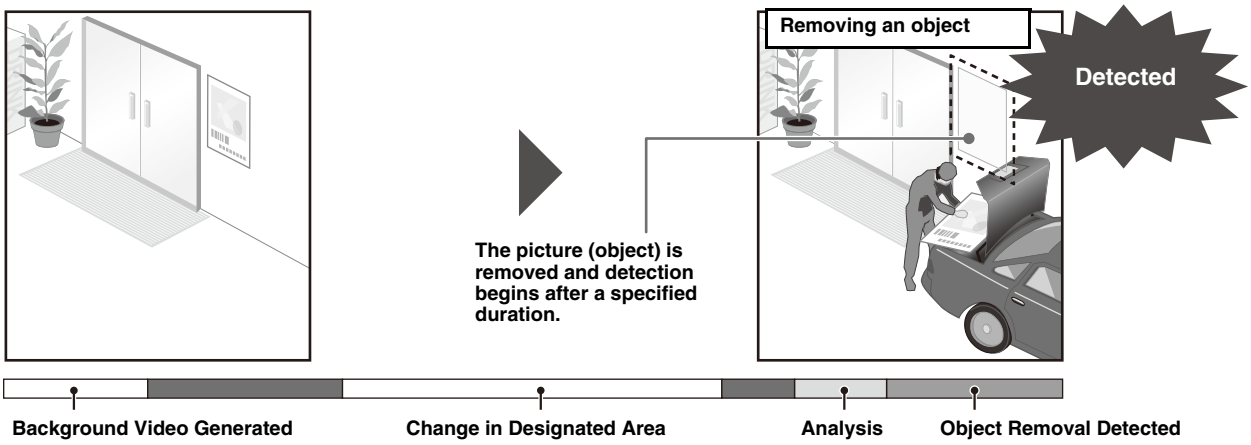
Abandoned Object Detection

Detect objects that are carried in and abandoned for a certain duration. This function can be used to detect suspicious objects that have been left behind. Abandoned object detection is triggered when an object is left in the detection area for a specified duration.



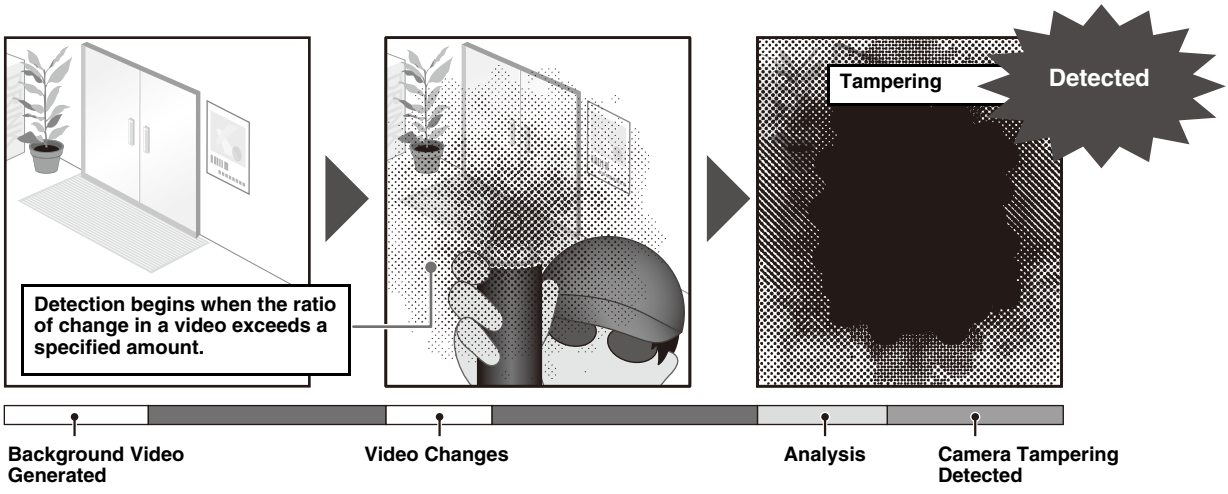
Removed Object Detection

Detect objects that have been removed. This can be used to detect actions such as the taking away of valuables. Removed object detection is triggered when an object is removed from the detection area for a specified duration.



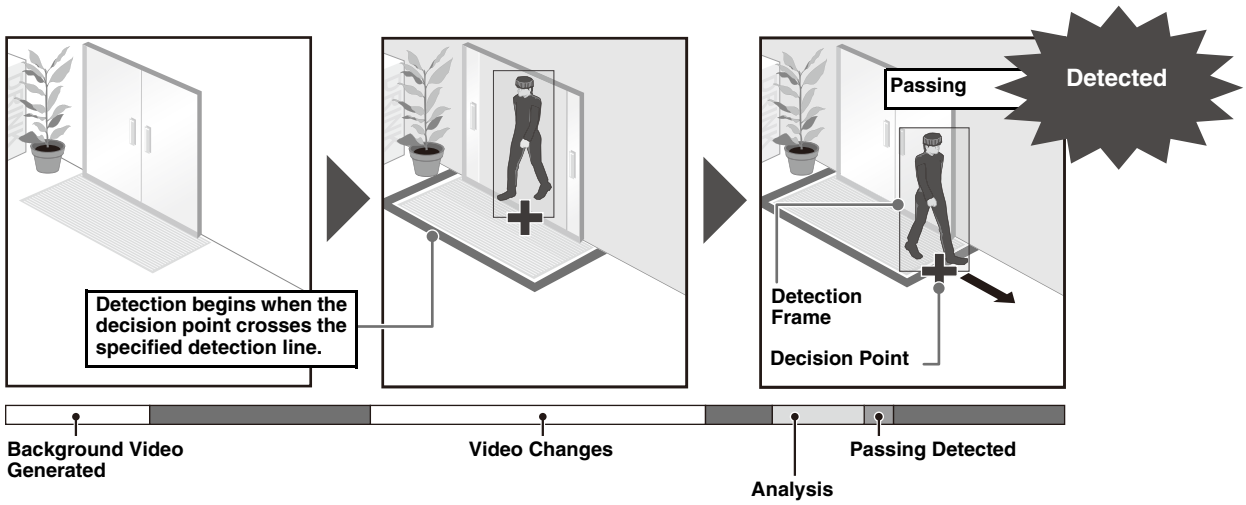
Camera Tampering Detection

Detect when capture is being disrupted. This can be used to detect when the camera orientation is changed or the video display is obscured with spray, etc. Camera tampering detection is triggered when an area exceeding a specified ratio of change is continuously altered.



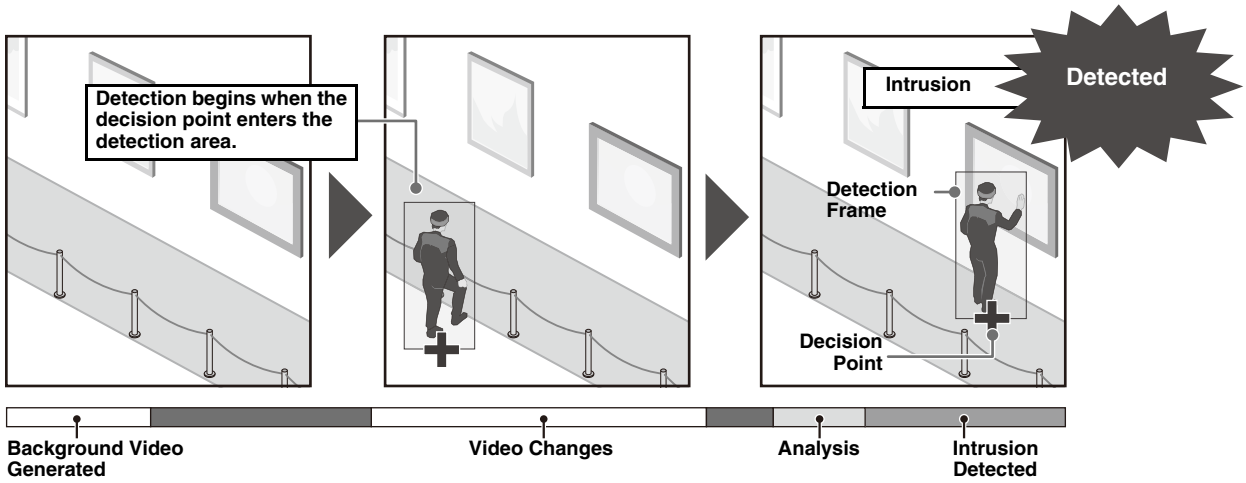
Passing Detection

Detect when a person or moving object crosses a specified line.
This determines that an object is passing when the decision point of the object detection frame crosses a detection line.



Intrusion Detection

Detect when a person or moving object crosses a specified area. This can be used to detect actions such as when someone climbs over a barrier and enters a restricted area in a museum, etc. This determines that an object is entering when the decision point of the object detection frame enters the detection area and the specified duration has elapsed.



Notes on Intelligent Function Settings and Operations

- When setting the Intelligent Function, do an actual detection test to confirm that detection will be performed correctly.
- If a sudden change in lightness or darkness occurs within the entire screen, proper detection may not be possible for up to five minutes.
- Detection will not be performed while the Intelligent Function is restarting.
- If the camera is operated while configuring or using the Intelligent Function, [Restarting intelligent function. Please wait.] is displayed and the Intelligent Function will restart.
- If the display switches the infrared setting, [Restarting intelligent function. Please wait.] is shown and intelligent function will restart.
- If [ND Mode] is set to [Auto] and the ND filter is inserted or removed due to changes in a lighting environment, [Restarting intelligent function. Please wait.] is displayed and the Intelligent Function will restart.
- If you change the zoom position, review the Intelligent Function settings.

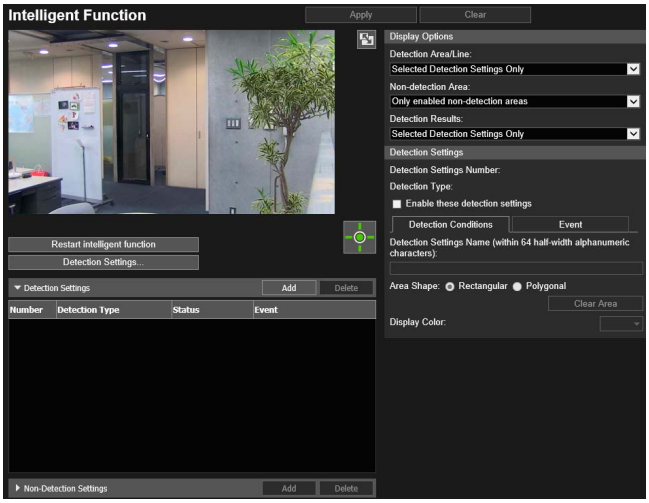
■ Difficult-to-Detect Subjects

The following subjects may not be detected, or may result in erroneous detection.

- Objects or areas where there is little contrast in color or brightness with the background may not be detected.
- Small objects and changes on the screen may not be detected.
- Partial or entire changes in brightness on the screen may trigger detection.
- When there are multiple overlapping objects, there may be a change in detection. For example, objects passing may either not be detected or the timing of detection may be incorrect.
- When there are large numbers of objects in the scene, objects may not be properly detected.

[Event] > [Intelligent Function]
- Video Detection -

In video detection, select the type to detect, and set the detection area for video changes while checking images on the camera. You should also set which operations (record video, outputting to an external device) should be carried out when changes are detected.



The following settings can be configured here.

- Detection Settings (List)
- Non-detection Area Settings (List)
- Display Options
- Detection Settings (Details)
- Non-detection Settings (Details)

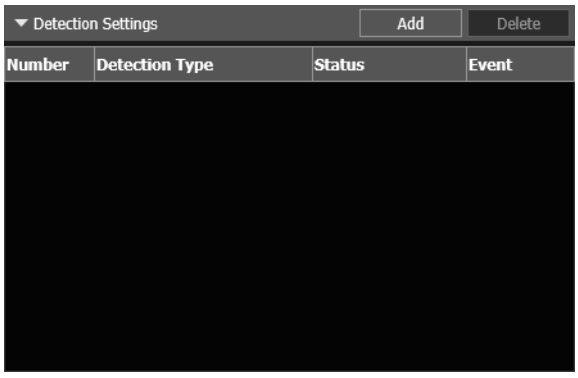
Steps for Configuring Video Detection

Set an area where changes in video are detected and an area where changes in video are not detected (non-detection area) as necessary.

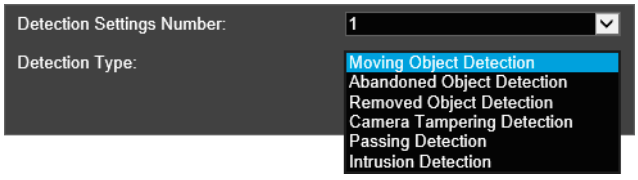
■ Configuring the Detection Area

The following are the basic steps for configuring a detection area. For details on settings for each type of detection, please refer to “Configuring Detection Criteria ([Detection Conditions] Tab)” (P. 128).

1 Click [Add] in [Detection Settings].



2 Select [Detection Settings Number] (1 to 15) and [Detection Type] for the detection setting to be added.

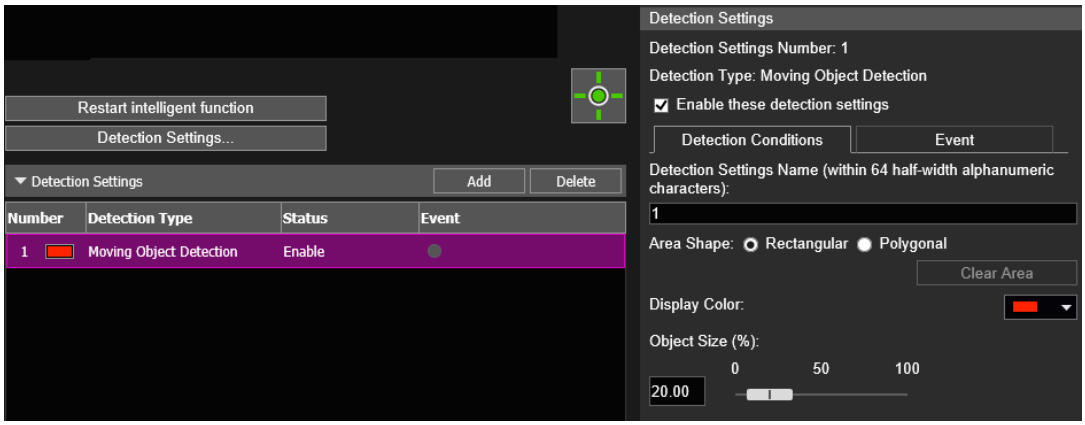


Note

You can register up to 15 detection settings.

3 Click [OK].

The detection settings added to [Detection Settings] are displayed and [Enable these detection settings] is selected.

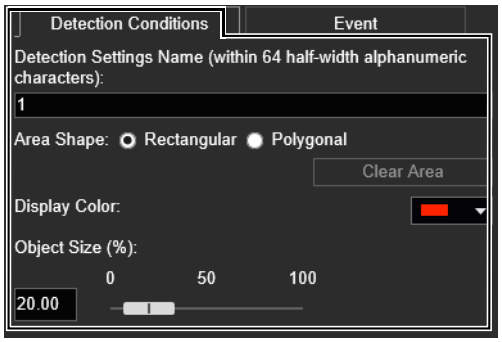


Note

- To disable the detection settings, clear the [Enable these detection settings] checkbox.
- Enter the [Detection Settings Name] if necessary (P. 128).
- To delete detection area settings, select the detection area settings to delete and click [Delete] in Detection Settings (List).

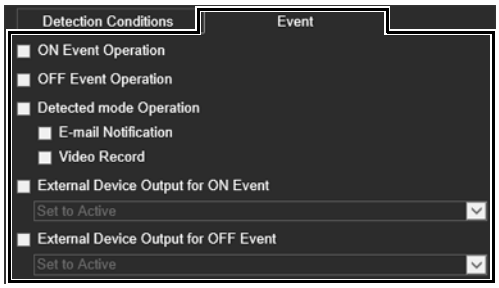
4 Configure the detection criteria.

Set criteria in the video display area or [Detection Conditions] tab (P. 128). The detection criteria differ according to the detection type.



5 Configure event settings.

Set which operations to carry out for video detection in the [Event] tab (P. 141).



6 To register multiple detection settings, repeat steps 1 to 5.

7 Click [Apply].

The settings are saved to the camera.

Note

To restore settings, click [Clear] before applying. This discards the settings you have specified and restores the settings saved in the camera. However, note that detection settings only added to the detection setting area by clicking [Add] are all discarded.

8 Check the detection result.

You can check the detection status of the specified detection settings in video display area, the [Event] column in [Detection Settings] or the [Event and Input/Output] menu in the Camera Viewer (P. 58).

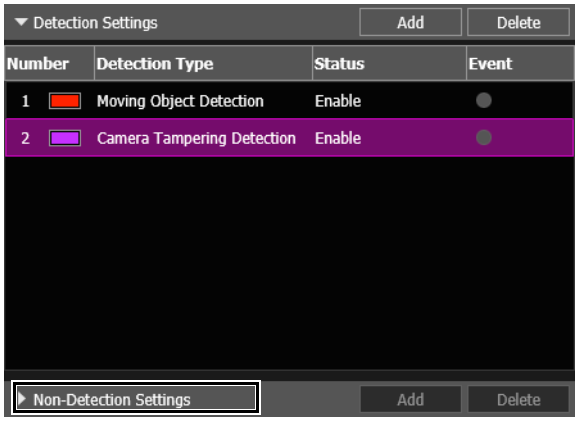
Setting a Non-Detection Area

You can set an area where changes are not detected, to prevent mis-detection and non-detection.

Important

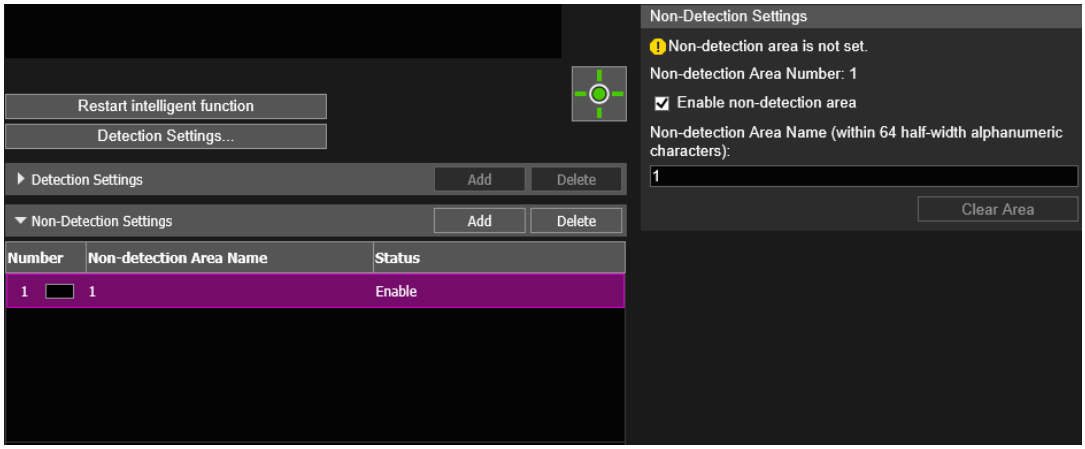
- The non-detection area set in the non-detection area settings is reflected in all detection settings.
- If the area in the detection settings and the area in the non-detection area settings overlap, the non-detection settings are prioritized.

1 Click [Non-Detection Settings] to display the list of non-detection area settings.



2 Click [Add].

The non-detection area settings added in [Non-Detection Settings] are displayed and the [Enable non-detection area] checkbox is selected.



Note

- Up to five non-detection area settings can be registered.
- To disable non-detection area settings, clear the [Enable non-detection area] checkbox.
- To delete non-detection area settings, select the non-detection area settings to delete and click [Delete] in Non-detection Area Settings (List).

3 Set a non-detection area in the video display area.

Click the mouse to create a polygon. For information on the creation method, please refer to “Using [Polygonal]” (P. 128).

Note

- You can create a polygonal area with a maximum of 32 vertices. You cannot set a non-detection area with only a straight line.
- Click [Clear Area] to set the non-detection area again.
- Enter [Non-detection Area Name (within 64 half-width alphanumeric characters)] as necessary.
- The non-detection area is shown in the video display area in black. The display color cannot be selected.

4 To register multiple non-detection areas, repeat steps 2 and 3.

5 Click [Apply].

The settings are saved in the camera.

Note

Click [Clear] to discard the settings and restore the settings saved in the camera. However, note that non-detection areas only added to the non-detection areas by clicking [Add] are all discarded.

6 Check the detection result.

The status of the specified non-detection settings can be checked in the video display area and the [Status] column in [Non-Detection Settings].
If the [Enable non-detection area] checkbox is cleared, [Disable] is displayed for the [Status] column in [Non-Detection Settings], and the non-detection area is not shown in the video display area.

Important

- Make sure to check the video display area to see whether the detection area and non-detection area are unintentionally overlapped.
- If you set the detection area and non-detection area close to each other, detection may be performed incorrectly.

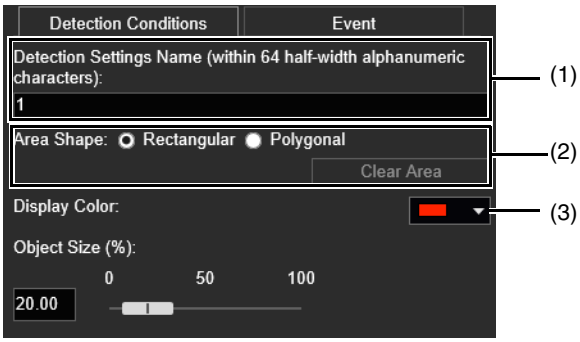
Configuring Detection Criteria ([Detection Conditions] Tab)

Detection criteria is controlled and set in the video display area for each type of detection.

Important

It is recommended that you configure the detection criteria in conditions as close as possible to the actual conditions in which you will use the camera.

Settings Common to Each Detection Type



(1) [Detection Settings Name (within 64 half-width alphanumeric characters)]
Enter a detection name. Be sure to enter a name in [Detection Settings Name (within 64 half-width alphanumeric characters)].

(2) [Area Shape]
Configure whether the detection area is a rectangle or a free-shape polygon.

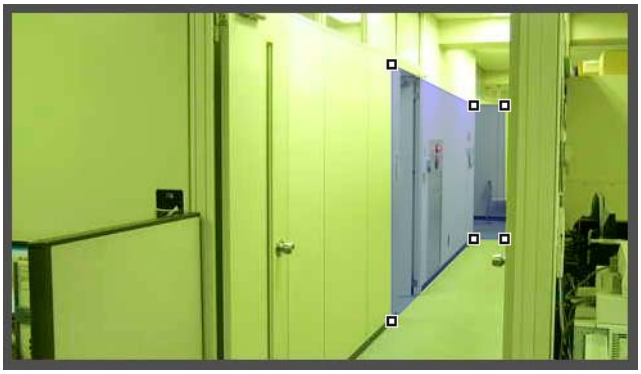
Note

You cannot select [Area Shape] for camera tampering detection.

Using [Rectangular]
Configure the detection area by moving, resizing or changing the shape of the rectangle that is shown in the video display area.

Drag the area to move it, and drag the vertices to resize it.

Using [Polygonal]
Click the video display area to place a vertex for the polygon at the clicked position.
Place the vertices in order, then either click the first vertex again or double-click the last vertex to set the polygon detection area.



Drag the area to move it, and drag the vertices to resize it.
You can specify polygonal areas with a maximum of 32 vertices.

Note

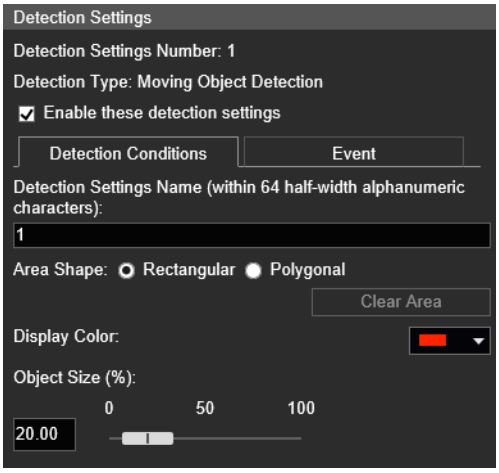
If you change the shape of a detection area you have already configured, the area is deleted and you switch to configuring a new area.

[Clear Area]
The detection area configured with [Polygonal] is deleted.

(3) [Display Color]
Select the color for detection areas and detection lines.

How to Configure Moving Object Detection

Set the area you want to detect a moving object in as a detection area.

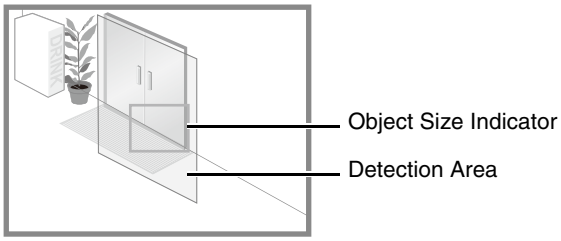


1 Select [Rectangular] or [Polygonal].

2 In the video display area, draw the area in which you would like to detect moving objects (P. 128).

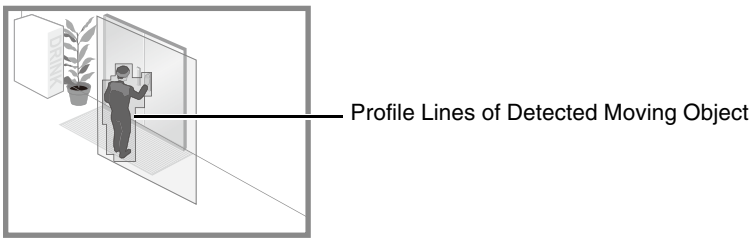
3 Configure the size of the object needed for triggering detection in [Object Size (%)].

This determines how large the moving object must be in relation to the detection area you set in step 2 for motion detection to be triggered.
When the setting values or slider is changed, an indicator representing the object size is shown for one second in the center of the video display area allowing you to check the size ratio while specifying the setting.



Detection Status for Moving Object Detection

All moving objects detected are displayed with profile lines.
If a moving object is smaller than [Object Size (%)], its profile lines are white.
If the moving object is larger than [Object Size (%)], its profile lines take on the same color as the detection area indicating “detected” status has been triggered.

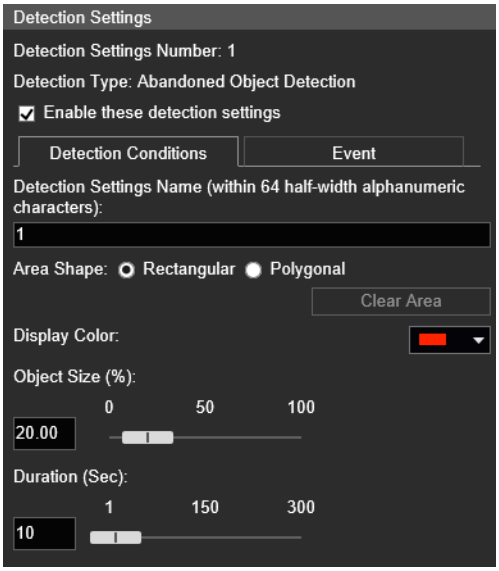


Note

If an object is placed in or removed from the moving object detection area, “detected” status will be triggered for Moving Object Detection.

How to Configure Abandoned Object Detection

Set the area you want to detect an abandoned object in as a detection area.



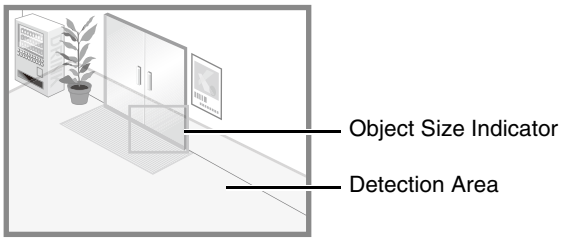
1. Select [Rectangular] or [Polygonal].

2. In the video display area, draw the area in which you would like to detect abandoned objects (P. 128).

3. Configure the size of the object needed for detection in [Object Size (%)].

   This determines how large the abandoned object must be in the detection area you set in step 2 to detect as an abandoned object.
   When the setting values or slider is changed, an indicator representing the object size is shown for one second in

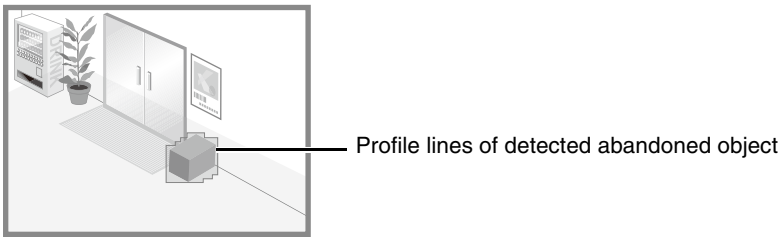
the center of the video display area allowing you to check the size ratio while setting.



4 Configure [Duration (Sec)] for the time required for an object to be detected as an abandoned object.

Detection Status for Abandoned Object Detection

All moving objects detected are displayed with profile lines.
If [Object Size (%)] and [Duration (Sec)] are not met, profile lines are white.
If both [Object Size (%)] and [Duration (Sec)] are exceeded, the profile lines take on the same color as the detection area, indicating that “detected” mode has been triggered.



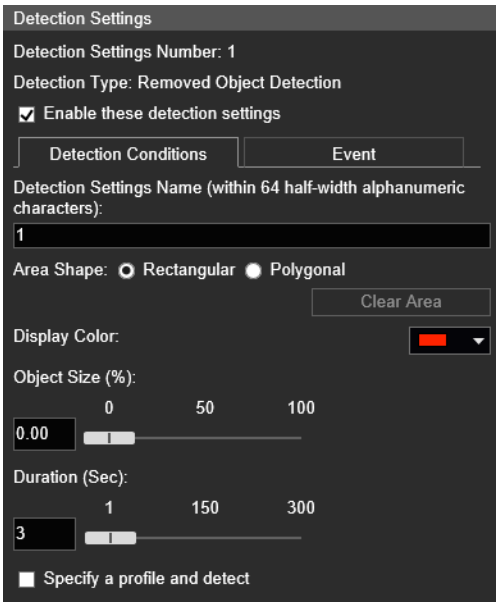
How to Configure Removed Object Detection

Set an area around the target objects, for Removed Object Detection. The following methods are available for configuring removed object detection.

- Setting a broad area for detecting the removal of objects
- Specifying the profile lines of objects for removal detection

If you cannot detect the intended objects using one of these methods, use the other method.

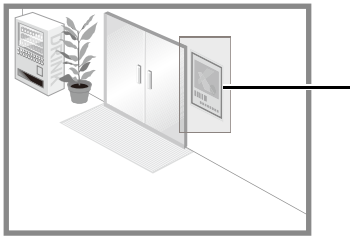
Setting a Broad Area for Detecting Removed Objects



Configure the following settings with the [Specify a profile and detect] checkbox cleared.

1 Select [Rectangular] or [Polygonal].

2 In the video display area, draw a broad area to detect removed objects (P. 128).



3 Configure the size of the object needed for triggering detection in [Object Size (%)].

Set how large an object that is removed must be to trigger removed object detection in the detection area set in step 2.
When the setting values or slider is changed, an indicator representing the object size is shown for one second in the center of the video display area allowing you to check the size ratio while specifying the setting.
A removed object is detected when the setting value in [Object Size (%)] is exceeded.

4 Configure [Duration (Sec)] for time required for an object to be detected as a removed object.

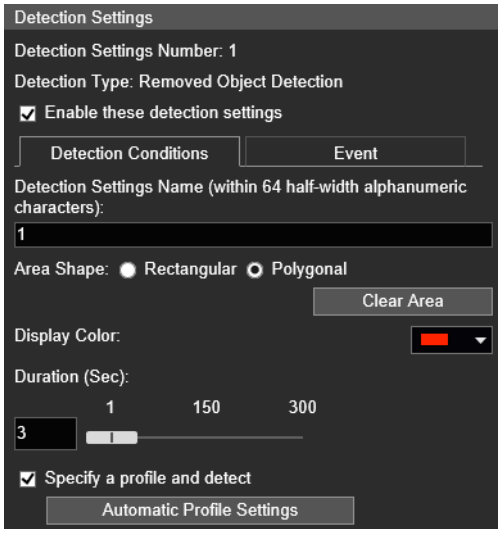
5 Click [Apply].

Important

- A removed object may not be detected in the following cases.
  - When long and thin objects are removed
  - When the same object is placed continuously and some of the objects are removed
  - When objects of the same shape are placed together and some of the objects are removed
- If the video inside the detection area changes without an object being removed, it may be misdetected as a removed object.

Specifying the Profile Lines of Objects for Removal Detection

1 Select the [Specify a profile and detect] checkbox.



2 Select [Rectangular] or [Polygonal].

3 Use the video display area to configure an area along the profile lines of the object you do not want removed (P. 128).
Alternatively, set the profile lines automatically using the following procedure.

Temporarily remove the target object for removed object detection from the video display area.

▼

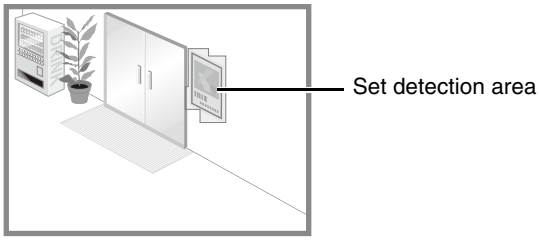
Click [Restart intelligent function] (P. 141).
The background image is generated

▼

Return the target object to its original position.

▼

Click [Automatic Profile Settings].
A profile line of the object is drawn using a polygon with up to 32 vertices.
If there are multiple objects detected, the profile lines are drawn around the object occupying the largest area.



▼

Click [Restart intelligent function] again.

Important

Set detection areas so that they precisely match the profile lines of the target object. Influence from the target object's shadow or adjacent objects may result in the target object being recognized as larger than it actually is and may not trigger removed object detection. If this occurs, reconfigure the detection area to outline the recognized target object.

4 Follow steps 4–5 in "Setting a Broad Area for Detecting Removed Objects" (P. 132).

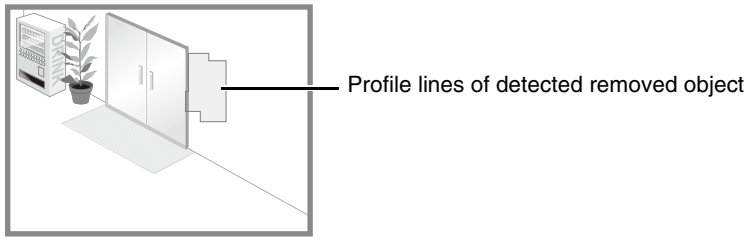
Detection Status for Removed Object Detection

All moving objects detected are displayed with profile lines.
If you set [Object Size (%)] and [Duration (Sec)], the following occurs.

- If [Object Size (%)] and [Duration (Sec)] are not met, the profile line is displayed with a white line.
- If both [Object Size (%)] and [Duration (Sec)] are exceeded, the profile line is displayed in the same color as the detection area to indicate that something has been detected.

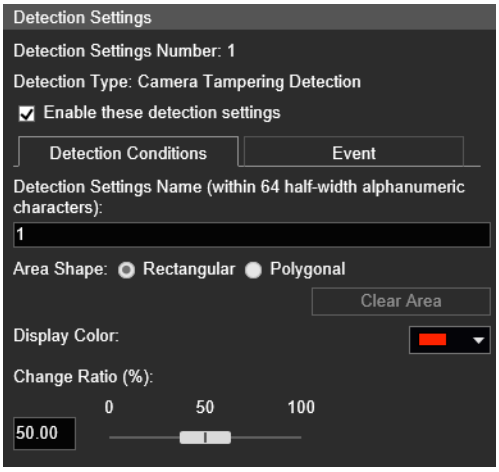
If removed object detection is set in [Specify a profile and detect], the following occurs.

- As long as [Duration (Sec)] is not exceeded, profile lines are white.
- When [Duration (Sec)] is exceeded, profile lines take on the same color as the detection area, indicating that an object has been removed.

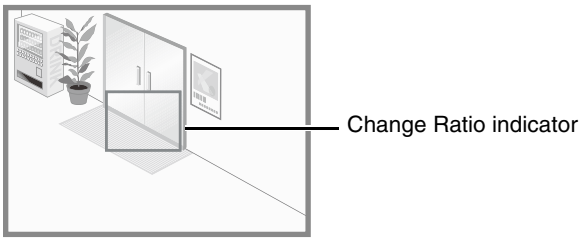


How to Configure Camera Tampering Detection

For [Camera Tampering Detection], the entire video display area is the detection area. The area cannot be changed.

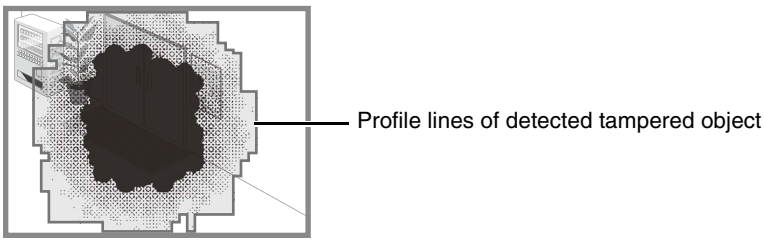


In [Change Ratio (%)], you can set the ratio of screen change for the entire video display area to determine as tampering detection.
When the setting values or slider is changed, an indicator representing the ratio of the entire video display area is shown for one second in the center of the video display area allowing you to check while specifying the setting.



Detection Status for Camera Tampering Detection

Moving objects detected are displayed with profile lines.
If an object is smaller than [Change Ratio (%)], its profile lines are white.
If the obscured area in the video exceeds [Change Ratio (%)], profile lines take on the same color as the detection area, indicating that the camera has “detected” tampering.

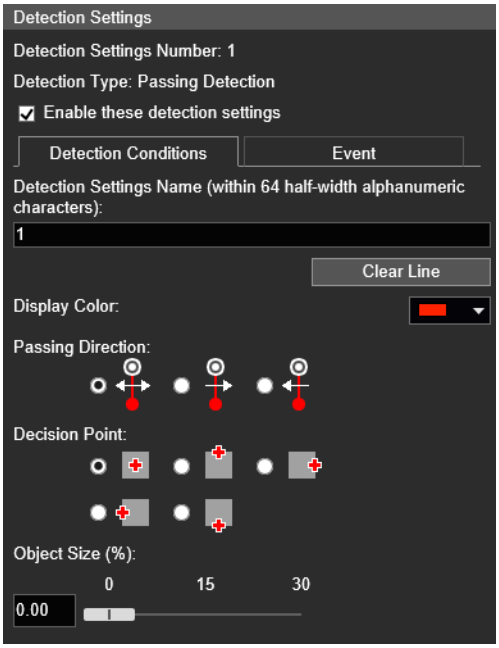


Note

Detection will not be possible for three seconds after the change ratio for camera tampering detection is changed, or when switching to camera tampering detection settings from settings for another detection mode.

How to Configure Passing Detection

The detection line for passing moving objects is determined by setting the passing direction and object decision point.



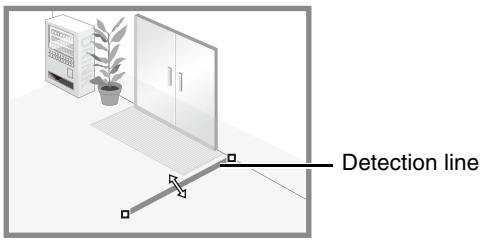
1 Follow the steps below to configure the passing detection line in the video display area.

In the video display area, click the start point of the detection line.

▼

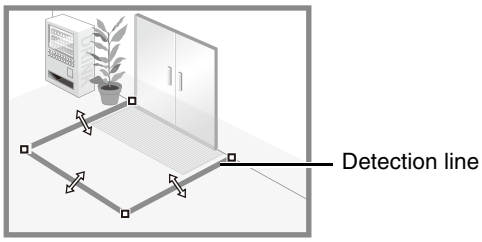
Click another point.

The passing detection line will be set between the start point and next point you clicked.



▼

To configure a polygonal detection line, click the vertices of the line in order.



You can configure a polygonal detection line with a maximum of 32 vertices.

▼

Click any of the set vertices.

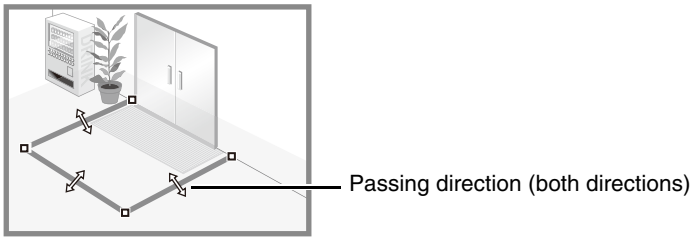
The detection line is determined.

Note

- Even after configuring a detection line, you can drag each vertex to change the shape of the detection line and the lines between vertices to move the entire detection line.
- Click [Clear Line] to delete a detection line.

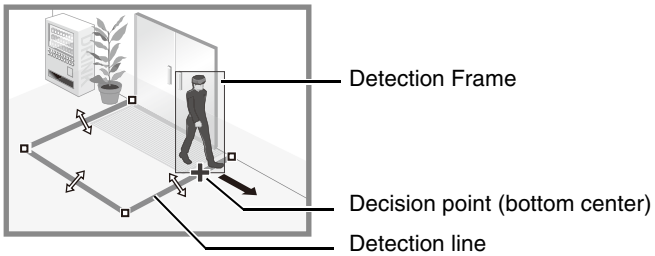
2 In [Passing Direction], select the direction for moving objects to pass the detection line.

If a moving object crosses the detection line in the selected direction, it will be detected as 'passed'.
A preview display shows the selected passing direction on the detection line in the video display area.



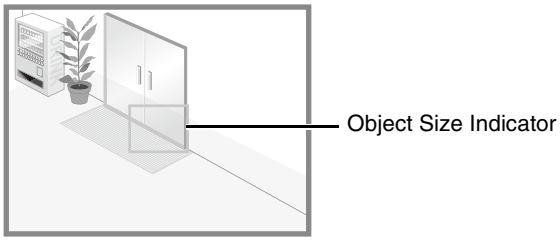
3 In [Decision Point], select the point of a moving object that will be used for triggering passing detection when the moving object crosses a detection line.

If the selected decision point crosses the detection line, it will be detected as 'passed'.
The decision point is indicated by a cross on the detection frame of the moving object.



4 Configure the size of the moving object needed for triggering detection in [Object Size (%)].

Set the size ratio of moving objects for the entire screen.
If the moving object exceeds the set value for [Object Size (%)], it will be targeted for passing detection.
When the setting values or slider is changed, an indicator representing the object size is shown for one second in the center of the video display area allowing you to check the size ratio while specifying the setting.



Note

A ratio of up to 30% can be set in [Object Size (%)] for passing detection.

Detection Status for Passing Detection

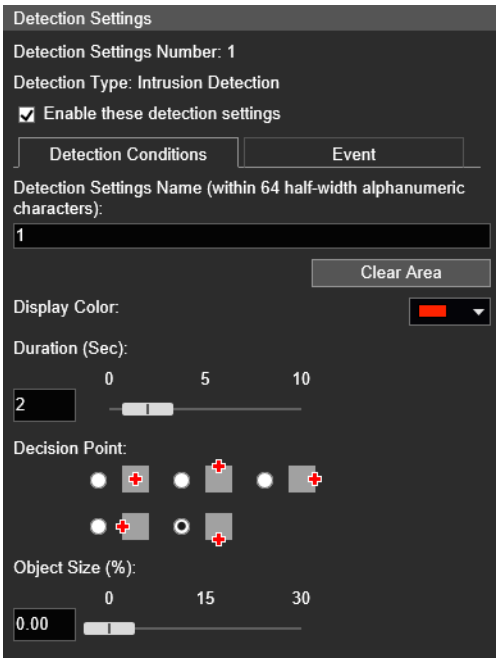
All moving objects detected are displayed with white profile lines.
When the [Decision Point] of a moving object that meets the [Object Size (%)] setting crosses a detection line in the direction specified in [Passing Direction], the profile line changes to the same color as the detection line, and the status becomes "detected".
Notification of a passing detection event occurs only when the decision line is crossed. Take care in setting the operation to be performed when an event occurs.

Important

Perform a detection test after configuring passing detection to make sure the detection frame of a moving object continues to be displayed.

How to Configure Intrusion Detection

Set the area for which you want to detect intrusions.

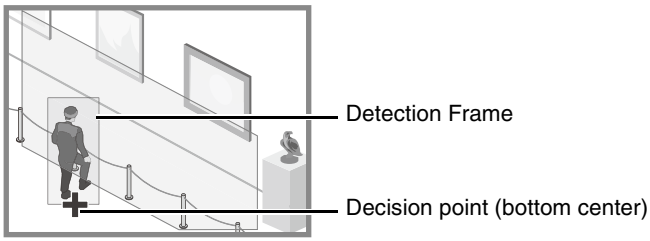


1 In the video display area, draw the area in which you would like to detect intruding objects (P. 128).

2 Configure [Duration (Sec)] for the time required for an object to enter a detection area, and be detected as an intrusion.

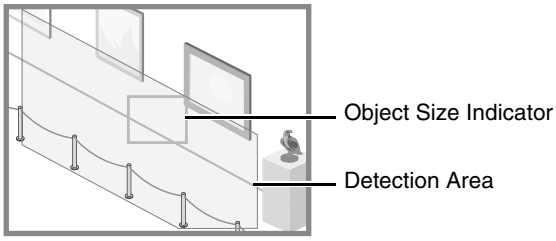
3 In [Decision Point], select the point of a moving object that will be used for triggering intrusion detection when the moving object enters a detection area.

The decision point is indicated by a cross on the detection frame of the moving object.



4 Configure the size of the moving object needed to trigger detection in [Object Size (%)].

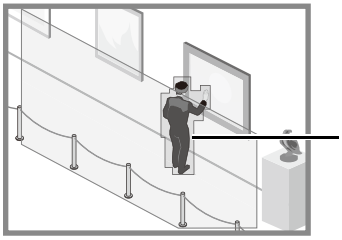
Set the size ratio of moving objects for the entire screen.
When the setting values or slider is changed, an indicator representing the object size is shown for one second in the center of the video display area allowing you to check the size ratio while specifying the setting.



Detection Status for Intrusion Detection

All moving objects detected are displayed with profile lines.

When [Decision Point] of a moving object larger than [Object Size (%)] enters a detection area and exceeds [Duration (Sec)], its profile lines take on the same color as the detection area, indicating that “detected” mode has been triggered.



Important

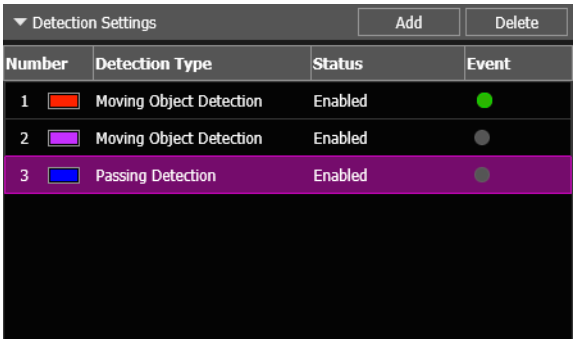
After the Intrusion Detection is set, please confirm that the system continues to show profile lines of the detected moving object.

Configuring Operations for “Detected” ([Event] Tab)

Set operations to be performed upon detection of changes in a subject.
For details on settings, please refer to “Configuring Operations for “Detected” ([Event] Tab)” (P. 141).

Checking Event Status

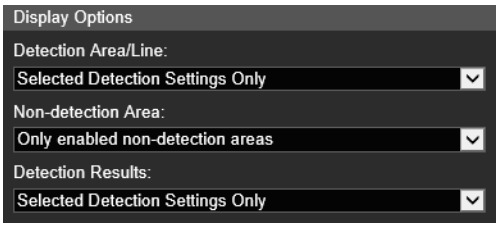
If the intelligent function (moving object detection, abandoned object detection, removed object detection, camera tampering detection, passing detection, and intrusion detection) detects something, the event icon in that row turns green. The detection status of video detection can also be checked in the Event and Input/Output menu of the Camera Viewer (P. 59).



No.1: Video Detection Status is ON
No.2 and 3: Video Detection Status is OFF

Displaying Settings for Detection Areas/Detection Lines, Non-Detection Area and Detection Results (Display Options)

Configure the detection area/line, non-detection area, and detection results displayed in the video display area.



You can select the following for either [Detection Area/Line] or [Detection Results].

[Selected Detection Settings Only]
Show the detection areas/lines or detection results only for those detection settings selected in Detection Settings (List).

[All Detection Settings]
Show the detection areas/lines or detection results for all detection settings in Detection Settings (List).

[Detection Settings of the Same Type]
Show the detection areas/lines or detection results for the same types of detection settings as those selected in Detection Settings (List).

[Disable]
No detection areas/lines or detection results are displayed.

The following settings can be selected for [Non-detection Area].

[Only selected non-detection areas]
Only the non-detection areas selected in the Non-detection Area Settings (List) are displayed.

[All non-detection areas]
All the non-detection areas in the Non-detection Area Settings (List) are displayed.

[Only enabled non-detection areas]
Only the non-detection areas with [Status] set to [Enabled] in the Non-detection Area Settings (List) are displayed.

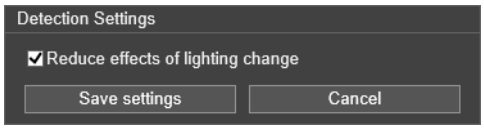
[Disable]
No non-detection areas are displayed.

Reducing Effects of Lighting Change (Detections Settings)

The Intelligent Function may not work when the entire screen is exposed to sudden changes in brightness, for example, when indoor lights are turned on or off. Changing the detection settings may reduce this effect.

1 Click [Detection Settings].

2 Select [Reduce effects of lighting change] checkbox.



3 Click [Save settings].

The settings are saved and the Intelligent Function restarts.

Important

- It takes several seconds for the Intelligent Function to restart. No detection is performed while restarting.
- Settings in [Reduce effects of lighting change] may not work depending on the operating environment. Repeated sudden changes in brightness may also have the same effect. Perform a detection test to check whether settings work correctly.

Context Menu

Right-click on the video display area, Detection Settings (List) and Non-Detection Settings (List) to display a menu that allows you to use the following functions. Unavailable functions will be grayed out when you right-click.

[Copy detection area/line]
Copy the detection area/line of the selected detection setting to the clipboard.

[Paste detection area/line]
Paste the copied detection area/line from the clipboard to the detection setting being configured. Paste cannot be used with camera tampering detection.
Pasting a detection line is possible only when setting passing detection in the copy source and the paste target.

[Clear detection area/line]
Delete the detection area/line of the selected detection setting. If the shape of the area is rectangular, or the area is a camera tampering detection area, the area cannot be deleted.

[Copy detection condition settings]
Copy the detection criteria of the selected detection setting to the clipboard. The detection settings name and display color are not copied.

[Paste detection condition settings]
Paste the copied detection criteria from the clipboard to the detection setting being configured. Pasting is possible only if the source and the target are the same detection type.

[Copy event settings]
Copy the event settings of the selected detection setting to the clipboard.

[Paste event settings]
Paste the copied event settings from the clipboard to the detection setting being configured.

[Copy non-detection area]
Copies a non-detection area that has been set to the clipboard.

[Paste non-detection area]
Pastes a non-detection area copied to the clipboard to the non-detection area that is being set.

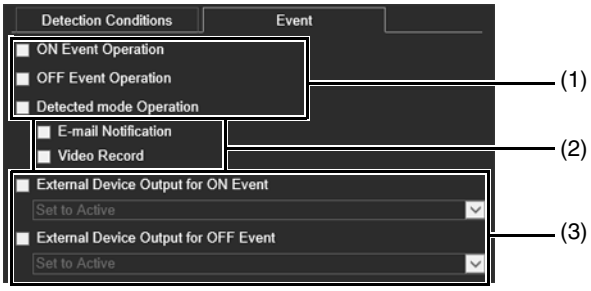
[Clear non-detection area]
Deletes the non-detection area that is being set.

[Event] > [Intelligent Function]
- Shared Operations -

This explains functions common to video detection.

Configuring Operations for “Detected” ([Event] Tab)

Set operations to be performed upon detection of changes in a subject.



(1) Specify Operation Timing (Multiple Selections Possible)

[ON Event Operation]
When selected, the operations set in (2) are performed when the mode becomes “detected”.

[OFF Event Operation]
When selected, the operations set in (2) are performed when “detected” mode ends.

[Detected mode Operation]
When selected, the operations set in (2) are performed while “detected” mode is active.

(2) Specify Event Operation (Multiple Selections Possible)

[E-mail Notification]
When selected, e-mail notification is sent according to the timing set in (1). [Video Record] > [E-mail Notification] on the Setting Page must be set in advance (P. 114).

[Video Record]
When selected, video recording begins according to the timing specified in (1). [Video Record] > [Upload] (P. 110) or [Memory Card] > [Video Record Settings] (P. 155) on the Setting Page must be set in advance.

(3) External Device Output Operations

[External Device Output for ON Event]
Select this to start or pause output to an external device when the mode becomes “detected”, and to select the operation (active or inactive).

[External Device Output for OFF Event]
Select this to start or pause output to an external device when “detected” mode ends, and to select the operation (active or inactive).

Restarting Intelligent Function

If the background video has changed while you were specifying settings or detection results are not as specified, restart the Intelligent Function.

1 If you have not yet obtained the camera control privileges, click the [Obtain/Release Camera Control Privileges] button and obtain the control privileges.

2 Click [Restart intelligent function].

Important

It takes several tens of seconds for the Intelligent Function to restart. No detection is performed while restarting.

[Event] > [Infrared Switching]
Executing Presets When Switching Infrared Mode

When events trigger the switching of infrared mode, presets registered in advance can be executed, such as changing the camera angle or video quality settings.

The following settings can be configured here.
- Infrared Switching

Infrared Switching

[Preset when Switching to Normal Capture]
Executes the preset when switched to normal capture.

[Preset when Switching to Infrared]
Executes the preset when switched to the infrared mode.

Important

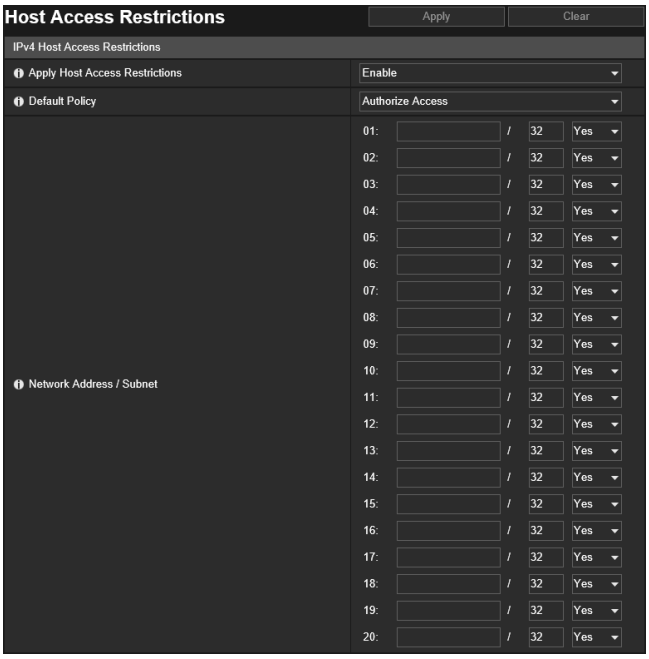
When the user has camera control privileges, the presets for [Preset when Switching to Normal Capture] and [Preset when Switching to Infrared] will not run.

Note

- It is necessary to set presets beforehand with [Camera] > [Preset] (P. 92).
- You can set the timing for event-triggered infrared switching in [Infrared Switching] in [External Device Input] (P. 117) or [Timer] (P. 118).

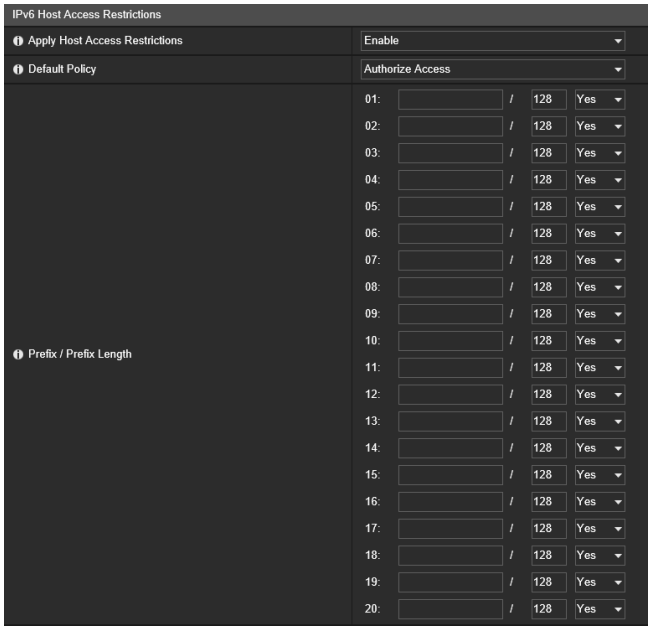
[Security] > [Host Access Restrictions]
Setting Access Restrictions

Separate access control from IPv4 and IPv6 addresses can be set.



The following settings can be configured here.

- IPv4 Host Access Restrictions
- IPv6 Host Access Restrictions



Important

- To prohibit access via a proxy server in HTTP connection, a proxy server address must be set.
- If host access restriction is set mistakenly, access to the Setting Pages themselves may be prohibited, in which case restoring the factory default settings will become the only means of recovery.

Note

If the same address is duplicated, the address policy that is displayed highest on the list will be applied.

IPv4 Host Access Restrictions

Specify the hosts from which IPv4 access is permitted and prohibited.

[Apply Host Access Restrictions]
Select whether to use IPv4 host access restrictions.

[Default Policy]
Select whether to allow or block access from IPv4 addresses that have not been specified in [Network Address / Subnet].

[Network Address / Subnet]
Enter IPv4 addresses into the list and select [Yes] or [No] for access for each address.
You can specify the subnet to set access restrictions by network or host.
If set to [No], access to all ports is blocked.

IPv6 Host Access Restrictions

Specify the hosts from which IPv6 access is permitted and prohibited.

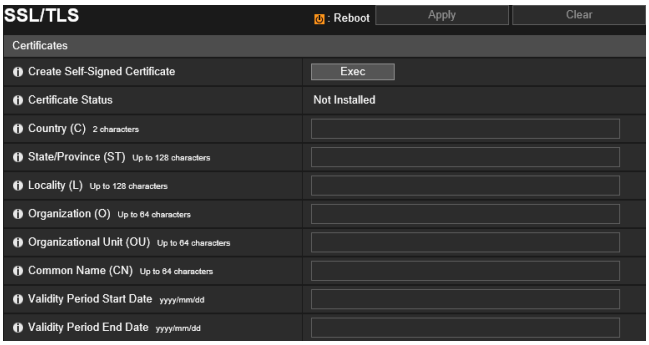
[Apply Host Access Restrictions]
Select whether to use IPv6 host access restrictions.

[Default Policy]
Select whether to allow or block access from IPv6 addresses that have not been specified in [Prefix / Prefix Length].

[Prefix / Prefix Length]
Enter IPv6 addresses (prefixes) into the list and select [Yes] or [No] for access for each address.
You can specify the prefix length to set access restriction by network or host.
If set to [No], access to all ports is blocked.

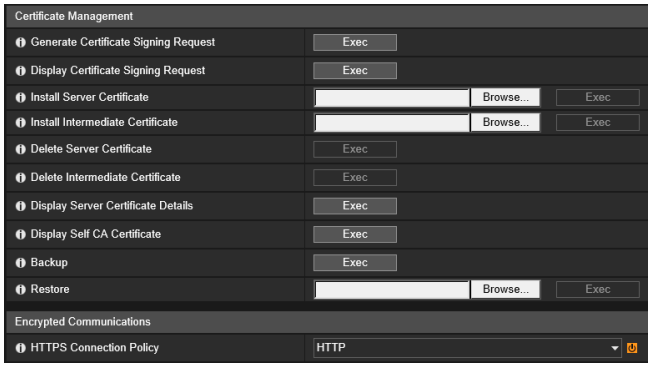
[Security] > [SSL/TLS]
Setting HTTP Communication Encryption

Certificate creation and management, and encrypted communication settings.



The following settings can be configured here.

- Certificates
- Certificate Management
- Encrypted Communications



Certificates

Create an SSL/TLS certificate.

Important

Use a self-signed certificate when complete security does not need to be ensured, such as through operation tests. For system operation, it is recommended that you acquire and install a certificate issued by a CA.

[Create Self-Signed Certificate]

Enter the following items, click [Apply], and click [Exec] to create a self-signed certificate.
Follow the displayed message and reboot. The certificate created will take effect after rebooting.

Note

Creating a certificate takes time, so it is recommended that you stop video transmission and upload processes.

[Certificate Status]

If no certificate is installed, [Not Installed] will be displayed. If a certificate is installed, the validity period for the certificate will be displayed.

[Country (C)]

Enter the ISO3166-1 alpha-2 country code.

[State/Province (ST)], [Locality (L)], [Organization (O)], [Organizational Unit (OU)], [Common Name (CN)]

Enter state/province name, locality, organization name, organizational unit and common name in alphanumeric characters (spaces or printable characters).
Enter an FQDN format host name, etc. to set the common name (required).

[Validity Period Start Date], [Validity Period End Date]

Set the validity period of the certificate to be created (required when creating a self-signed certificate).

Certificate Management

Manage the SSL/TLS certificate.

[Generate Certificate Signing Request]
Click [Exec] to create a server private key and generate a certificate signing request.
Once processed, the certificate signing request will be displayed in a separate window.

Note

Generating a certificate signing request takes time, so it is recommended that you stop video transmission and upload processes.

[Display Certificate Signing Request]
Click [Exec] to view the details of the certificate signing request.

[Install Server Certificate]
Perform this operation to install a server certificate.
Specify the certificate file to be installed using [Browse] and click [Exec].
The certificate installed will take effect after rebooting.

[Install Intermediate Certificate]
Perform this operation to install an intermediate certificate.
Specify the certificate file to be installed using [Browse] and click [Exec].
The certificate installed will take effect after rebooting.

Note

To install an intermediate certificate and a cross root certificate, use a text editor or similar software to place them in the same file and install them as an intermediate certificate.

[Delete Server Certificate]
Click [Exec] to delete the server certificate.
However, if SSL/TLS communications are enabled, the certificate cannot be deleted. Set [HTTPS Connection Policy] to [HTTP] before deleting a certificate.
The deletion will take effect after rebooting.

[Delete Intermediate Certificate]
Click [Exec] to delete the intermediate certificate along with the cross root certificate.
However, if SSL/TLS communications are enabled, the certificate cannot be deleted. Set [HTTPS Connection Policy] to [HTTP] before deleting a certificate.
The deletion will take effect after rebooting.

[Display Server Certificate Details]
Click [Exec] to view the details of the server certificate.

[Display Self CA Certificate]
Used for the purpose of testing SSL/TLS communications, but otherwise not normally used.

[Backup]
Click [Exec] to perform a backup of the certificates and private key. This can only be performed when [HTTPS] or [HTTP and HTTPS] is set for [HTTPS Connection Policy] to perform SSL/TLS communication.

[Restore]
Installs the certificates and private key from backup.
Click [Browse] to specify the backup file, then click [Exec]. This can only be performed when [HTTPS] or [HTTP and HTTPS] is set for [HTTPS Connection Policy] to perform SSL/TLS communication.
The restored certificate will take effect after rebooting.

Encrypted Communications

Set encrypted communications.

[HTTPS Connection Policy]
Set SSL/TLS communication with HTTPS connections.
Select [HTTP] if you do not want to perform SSL/TLS communication.
Select [HTTPS] or [HTTP and HTTPS] if you want to perform SSL/TLS communication. Connections using SSL/TLS are enabled after rebooting.

If you select [HTTPS], HTTP access is also redirected to HTTPS to perform SSL/TLS communication.

Important

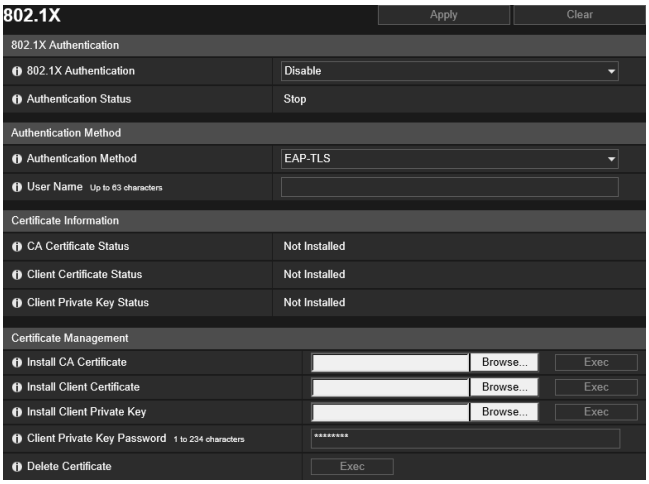
- Even if you set SSL/TLS communication here, SSL/TLS communication is not performed unless you install a certificate.
- Video distribution performance decreases when performing SSL/TLS communication.

Note

- It may take a few minutes to generate an SSL/TLS key.
- Depending on the type of the certificate being installed on the camera, a dialog box may be displayed indicating that the web browser has accepted the certificate and a connection can be made. If the dialog box is not displayed, register the CA certificate in the web browser.

[Security] > [802.1X]
Network Port Authentication Settings

Settings for 802.1X authentication and authentication status display, and for certificate management.



The following settings can be configured here.
- 802.1X Authentication
- Authentication Method
- Certificate Information
- Certificate Management

802.1X Authentication

Display the 802.1X authentication enable/disable control and status.

[802.1X Authentication]
Select this to enable or disable 802.1X authentication.

[Authentication Status]
Display the status of 802.1X authentication. There are three types of status: [Authenticated], [Unauthenticated], and [Stop].

Authentication Method

Set the authentication method used for 802.1X authentication.

[Authentication Method]
Select [EAP-MD5], [EAP-TLS], [EAP-TTLS], or [EAP-PEAP] as the authentication method to use for 802.1X authentication.

[User Name]
Enter the user name used for authentication.

[Password]
Enter the required password for authentication.
This is displayed only when [Authentication Method] is set to [EAP-MD5], [EAP-TTLS], or [EAP-PEAP].

Certificate Information

This is displayed only when [Authentication Method] is set to [EAP-TLS], [EAP-TTLS], or [EAP-PEAP].

[CA Certificate Status]
If no CA certificate is installed, [Not Installed] is displayed. If a CA certificate is installed, the validity period of the certificate is displayed.

[Client Certificate Status]
If no client certificate is installed, [Not Installed] is displayed. If a client certificate is installed, the validity period of the certificate is displayed.
This is displayed only when [Authentication Method] is set to [EAP-TLS].

[Client Private Key Status]
If no client private key is installed, [Not Installed] is displayed. If a client private key is installed, [Installed] is displayed.
This is displayed only when [Authentication Method] is set to [EAP-TLS].

Certificate Management

This is displayed only when [Authentication Method] is set to [EAP-TLS], [EAP-TTLS], or [EAP-PEAP].

Important

- If any CA certificates, client certificates, and client private keys already exist when installing certificates, they are discarded and new versions are installed.
- An error occurs if the format of the certificate or private key to be installed is incorrect.
- Client certificates and client private keys are checked as a pair when installing, and an error occurs if they do not match.
- The certificate and private key used for 802.1X authentication must be installed as separate items, irrespective of the installation status of certificates for SSL/TLS.

[Install CA Certificate]
Installs a CA certificate.
Specify the certificate file to be installed using [Browse] and click [Exec].

[Install Client Certificate]
Installs a client certificate.
Specify the certificate file to be installed using [Browse] and click [Exec].
This is displayed only when [Authentication Method] is set to [EAP-TLS].

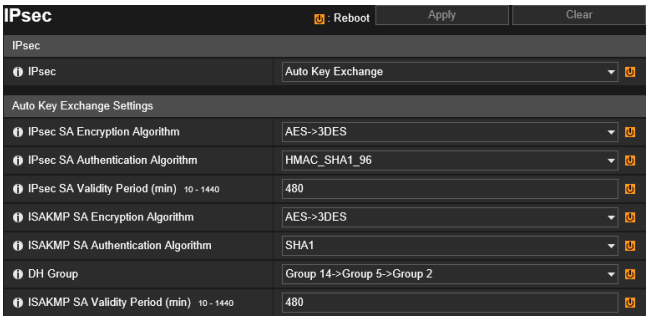
[Install Client Private Key]
Installs a client private key.
Specify the private key file to be installed using [Browse] and click [Exec].
This is displayed only when [Authentication Method] is set to [EAP-TLS].

[Client Private Key Password]
Enter the password for the client private key.
Required when a password has been configured for the private key.
This is displayed only when [Authentication Method] is set to [EAP-TLS].

[Delete Certificate]
Deletes all installed CA certificates, client certificates, and client private keys.
Only “CA Certificate” is displayed when [Authentication Method] is set to [EAP-TTLS] or [EAP-PEAP], but any installed client certificates and client private keys are also deleted.

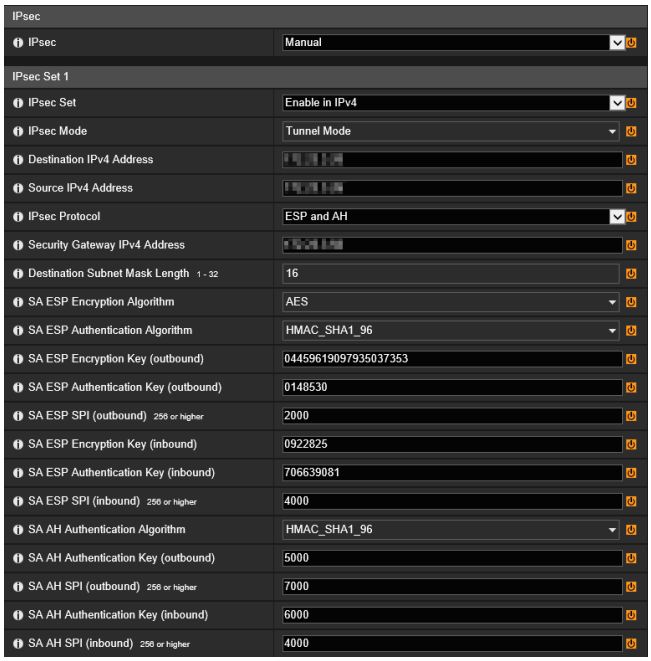
[Security] > [IPsec]
Setting IPsec

Settings for using IPsec.



The following settings can be configured here.

- IPsec
- Auto Key Exchange Settings
- IPsec Set 1 to 5



Important

- To run this camera with IPsec, the communicating devices and network must be set beforehand. Contact your system administrator for these settings.
- When connecting with IPsec, set the camera IP address manually.
  For IPv4 addresses, use addresses with [IPv4 Address Settings Method] set to [Manual] in [Basic] > [Network] > [IPv4].
  For IPv6 addresses, use addresses set with [IPv6 Address (Manual)] in [Basic] > [Network] > [IPv6].
- If the IPsec setting is changed and the camera may become inaccessible from the active web browser, a confirmation dialog box will be displayed. Click [OK] to apply the new settings.
  If you reboot the camera and cannot connect to the camera from the web browser, any available URI for connecting to the camera will be displayed in a message.
  If you cannot connect to the camera through the displayed URI, contact your system administrator.

Note

If IPsec is used, video transmission performance drops.

IPsec

[IPsec]
Select the key exchange method when using IPsec.

Auto Key Exchange Settings

[IPsec SA Encryption Algorithm]
Select the IPsec SA encryption algorithm.
The specified algorithm will be checked for an applicable encryption algorithm starting from the left.

[IPsec SA Authentication Algorithm]
Select the IPsec SA authentication algorithm.
The specified algorithm will be checked for an applicable authentication algorithm starting from the left.

[IPsec SA Validity Period (min)]
Enter the duration of validity for IPsec SA.

[ISAKMP SA Encryption Algorithm]
Select the SA encryption algorithm for use with auto key exchange protocol IKE.

[ISAKMP SA Authentication Algorithm]
Select the SA authentication algorithm for use with auto key exchange protocol IKE.

[DH Group]
Select the key generation information that will be used in the DH algorithm for key exchange via auto key exchange protocol IKE. The higher the group number, the stronger security will be.

[ISAKMP SA Validity Period (min)]
Enter the duration of validity for ISAKMP SA.

IPsec Set 1 to 5

IP security can be specified through auto key exchange or manual setting with up to five communicating devices.

■ Auto Key Exchange

Important
If the camera is rebooted during auto key exchange communication, a connection error may result after rebooting. If this occurs, connect again.

Note
If auto key exchange is used, it will take approximately 5 to 10 seconds before communication with the camera starts.

[IPsec Set]
Select which IPsec sets the camera will use; IPv4, IPv6, or neither.

[IPsec Mode]
Select the IPsec mode.

[Destination IPv4 Address], [Destination IPv6 Address]
Enter the IP address of the connection destination.

[Source IPv4 Address], [Source IPv6 Address]
Enter the IP address of the source.

[IPsec Protocol]
Select the IPsec protocol.

[Security Gateway IPv4 Address], [Security Gateway IPv6 Address]
Enter the IP address of the security gateway if [IPsec Mode] is set to [Tunnel Mode].

[Destination Subnet Mask Length], [Destination Prefix Length]
Enter the subnet mask (IPv4) or prefix length (IPv6) when [IPsec Mode] is set to [Tunnel Mode].

[IKE Pre-Shared Key]
Enter the pre-shared key for IKE (auto key exchange).

Manual

[IPsec Set]
Select which IPsec sets the camera will use; IPv4, IPv6, or neither.

[IPsec Mode]
Select the IPsec mode.

[Destination IPv4 Address], [Destination IPv6 Address]
Enter the IP address of the connection destination.

[Source IPv4 Address], [Source IPv6 Address]
Enter the IP address of the source.

[IPsec Protocol]
Select the IPsec protocol.
If you select [ESP], enter only the setting items relating to ESP.
If you select [AH], enter only the setting items relating to AH.
If you select [ESP and AH], enter all setting items.

[Security Gateway IPv4 Address], [Security Gateway IPv6 Address]
Enter the IP address of the security gateway if [IPsec Mode] is set to [Tunnel Mode].

[Destination Subnet Mask Length], [Destination Prefix Length]
Enter the subnet mask (IPv4) or prefix length (IPv6) when [IPsec Mode] is set to [Tunnel Mode].

If the Setting in [IPsec Protocol] Includes “ESP”

[SA ESP Encryption Algorithm]
Set the ESP encryption algorithm to suit the encryption algorithm supported by the device to connect to.
Normally [AES] or [3DES] is recommended.

[SA ESP Authentication Algorithm]
Set the ESP authentication algorithm to suit the authentication algorithm supported by the device to connect to.
If [ESP] is used alone, [No Authentication] cannot be selected.

[SA ESP Encryption Key (outbound)]
Enter the SA encryption key for outbound.
If [AES], [3DES] or [DES] was selected in [SA ESP Encryption Algorithm], set a 128-bit, 192-bit or 64-bit hexadecimal number, respectively. This item need not be set if [NULL] was selected.

[SA ESP Authentication Key (outbound)]
Enter the SA authentication key for outbound.
If [HMAC_SHA1_96] or [HMAC_MD5_96] was selected in [SA ESP Authentication Algorithm], set a 160-bit or 128-bit hexadecimal number, respectively. This item need not be set if [No Authentication] was selected.

[SA ESP SPI (outbound)]
Enter the SA SPI value for outbound.
Set a desired value in the range of 256 to 4294967295.

[SA ESP Encryption Key (inbound)]
Enter the SA encryption key for inbound.
If [AES], [3DES] or [DES] was selected in [SA ESP Encryption Algorithm], set a 128-bit, 192-bit or 64-bit hexadecimal number, respectively. This item need not be set if [NULL] was selected.

[SA ESP Authentication Key (inbound)]
Enter the SA authentication key for inbound.
If [HMAC_SHA1_96] or [HMAC_MD5_96] was selected in [SA ESP Authentication Algorithm], set a 160-bit or 128-bit hexadecimal number, respectively. This item need not be set if [No Authentication] was selected.

[SA ESP SPI (inbound)]
Enter the SA SPI value for inbound.
Set a desired value in the range of 256 to 4294967295.
Since this setting is used as an ID for identifying the SA, be careful not to specify an inbound SPI whose value is already used in another ESP’s SPI.

If the Setting in [IPsec Protocol] Includes “AH”

[SA AH Authentication Algorithm]
Set the AH authentication algorithm to suit the authentication algorithm supported by the device to connect to.

[SA AH Authentication Key (outbound)]
Enter the SA authentication key for outbound.
If [HMAC_SHA1_96] or [HMAC_MD5_96] was selected in [SA AH Authentication Algorithm], set a 160-bit or 128-bit hexadecimal number, respectively.

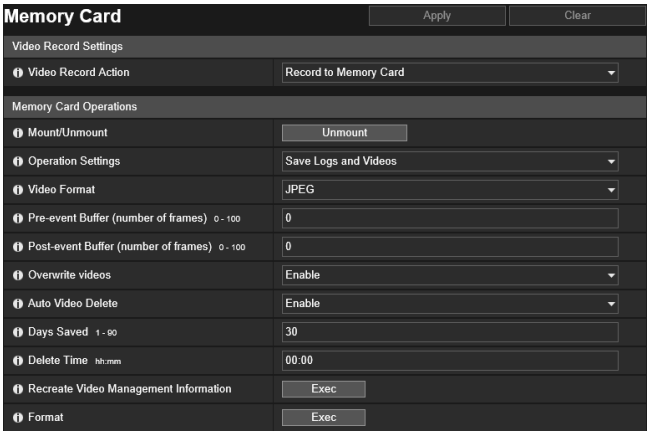
[SA AH SPI (outbound)]
Enter the SA SPI value for outbound.
Set a desired value in the range of 256 to 4294967295.

[SA AH Authentication Key (inbound)]
Enter the SA authentication key for inbound.
If [HMAC_SHA1_96] or [HMAC_MD5_96] was selected in [SA AH Authentication Algorithm], set a 160-bit or 128-bit hexadecimal number, respectively.

[SA AH SPI (inbound)]
Enter the SA SPI value for inbound.
Set a desired value in the range of 256 to 4294967295.
Since this setting is used as an ID for identifying the SA, be careful not to specify an inbound SPI whose value is already used in another AH’s SPI.

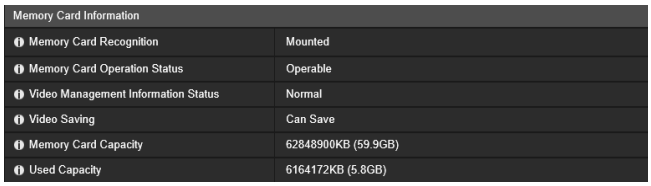
[Memory Card]
Memory Card Operations and Information Display

Settings for recording video to a memory card inserted in the camera. You can also see the status of the memory card. [Memory Card] is the same as [Video Record] > [Memory Card]. Settings configured on one [Memory Card] page are also reflected on the other.



The following settings can be configured here.

- Video Record Settings
- Memory Card Operations
- Memory Card Information



Important

Information recorded to the memory card may be regarded as “personal information”. Take sufficient precautions for handling this information when releasing the camera to third parties for disposal, transfer or repair.

Note

- Memory card videos can be viewed and managed using the Recorded Video Utility. For information on operating the Recorded Video Utility and its downloaded data, please refer to “Recorded Video Utility User Manual”.
- When a large number of files have been recorded onto a memory card, the Recorded Video Utility can take a considerable amount of time to process the video list (the greater the number of files, the longer it will take). Please reduce the number of days saved in [Auto Video Delete], or manually delete unneeded files with the Recorded Video Utility, on a regular basis.
  The number of files saved on the memory card can greatly be reduced, by using H.264 as the video format, instead of JPEG.
- The following memory cards can be used.
  – microSD memory card, microSDHC memory card, microSDXC memory card
- For inserting and removing the memory card, please refer to “Setup Guide”.
- If you are using the memory card in the camera for the first time, format the memory card after inserting it into the camera (P. 157).

Video Record Settings

Sets whether to record video from the camera to a memory card or upload it with HTTP or FTP.
These can also be set with [Video Record] > [Upload] (P. 110) and will be reflected in [Video Record Settings] here.

[Video Record Action]
Select [Record to Memory Card] to record to a memory card.

Memory Card Operations

The setting items will change depending on the memory card status (unmounted/mounted).

Important

Be sure to perform the unmount process when turning off the power to the camera or removing the memory card. Failing to unmount first may result in management file problems or the memory card becoming inaccessible.
You can use the Camera Management Tool to batch mount/unmount memory cards from multiple cameras.

The memory card will be automatically mounted when you insert it into the memory card slot. It will also be automatically mounted if it has been inserted in the memory card slot when the camera starts up.

[Mount/Unmount]
Click [Unmount] to unmount the memory card.
Be sure to unmount the memory card when turning off the power to the camera or removing the memory card.
Also click [Mount] with the memory card inserted to mount the memory card.

[Operation Settings]
Select the data to save to the memory card.
When [Save Logs and Videos] has been set, the following data is saved automatically.

- Video files when HTTP or FTP upload failed
- Video files manually recorded by the user from the Camera Viewer
- Video files recorded by [External Device Input] and [Intelligent Function] when an event occurs
- Video files recorded using a timer
- Log
- Video recorded with ONVIF

Note

New files cannot be saved to the memory card if there is no free space. When [Overwrite videos] is set to [Enable], old video can be deleted to save new video (P. 156).

[Video Format]
Select the video format to record to a memory card.
Video size and quality of the recorded video follow the settings in [Video] (P. 77).

Important

- For [H.264(1)] or [H.264(2)], the following settings must be configured in [Basic] > [Video] > [H.264(1)] (P. 78), [H.264(2)] (P. 78).
  - [Bit Rate Control]: [Use bit rate control (constant bit rate)]
  - [Target Bit Rate (kbps)]: [3072] or less
  - [I Frame Interval (sec)]: [0.5], [1] or [1.5]
- You cannot select a different H.264 format from that in [Video Record] > [Upload] > [General Upload] > [Video Format] (P. 110).

Note

When set to [JPEG] and an upload error occurs, the frame rate of video recorded in JPEG format is always 1 fps.

[Pre-event Buffer (number of frames)] (JPEG)/ [Pre-event Buffer (sec)] (H.264)
Enter the number of frames or seconds of video to be buffered before the event.
Enter the maximum number of frames for [JPEG] or the maximum number of seconds for [H.264(1)] or [H.264(2)] in [Video Format].
Depending on conditions, however, saving the set number of frames or seconds may not be possible.

[Post-event Buffer (number of frames)] (JPEG)/ [Post-event Buffer (sec)] (H.264)
Enter the number of frames or seconds of video to be buffered after the event.
Enter the maximum number of frames for [JPEG] or the maximum number of seconds for [H.264(1)] or [H.264(2)] in [Video Format].
Depending on conditions, however, saving the set number of frames or seconds may not be possible.

[Overwrite videos]
Select whether to allow overwriting data when the available space on the memory card becomes too low while recording video to a memory card due to an event being triggered.
If you select [Enable], videos recorded due to an event, timer or ONVIF will be overwritten starting from the oldest file.
If you select [Disable], use the Recorded Video Utility to delete unnecessary videos. For information on the procedure, please refer to “Recorded Video Utility User Manual.”

[Auto Video Delete]
Select to automatically delete video from the memory card that has exceeded the [Days Saved] setting.

If you select [Enable], set [Days Saved] and [Delete Time].

[Days Saved]
Enter the number of days for which video recorded to the memory card should be saved.

[Delete Time]
Enter the time to delete video that has exceeded the [Days Saved] setting.

[Recreate Video Management Information]
If you click [Exec], the management information file for recorded video will be recreated on the memory card.
The memory card cannot be accessed during this process. It is also recommended that users not upload or stream video from the camera.
When recreating video management information files, the more files you recreate, the longer the process will take; it may require several hours.

[Format]
Click [Exec] to format the memory card.
Formatting erases all files and directories on the memory card.

Note

Formatting is performed using a quick format.

Memory Card Information

Displays the status of the memory card inserted in the camera and information about card capacity.

[Memory Card Recognition]
Displays the current status of the memory card.

[Memory Card Operation Status]
Displays the operation status of the memory card.
[Operable]: All operations are possible.
[Recreating video management information]: This status indicates that video management information is being recreated. Other operations cannot be performed.
[Deleting videos]: This status indicates that videos are being deleted. Other operations cannot be performed.

[Video Management Information Status]
Displays the status of the video management information.
[Normal]: This status indicates that video management information is normal.
[Video Management Information Recreation Required]: This status indicates that management files are corrupted or not consistent with saved video files.
It is necessary to click [Exec] in [Recreate Video Management Information] to recreate the management file.
If the management files are not recreated even when [Recreate Video Management Information] is used, [Format] (P. 157) must be used.

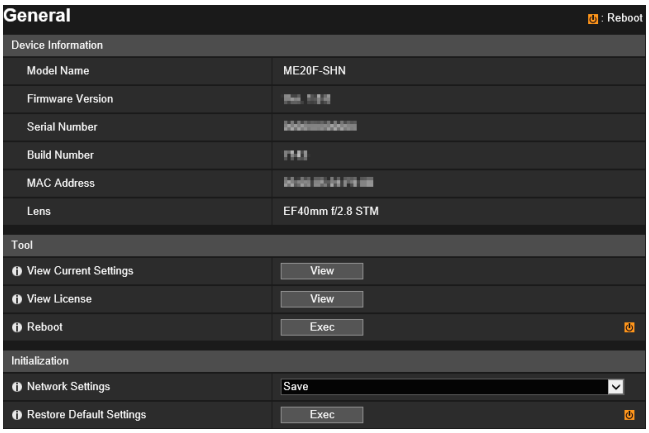
[Video Saving]
Displays whether videos can be saved to the memory card.
[Cannot Save] may occur for the following reasons.
- Memory card is not mounted.
- The video management file is corrupted.
- The card is write-protected.
- The memory card is full and [Overwrite videos] is set to [Disable].

[Memory Card Capacity]
Displays the current capacity of the memory card.

[Used Capacity]
Displays the current used capacity of the memory card.

[Maintenance] > [General]
Displaying Camera Device Information and Perform Maintenance

Check camera information, such as the firmware version, and perform maintenance on the camera system.



The following settings can be configured here.
- Device Information
- Tool
- Initialization

Device Information

[Model Name], [Firmware Version], [Serial Number], [Build Number], [MAC Address], and [Lens]
Displays information about the camera.

Note

The firmware version displayed here is of the network camera. Note that it is different from the firmware version of the imaging unit displayed on the external monitor connected using the 3G/HD-SDI terminal or HDMI OUT terminal.

Tool

You can configure/reboot the camera and display licenses.

[View Current Settings]
Display a list of current settings for the Setting Page.

[View License]
Display information on the third-party software licenses.

[Reboot]
Reboot the camera.

Initialization

Initialize the camera.

Caution
• You must not turn off the camera while [Restore Default Settings] is in operation. Turning off the camera at this stage may result in disabling its ability to boot correctly. • Once [OK] is clicked, you can no longer stop the process of restoring the default settings.

[Network Settings]
If you set this to [Save], the following settings are retained when initializing.
- Administrator Name

- Administrator Password
- Network Settings
- NTP Server
- HTTP Server
- Host Access Restrictions
- Time Zone
- Certificates
- Private Key
- IPsec

If you set this to [Do not save], the above settings are also initialized.
Since the administrator account is also initialized, you will become unable to connect to the camera. Use the Camera Management Tool to configure the initial settings.

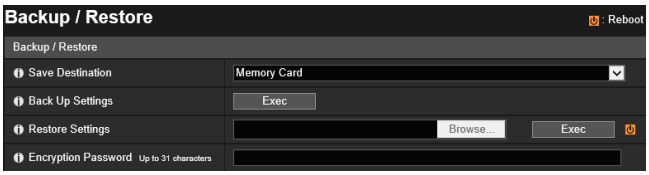
[Restore Default Settings]
The initial settings are restored according to the selection in [Network Settings] after rebooting.

Note

- It is recommended that you back up each current setting before you click [Exec] in [Restore Default Settings].
- The camera can also be restored to factory default settings using the reset switch. Note, however, that this will reset all camera settings to factory default settings except for date and time (P. 185).

[Maintenance] > [Backup / Restore]
Saving/Restoring Camera Settings

You can save/restore all the camera settings.



The following settings can be configured here.
- Backup / Restore

Backup / Restore

Configure the settings regarding backup and restoring.

Caution
You must not turn off the camera while [Back Up Settings] or [Restore Settings] are in operation. Turning off the camera at this stage may result in disabling its ability to boot correctly.

[Save Destination]
Select the destination for saving the camera settings when backing up.

[Back Up Settings]
All settings, except date and time, will be backed up. The administrator account, certificates used by SSL/TLS and 802.1X and private key will also be backed up.

[Restore Settings]
Restores all settings, except date and time, from the backup file created with [Back Up Settings].
If [PC] is selected in [Save Destination], click [Browse] to specify the backup file.
The administrator account, IP address, certificates used by SSL/TLS and 802.1X and private key will also be restored.
After restore is completed, the camera will be rebooted.

Important

- Take care when restoring from the backup file of another camera, as problems such as not being able to connect to the camera may occur due to the network address conflicting or the administrator password being overwritten.
- When restoring the settings, do not use a backup file created with a firmware version newer than that of the camera to restore.

[Encryption Password]
Set the password to use when backing up and restoring. This is the password for encrypting the backup data itself.
When restoring from encrypted backup data, enter the password set when backing up.

Note

The settings are not restored if the password set when backing up and the password set when restoring do not match.

[Maintenance] > [Update Firmware]
Updating the Camera Firmware

You can update the firmware.

The following settings can be configured here.
- Device Information
- Update Firmware

Device Information

[Model Name] and [Firmware Version]
Displays the information about the connected camera.

Update Firmware

Configure the settings related to firmware updates.

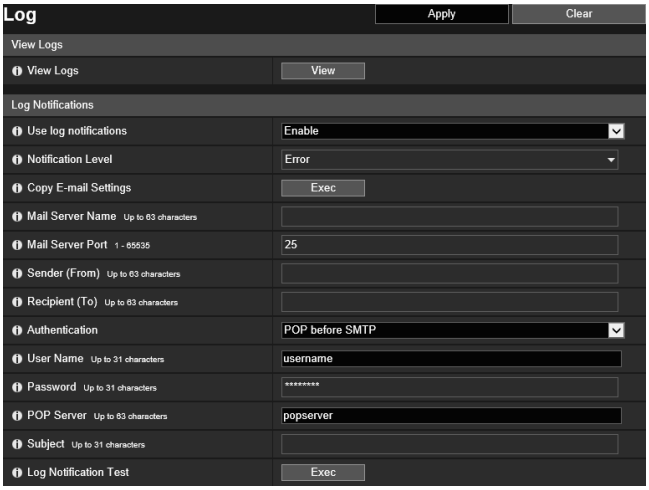
Caution
You must not turn off the camera while it is performing the [Update Firmware] operation. Turning off the camera at this stage may result in disabling its ability to boot correctly.

[Restore Default Settings]
The initial settings are restored when the firmware is updated.
If you set this to [Restore], the following settings are retained when initializing.
- Administrator Name
- Administrator Password
- Network Settings
- NTP Server
- HTTP Server
- Host Access Restrictions
- Time Zone
- Certificates
- Private Key
- IPsec

[Update Firmware]
Click [Browse], specify a firmware file for update, and click [Exec]. When the confirmation message is displayed, click [OK] to start the firmware update.
The camera is rebooted after the firmware is updated.

[Maintenance] > [Log]
Checking/Sending Camera Log Information

You can check the camera operations and connection history, and set log message e-mail transmission.



The following settings can be configured here.
- View Logs
- Log Notifications

View Logs

Display a history of camera operations and connections.

[View Logs]
If you click [View], the log messages saved since the camera was started are displayed.
For details on log messages, please refer to “List of Log Messages” (P. 170).

Log Notifications

Set the mail server and e-mail address to use for log notification.

[Use log notifications]
If you select [Enable], the following setting items for log notification are displayed.

[Notification Level]
Select the log notification level.
For details on levels of log messages, please refer to “Log Messages on the Camera” (P. 170).

[Copy E-mail Settings]
Copies the e-mail settings used in [Video Record] > [E-mail Notification] (P. 114). However, [Password] is not copied.

[Mail Server Name]
Enter the host name or IP address of the SMTP server.

[Mail Server Port]
Enter the port number for the SMTP server (factory default setting is [25]).

[Sender (From)]
Enter the e-mail address of the sender.

[Recipient (To)]
Enter the e-mail address of the recipient.

[Authentication]
Select an authentication method suited to the destination SMTP server.

[User Name], [Password], [POP Server]
Enter the user name and password needed for authentication, and the POP server host name or IP address when e-mail authentication is set to [POP before SMTP].
Enter the user name and password needed for authentication when e-mail authentication is set to [SMTP-AUTH].

[Subject]
Enter the subject of the e-mail in alphanumeric characters.

[Log Notification Test]
Clicking [Exec] initiates an e-mail notification test based on the settings currently entered.
If something other than [None] is selected for [Authentication], click [Exec] before clicking [Apply] after entering the [Password].

Appendix

This chapter provides supplementary information on camera functions, and explains the measures to take when trouble occurs or a message is displayed during camera use. It also explains how to reset the camera to the factory default setting state.

Modifiers

According to the setting item, you can specify parameters using modifier “% characters”.

Modifiers	Meaning	Description of character string entered
%n	Reason for capture (number)	0 (test) |1 (External device input) | 33 (Timer 1) | 34 (Timer 2) | 35 (Timer 3) | 36 (Timer 4) | 161 (Intelligent Function Detection Setting 1) | 162 (Intelligent Function Detection Setting 2) | 163 (Intelligent Function Detection Setting 3) | 164 (Intelligent Function Detection Setting 4) | 165 (Intelligent Function Detection Setting 5) | 166 (Intelligent Function Detection Setting 6) | 167 (Intelligent Function Detection Setting 7) | 168 (Intelligent Function Detection Setting 8) | 169 (Intelligent Function Detection Setting 9) | 170 (Intelligent Function Detection Setting 10) | 171 (Intelligent Function Detection Setting 11) | 172 (Intelligent Function Detection Setting 12) | 173 (Intelligent Function Detection Setting 13) | 174 (Intelligent Function Detection Setting 14) | 175 (Intelligent Function Detection Setting 15) |
%N	Reason for capture (character string)	<External input device name (alphanumeric characters) > | Intelligent Function Detection Setting name (alphanumeric characters) | NULL (blank entry or interval timer test)
%O	Reason for capture (ON/OFF)	OFF | ON
%X	Width of image	Number of pixels in horizontal direction
%Y	Height of image	Number of pixels in vertical direction
%C	Camera number	1
%D	Camera Name	Setting for [Camera Name (alphanumeric characters)]
%P	Pan position	0
%T	Tilt position	0
%Z	Zoom position	0
%R	Rotation position	0
%V	Camera server	ME20F-SHN
%y	Year of capture time	2001 – 2031
%m	Month of capture time	01 – 12
%d	Day of capture time	01 – 31
%w	Day of week of capture time	0 – 6 (Sunday to Saturday)
%H	Hours of capture time	00 – 23
%M	Minutes of capture time	00 – 59
%S	Seconds of capture time	00 – 59
%s	Milliseconds of capture time	000 – 999
%z	Time zone of capture time	-1200 – +1300
%a	Weekday name of capture time	Sun | Mon | Tue | Wed | Thu | Fri | Sat
%b	Month name of capture time	Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec
%h	Host Name	

Note

- A runtime error will occur if the specified name does not match.
- If this modifier is not defined, “%” will be deleted.

Available Modifiers

The modifiers that can be used for each setting item are specified below.

[HTTP Upload] (P. 111)
[Parameter (query string)]
All modifiers can be used.

[FTP Upload] (P. 112)
[Subdirectory Name to Create]
Only the modifiers %y, %m, %d, %w, %H, %h, %n can be used.

[File Name to Create]
Only the modifiers %y, %m, %d, %w, %H, %M, %S, %s, %n can be used.

[E-mail Notification] (P. 114)
[Message Body]
All modifiers can be used.

Troubleshooting

Before contacting the dealer from whom you purchased the product or Canon Customer Service Center, check the following items. If a log message is displayed, check the details of the message and the corresponding countermeasures in the log message list.

Note

- For information on troubleshooting for the Camera Management Tool, Recorded Video Utility, and Mobile Camera Viewer, please refer to each individual manual.
- A problem caused by the security software may occur. Configure to exclude the camera, or the software where the problem occurred, in your security software.

Problem	Countermeasures
The camera does not launch.	• If you are using a PoE+ hub, check if the LAN cable is connected correctly. • Turn the camera off and on again (please refer to “Setup Guide”). • Depending on the PoE+ hub, the power consumption per port or the total power consumption of each port may be limited. Please check the user manual of your PoE+ hub because it may not start if the limit is exceeded.
Cannot connect to the camera.	• Check if the LAN cable is connected correctly. • Check if the network to which the camera is connected is set up correctly. In particular, check if the IP address, subnet mask and default gateway address are set within the ranges supported by the applicable network. • If you have changed the IP address, the new address will not become effective until the camera is rebooted. • Check if the correct URI (camera IP address) is entered in your web browser. • Check whether the connection is from a computer whose access is blocked in [Security] > [Host Access Restrictions] (P. 144) on the Setting Page. • Ask your system administrator whether the authentication method set in [Security] > [802.1X] (P. 149) on the Setting Page and the combination of [User Name], [Password] and certificates match the rules of the network to connect to. • Configure to exclude the camera, or the software where the problem occurred, in your security software.
The Camera Viewer will not launch.	• If the message “Your web browser is not supported.” is displayed, use Internet Explorer 9 or greater, or a version of Chrome that is guaranteed to operate. • If the message “JavaScript is not available or disabled on your web browser.” is displayed, click [Network and Internet] > [Internet Options] > [Security] > [Custom level] in [Control Panel], and set [Active scripting] to [Enable]. • To enable authorized users and guest users to use the Camera Viewer, specify the following settings on the Setting Page. – Assign [Camera Control] or [Video Distribution] to authorized users/guest users in [Basic] > [User Management] > [User Authority]. – Set [Basic] > [Viewer] > [General] > [Default Page] to [Display Viewer]. – To also enable guest users to use the Camera Viewer, set [Basic] > [Viewer] > [Viewer Settings] > [User Authentication] to [Do not authenticate]. • Use one of the following procedures, when you launch the Camera Viewer and a file block security warning is displayed because of an unverified publisher. – Launch the Camera Viewer after executing Windows Update to the latest version, when using the camera in an internet connection environment. – Download the root certificate installer from the Canon download site on a connectable computer and install it in the target environment, when in an environment not connectable to the internet.
Cannot use some functions of the Camera Viewer.	• Follow the procedure in “Adding the Camera IP Address as a Trusted Site” (P. 24) to add this website to [Trusted sites] in the [Security] settings, and disable the protected mode for the trusted sites (when not using Windows Server, also disable the protected mode in a similar manner). • If you are using a web browser other than Internet Explorer or if the Canon Network Camera Addon Module is not correctly installed when using Internet Explorer, the following functions cannot be used. – Receiving audio – Receiving/playing H.264 video

Problem	Countermeasures
Video is not displayed.	• The number of Viewers that can access the camera at the same time is restricted by the setting in [Maximum Number of Clients] in [Server] > [Video Server] (a maximum of 30 can be specified). If this restriction is exceeded, a message is shown and video is not displayed. • Video can only be displayed by authorized users and guest users if [Video Distribution] privileges are assigned. Ask your administrator to assign [Video Distribution] privileges in [Basic] > [User Management] > [User Authority]. • Check if [System Frequency], [System Frame Rate], and [System Resolution] are set up correctly in [System Settings] on the Setting Page (P. 80). • If the Viewer is opened with Internet Explorer 10 or 11 on a 64-bit operating system, H.264 video may not be able to be received or played if the camera is added to the list of trusted sites and the enhanced protected mode is enabled. In this case, add the camera to the list of trusted sites and disable the protected mode of trusted sites. • Configure to exclude the camera, or the software where the problem occurred, in your security software.
There is no audio.	• If there is no audio, check the settings in [Video and Audio] > [Audio] or in [Server] > [Audio Server] on the Setting Page as well as the sound and audio device settings for the computer. • Audio can only be used by authorized users and guest users if [Audio Distribution] privileges are assigned. Ask your administrator to assign [Audio Distribution] privileges in [Basic] > [User Management] > [User Authority]. • If the Viewer is opened with Internet Explorer 10 or 11 on a 64-bit operating system, the audio may not be able to be received or transmitted if the enhanced protected mode is enabled. In this case, add the camera to the list of trusted sites and disable the protected mode of trusted sites. • Configure to exclude the camera, or the software where the problem occurred, in your security software.
The camera cannot be controlled.	• If you connect the Camera Viewer as an administrator, you will have exclusive possession of the camera control privileges. If you connect to the Viewer as an authorized user or guest user, you cannot control the camera unless the administrator releases camera control. Consult the administrator (P. 33).
The viewer gets disconnected.	• Check the network and computer for abnormality. • Reboot the computer and connect again. • Configure to exclude the camera, or the software where the problem occurred, in your security software.
You forgot the administrator password.	• You can initialize all settings of the camera excluding date and time using the reset switch (P. 185). After performing initialization, use the Camera Management Tool to register the administrator account again. The IP address and subnet mask, etc. also need to be set again because the network settings are initialized.
Data cannot be uploaded.	• Check that the upload destination of [Video Record] > [Upload] and the upload operation upon an event of the [Event] menu are both set correctly. • The settings for an upload destination that has been applied can be checked by executing a server upload test in [Video Record] > [Upload] on the Setting Page (P. 110). • Check [Maintenance] > [Log] > [View Logs] > [View Logs] or logs on the server to check the detailed operating environment. For details on [View Logs], please refer to “Uploader error” (P. 174), “Uploader warning” (P. 177), or “Uploader notification” (P. 181) of “List of Log Messages”. Also please refer to “Important” on P. 110. • For the server settings, contact your system administrator.
Video cannot be recorded on a memory card.	• Check [Memory Card] > [Memory Card Information] on the Setting Page (P. 157). • Video cannot be recorded if the memory card has insufficient space and [Memory Card] > [Memory Card Operations] > [Overwrite videos] is set to [Disable] on the Setting Page (P. 156). Set [Overwrite videos] to [Enable] or use the Recorded Video Utility to delete unnecessary videos. • To record video to a memory card when an event occurs, check the [Video Record Action] settings under [Memory Card] > [Video Record Settings] on the Setting Page. When [Video Record Action] is set to [Upload], change it to [Record to Memory Card]. • When video for which the HTTP/FTP upload failed is not stored on the memory card, check [Operation Settings] under [Memory Card] > [Memory Card Operations] on the Setting Page. When [Operation Settings] is set to [Save Log], change it to [Save Logs and Videos]. • To manually save recordings to a memory card, obtain camera control privileges.
Files cannot be saved.	• Windows prohibits saving to certain folders. Accordingly, an attempt to save a file may fail. Specify [Documents], [Pictures] and other folders.

List of Log Messages

Log Messages on the Camera

The list of log messages displayed in [View Logs] in [Maintenance] > [Log] > [View Logs] on the Setting Page (P. 162).
Log messages are classified into the following types.

Category	Level	Code	Fault level
crit	Error	4xx	Software-level failure (Task operations will stop)
err	Error	3xx	Operational error (Operations will continue)
warning	Warning	2xx	Non-operational error
notice	Warning	1xx	Error external to the system
info	Information	0xx	Information on normal operation

Note

If no content is recorded in a log for approximately two hours, "-- MARK --" will be recorded in the message area.

Error Log

System Error

S302 Error on saving settings [err]

Description	Can't update system settings (S302)
Meaning	An error generated while the system was saving a setting. Setting could not be saved.
Countermeasure	Provide enough memory space by deleting unnecessary files in the user memory area, etc.

S303 Error on saving settings [err]

Description	Can't update files of system settings (S303)
Meaning	An error generated while the system was saving a setting. Setting could not be saved.
Countermeasure	Provide enough memory space by deleting unnecessary files in the user memory area, etc.

S307 Error on saving settings [err]

Description	(vbadmin.c XXX) Can't update system settings (S307)
Meaning	An error generated while the settings were saved by the setup protocol. Setting could not be saved.
Countermeasure	Provide enough memory space by deleting unnecessary files in the user memory area, etc.

S310 Working error in event service [err]

Description	cannot work event [%1][%2][%3] (S310)
%1	Error number
%2	Cause of error
%3	Error information
Meaning	An error occurred while the event service was running.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S311 Working error in external input/output service [err]

Description	cannot work extio [%1][%2][%3] (S311)
%1	Error number
%2	Cause of error
%3	Error information
Meaning	An error occurred while the external input/output device service was running.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S312 Working error in timer service [err]

Description	cannot work timer [%1][%2][%3] (S312)
%1	Error number
%2	Cause of error
%3	Error information
Meaning	An internal error occurred in the timer service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S320 PAN/TILT operation error [err]

Description	%1 error occurred. [%2] (S320)
%1	PAN | TILT
%2	Warning details
Meaning	An error occurred during operation or stopping of PAN/TILT.
Countermeasure	Check that the camera is not touching the dome, etc. If the error is not caused by problems such as contact with peripheral items, the camera is faulty. Arrange for servicing.

S330 Failure of the fan [err]

Description	fan [%1] is stopped. (S330)
%1	Fan number
Meaning	The fan does not rotate or is detected that the rotation speed has been considerably lowered.
Countermeasure	If the problem persists after rebooting, the fan may be faulty. Arrange for servicing.

S340 Temperature warning [err]

Description	The camera's internal temperature has risen to a predetermined level. (S340)
Meaning	The camera's internal temperature is unnecessarily high.
Countermeasure	Turn off the camera and wait until the temperature has decreased. If the problem persists, arrange for servicing.

S341 Cooling fan warning [err]

Description	The cooling fan may not be working properly. (S341)
Meaning	The cooling fan may be faulty.
Countermeasure	Arrange for servicing.

S342 Lens communication error [err]

Description	There was a communication error between the camera and the lens. (S342)
Meaning	Unable to communicate with the lens normally.
Countermeasure	Reboot the camera. Alternatively, turn off the camera, remove the lens, and clean the lens's contact. If the problem persists, arrange for servicing.

S343 ABB error [err]

Description	An error occurred while the camera was automatically adjusting the black balance. (S343)
Meaning	The automatic black balance (ABB) may not have functioned correctly.
Countermeasure	Firmly attach the body cap to block light from entering the camera, and then perform the ABB operation again (refer to "Setup Guide" for details of operating procedure). If the problem persists, arrange for servicing.

S410 Event service initialization error [crit]

Description	event initialization error [%1][%2] (S410)
%1	Error number
%2	Cause of error
Meaning	An error occurred in the initialization of the event service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S411 External input/output service initialization error [crit]

Description	extio initialization error [%1][%2] (S411)
%1	Error number
%2	Cause of error
Meaning	An error occurred in the initialization of the external input/output device service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S412 Timer service initialization error [crit]

Description	timer initialization error [%1][%2] (S412)
%1	Error number
%2	Cause of error
Meaning	An error occurred in the initialization of the timer service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S413 Timer service runtime error [crit]

Description	timer working error [%1] (S413)
%1	Error number
Meaning	An error occurred while the timer service was running.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S414 Serial communication service initialization error [crit]

Description	seriald initialization error [%1] (S414)
%1	Error number
Meaning	An error occurred in the initialization of the serial communication service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

S420 External IO controller has failed [crit]

Description	external io controller is broken.(S420)
Meaning	The external IO controller has failed.
Countermeasure	The external IO controller firmware must be updated. If the problem persists after updating the firmware, the camera is faulty. Arrange for servicing.

S430 Failure of the temperature sensor [crit]

Description	cannot get temperature (S430)
Meaning	Unable to obtain the temperature from the temperature sensor.
Countermeasure	If the problem persists after rebooting, the board may be faulty. Arrange for servicing.

Audio server error

B301 Audio device error [err]

Description	cannot use audio device for %1[%2:%3] (B301)
%1	Send/Receive type (rx | tx)
%2	Error type (open | write | flush)
%3	Error number
Meaning	Detected an error in the audio device
Countermeasure	If the problem persists, please arrange for servicing.

B402 Audio server initialization failed [err]

Description	wvaudio initialization error [%1] (B402)
%1	Error number
Meaning	The audio server could not be initialized. The audio server stops.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

B403 Settings change failed [err]

Description	cannot set config [%1:%2] (B403)
%1	Error notification number
%2	Error number
Meaning	The settings could not be updated. The audio server stops.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

Video error

V300 Video input error [err]

Description	video %1 warning - %2 (V300)
%1	Video number
%2	Error number
Meaning	An error in the video input was detected that may adversely affect the operation of the camera.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V320 Internal error in intelligent service [err]

Description	cannot work intelligent [%1][%2][%3]. (V320)
%1	Error number
%2	Cause of error
%3	Error information
Meaning	An internal error occurred in intelligent service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V321 Pseudo mode setting error in intelligent service [err]

Description	pseudo mode setting fail. (V321)
Meaning	An error occurred in the pseudo mode setting of intelligent service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V400 Video input initialization error [crit]

Description	video %1 initialization failure - %2(%3) (V400)
%1	Video number
%2	Process description
%3	Error details
Meaning	The video input function was stopped because the video input system could not be initialized.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V401 Video input command error [crit]

Description	video %1 command error - %2(%3) (V401)
%1	Video number
%2	Process description
%3	Error details
Meaning	The video input function was stopped because a video input command could not be processed.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V402 Video input frozen [crit]

Description	video %1 stalled (V402)
%1	Video number
Meaning	The video input function was stopped because video generation stopped.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V403 Video input error [crit]

Description	video %1 fatal error - %2 (V403)
%1	Video number
%2	Error number
Meaning	The video input function was stopped because an error that does not permit recovery of the video input system was detected.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V420 Could not start intelligent service [crit]

Description	intelligent initialization error [%1][%2]. (V420)
%1	Error number
%2	Cause of error
Meaning	Failed to initialize intelligent service.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

V421 Intelligent service error [crit]

Description	intelligent working error [%1][%2]. (V421)
%1	Error number
%2	Cause of error
Meaning	An error that does not permit recovery occurred while intelligent service was running.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

Uploader error

A470 Uploader initialization failed [crit]

Description	uploader initialization failure - %1 (A470)
%1	Error number
Meaning	The uploader could not be initialized.
Countermeasure	If the problem persists after rebooting, the camera is faulty. Arrange for servicing.

Memory card error

M301 Memory card control module error [err]

Description	%1 process failure (M301)
%1	mount or unmount
Meaning	Mount or unmount process failed.

M302 Cannot remove invalid file [err]

Description	Invalid file (%1) can not remove. (M302)
%1	Name of removed file
Meaning	The invalid file could not be removed.

M303 Cannot process directory [err]

Description	Can not open directory(%1)(M303)
%1	Directory name
Meaning	Could not open directory to be processed.

M304 Failed to recreate management information [err]

Description	Fail updating management file(%1)(M304)
%1	Management information identification number
Meaning	Process to recreate management information failed.

M305 Error when writing a video file [err]

Description	write error %1 (%2) (M305)
%1	Video file path
%2	Reason for error
Meaning	An error occurred when writing a video file.

M400 Failed to initialize a memory card [crit]

Description	Fail SD card initialization(%1).(M400)
%1	Card initialization NG (det), power supplies control NG (proc)
Meaning	Process to initialize a memory card failed.

ONVIF error (RTP)

R301 Distribution communication error [err]

Description	message queue open error. %1 (R301)
%1	Modules that generate errors RTP_CTRL_QUEUE RTP_DATA_QUEUE VIDEO_CTRL_QUEUE VIDEO_DATA_QUEUE AUDIO_CTRL_QUEUE AUDIO_DATA_QUEUE EVENT_CTRL_QUEUE RECVQ_META SENDQ_MEDIA
Meaning	A communication error occurred between modules.
Countermeasure	If the problem persists after repeated attempts and rebooting, the camera may be faulty. Arrange for servicing.

R302 Parameter acquisition failure [err]

Description	cannot get parameter: %1 (R302)
%1	user_account: User account IP_address: IP address of the camera profile_media_configuration: MediaConfiguration information RTSP_port_number: RTSP port number
Meaning	Parameter acquisition has failed.

R303 Metadata distribution initialization failure [err]

Description	metadata initialization error (R303)
Meaning	Metadata distribution initialization has failed.

R304 Abnormal termination of client [err]

Description	delete session from some kind of error: client_IP=%1, session_ID=%2 (R304)
%1	Client IP address
%2	Session ID
Meaning	The client session terminated abnormally.

R304 Client disconnected [err]

Description	connection reset by peer: client_IP=%1 (R304)
%1	Client IP address
Meaning	Disconnected from client.

R304 Client disconnected [err]

Description	RTP/HTTP connection closed by client (R304)
Meaning	Disconnected from client.

R305 RTSP processing error [err]

Description	RTSP Error: error_code=500: Internal Server Error (R305)
Meaning	An RTSP processing error occurred.

Warning Log

■ System warning

S220 PAN/TILT operation warning [warning]

Description	%1 warning detected. [%2] (S220)
%1	PAN | TILT
%2	Warning details
Meaning	An error occurred during operation or stopping of PAN/TILT.
Countermeasure	Check that the camera is not touching the dome, etc.

S230 Fan rotation speed lowered [warning]

Description	fan [%1] speed is too slow. (S230)
%1	Fan number
Meaning	Detected that the rotation speed of the fan has been lowered
Countermeasure	Arrange for servicing if it frequently occurs.

■ HTTP server warning

H143 User name specification error [notice]

Description	(http_auth.c.XXX) get_password failed, IP:%1 (H143)
%1	IP address
Meaning	An unknown user was specified in user authentication. This log message may also be displayed during normal operations when using a web browser other than Internet Explorer.

H144 Password specification error [notice]

Description	(http_auth.c.XXX) password doesn't match for %1 username%2, IP:%3 (H144)
%1	URL XSS vulnerability countermeasure implementation (process equivalent to ftpd)
%2	User Name
%3	IP address
Meaning	A wrong password was specified in user authentication.

H201 Timeout disconnect [warning]

Description	a request for %1 timed out after writing %d seconds (H201)
%1	Request URI
%d	360 (Timeout time)
Meaning	Disconnected due to HTTP server timeout (360 sec.).

wvhttp warning

W101 Invalid user name [notice]

Description	user <User name> not found (W101)
Meaning	The camera was accessed by an unauthorized user.

W102 Invalid password [notice]

Description	user <User name> password mismatch (W102)
Meaning	The password is invalid.

W130 Buffer recovered [notice]

Description	stream buffer recovered (W130)
Meaning	Image buffer for stream recording has recovered.

W201 Invalid panorama image [warning]

Description	corrupt panorama image - ignored (W201)
Meaning	Panorama image information acquisition failed.

W230 Buffer overflow [warning]

Description	stream buffer overflowed (W230)
Meaning	The image buffer for the stream recording overflowed and images were discarded.

Audio server warning

B101 Received unusual request [notice]

Description	%1 unusual request[%2] (B101)
%1	Client host's IP address
%2	Unusual type (400 | 404)
Meaning	Refused due to command error (400) and parameter error (404).

B102 Client connection denied [notice]

Description	%1 request denied[%2] (B102)
%1	Client host IP address
%2	Denial type (41 | 43 | ...)
Meaning	Client connection was denied due to an authentication error (41), time specification error (42), insufficient resource (43), specification of unsupported codec (45), specification of unpermitted user level (47), too many clients (49) or invalid operation mode (4a).
Countermeasure	41: Check user name, password or user list used when connecting. 42: Check playtime or maximum connection time settings used when connecting. 43: Reconnect or restart. 45: Use supported client software. 47: Check user level used when connecting. 49: Check client number settings. 4a: Check if usage of audio server is enabled.

B103 Client forcibly disconnected [notice]

Description	%1 access denied[%2] (B103)
%1	Client host IP address
%2	Denial type (41 | 42 | 4a)
Meaning	Connection was initially permitted, but the setting has subsequently been changed to prohibit access, thereby triggering a forced disconnection (the denial type is the same with B102).

B201 Event notification failure [warning]

Description	cannot notify %1 event [%2] (B201)
%1	Event type (ald)
%2	Error number
Meaning	Failed to notify event.

B202 Event receive failure [warning]

Description	cannot recv event [%1] (B202)
%1	Error number
Meaning	Failed to receive event.

B203 Audio message send failure [warning]

Description	audio message send error %1 [%2] (B203)
%1	Message type
%2	Error number
Meaning	Failed to send audio message.

B204 Audio message receive error [warning]

Description	audio message recv error [%1:%2] (B204)
%1	Error number
%2	Reason for error
Meaning	Failed to receive audio message.

Camera application warning

C211 Camera control command overflow [warning]

Description	command queue overflowed (C211)
Meaning	The camera control command queue overflowed, and some commands were discarded.
Countermeasure	Allow a longer interval (200 ms) for sending the camera control command.

Video warning

V200 Video input warning [warning]

Description	video %1 warning - %2 (V200)
%1	Video number
%2	Error number
Meaning	An error that permits recovery of the video input system was detected.
Countermeasure	Change video size or video quality, or decrease data size for each JPEG image.

Uploader warning

A120 Resolution of upload destination name failed [notice]

Description	uploader cannot resolve the server name (A120)
Meaning	The name of the upload destination could not be resolved.

A121 Connection to upload destination failed [notice]

Description	uploader cannot connect to the server (A121)
Meaning	Execution of connect to upload destination failed.

A122 Connection to upload destination failed [notice]

Description	uploader cannot connect to the server (A122)
Meaning	The upload destination could not be connected due to a reason other than A120 and A121.

A134 Invalid upload setting (FTP/HTTP mode) [notice]

Description	ftp/http mode invalid. uploader set <none> forcibly (A134)
Meaning	The upload mode setting is invalid. The upload function was forcibly disabled.

A135 Invalid upload setting (FTP PORT/ PASV mode) [notice]

Description	ftp port/pasv mode invalid. uploader set <pasv> forcibly (A135)
Meaning	The PORT/PASV mode setting in connection with FTP upload is invalid. The PASV mode was forcibly set.

A136 Invalid upload setting (HTTP notification only/image mode) [notice]

Description	http notice/image mode invalid. uploader set <image> forcibly (A136)
Meaning	The notification only/image mode setting in connection with HTTP upload is invalid. The image mode was forcibly set.

A137 Invalid upload setting (E-mail notification) [notice]

Description	mode invalid. uploader set <none> forcibly (A137)
Meaning	The e-mail notification setting is invalid. Email notification was forcibly disabled.

A138 Invalid upload setting (E-mail notification authentication mode) [notice]

Description	authentication mode invalid. uploader set <smtp auth> forcibly (A138)
Meaning	The setting for e-mail notification authentication mode is invalid. “SMTP_AUTH” was forcibly set.

A274 Event buffer for upload overflowed [warning]

Description	event queue is full (A274)
Meaning	Event buffer for upload overflowed.
Countermeasure	Make adjustments to reduce the number of event occurrences.

A275 Image buffer for upload overflowed [warning]

Description	buffer queue is full (A275)
Meaning	Image buffer for upload overflowed.
Countermeasure	Make adjustments to reduce the number of event occurrences. Also adjust the video quality, video size and frame rate for upload.

Memory card warning

M201 Memory card is write-protected [warning]

Description	Readonly filesystem (M201)
Meaning	A write-protected memory card is inserted.

M203 Not enough space on memory card [warning]

Description	There is not available space (M203)
Meaning	Insufficient memory card capacity.

M204 Invalid file removed [warning]

Description	Invalid file (%1) was removed. (M204)
%1	Name of removed file
Meaning	An invalid file was removed.

M205 Checking management information file [warning]

Description	%1 checking management file (M205)
%1	Start | Finish
Meaning	The memory card may have been removed without being unmounted. Start/finish checking management information file.

M206 Invalid management information removed [warning]

Description	Invalid db information(%1)(%2) was removed(M206)
%1	Name of management information file containing invalid information
%2	ID of invalid information
Meaning	Invalid management information was removed.

M207 Memory card removed without unmounting [warning]

Description	Memory card was pulled before unmount. (M207)
Meaning	Memory card was removed when mounted.

ONVIF warning (RTP)

R101 RTP session timeout [notice]

Description	session timeout: session ID=%1 (R101)
%1	Session ID
Meaning	RTP session has timed out.

R102 Information acquisition failure (RTP payload size) [notice]

Description	cannot get parameter: RTP_payload_size (R102)
Meaning	Information acquisition has failed (RTP payload size).

R102 Information acquisition failure (IP address) [notice]

Description	cannot get parameter: IP_address (R102)
Meaning	Information acquisition has failed (IP address).

R103 RTSP authentication failure [notice]

Description	RTSP authorization error (R103)
Meaning	RTSP authentication has failed.

R107 RTSP connection failure [notice]

Description	RTSP Error: error_code=%d: Service Unavailable (R107)
%d	400: Value used for RTSP is invalid. 401: RTSP authentication failure or missing valid authentication information. 457: Playback time for RTSP is invalid. 501: An invalid RTSP option was used. 503: Failure to offer service, due to insufficient resources. The number of maximum RTP sessions, has passed the limit.
Meaning	RTSP connection has failed.

Notification Log

■ System notification

S001 System started [info]

Description	starting paramd (S001)
Meaning	Parameter management module started.

S002 System settings changed [info]

Description	Updated system settings. (S002)
Meaning	Settings not requiring rebooting were changed.

S010 Event service started [info]

Description	starting event (S010)
Meaning	The event service was started.

S011 Event service shut down [info]

Description	shutdown event (S011)
Meaning	The event service was shut down.

S012 External device service started [info]

Description	starting extio (S012)
Meaning	The external device input/output service was started.

S013 External device service shut down [info]

Description	shutdown extio (S013)
Meaning	The external device input/output service was shut down.

S014 Timer service started [info]

Description	starting timer (S014)
Meaning	The timer service was started.

S015 Timer service shut down [info]

Description	shutdown timer (S015)
Meaning	The timer service was shut down.

S017 qtimer service started or shut down [info]

Description	%1 qtimer (S017)
%1	Starting or stopping
Meaning	The qtimer service was started or shut down.

S019 bpc service started or shut down [info]

Description	%1 bpc (S019)
%1	Starting or stopping
Meaning	The bpc service was started or shut down.

S020 Serial communication service started or shut down [info]

Description	%1 seriald (S020)
%1	Starting or stopping
Meaning	The serial communication service was started or shut down.

S040 Lens attachment status [info]

Description	%1 the lens (S040)
%1	(attach) or (remove)

S041 Lens name [info]

Description	%1 (S041)
%1	Lens name

S070 Change to certificate [info]

Description	%1: succeeded to %2 certificate (S070)
%1	ssl or 802.1X
%2	generate | load | delete | restore
Meaning	A certificate was generated/loaded/ deleted/restored

wvhttp notification

W001 Starting and stopping of system [info]

Description	%1 webview (W001)
%1	Starting or stopping
Meaning	wvhttp server (webview) has started or stopped.

W030 Startup and shutdown of WebView Livescope Client [info]

Description	%1%2 host=<Host>, user=<User>, prio=<Priority>(W030)
%1	W: WebView session, V: Session-less video client, N: Session-less event client
%2	+: Connect, -: Disconnect
Meaning	The camera server client was connected or disconnected.

W031 Transmitted video data size [info]

Description	%1= host=<Host>, user=<User>, video=<jpg|h264>:<Number of frames> (W031)
%1	W: WebView session, V: Session-less video client
Meaning	When a client disconnected, the total data that was sent to the client is displayed in number of frames.

W040 Clearing to external memory [info]

Description	%1 the image storing - %2 (W040)
%1	Starting or stopping
%2	Reason for starting/stopping
Meaning	Started or stopped clearing stream recording to external memory.

Audio server notification

B001 Starting and stopping of audio server [info]

Description	%1 audio. (B001)
%1	starting | stopping
Meaning	The audio server was started/shut down.

B011 Audio client connected [info]

Description	[%1] %2 connected n=%3 (B011)
%1	Client type (send | recv)
%2	Client host IP address
%3	Total number of clients
Meaning	An audio client was connected.

B012 Audio client closed [info]

Description	[%1] %2 closed n=%3 (B012)
%1	Client type (send | recv)
%2	Client host IP address
%3	Total number of clients
Meaning	An audio client was disconnected.

Camera application notification

C001 Starting and stopping of camera control module [info]

Description	%1 camerad (C001)
%1	starting | stopping
Meaning	The camera control module started/ stopped.

C002 Camera application started and stopped [info]

Description	starting cameraappl (C002)
Meaning	The camera application started.

Video notification

V001 Starting and stopping of video server [info]

Description	%1 video (V001)
%1	Starting or stopping
Meaning	The video server was started/stopped.

V020 Starting intelligent service [info]

Description	starting intelligent. (V020)
Meaning	Intelligent service was started.

V021 Shutting down intelligence service [info]

Description	shutdown intelligent. (V021)
Meaning	Intelligent service was shut down.

Uploader notification

A004 Starting and stopping of uploader [info]

Description	%1 uploader (A004)
%1	Starting or stopping
Meaning	The uploader was started or stopped.

A040 Number of uploads (MAIL) [info]

Description	uploader mail: normal=%1 test=%2 (A040)
%1	Number of normal uploads.
%2	Number of test uploads.
Meaning	Shows the number of uploads executed.

A041 Number of uploads (FTP) [info]

Description	uploader ftp: normal=%1 test=%2 (A041)
%1	Number of normal uploads.
%2	Number of test uploads.
Meaning	Shows the number of uploads executed.

A042 Number of uploads (HTTP) [info]

Description	uploader http: normal=%1 test=%2 (A042)
%1	Number of normal uploads.
%2	Number of test uploads.
Meaning	Shows the number of uploads executed.

Memory card notification

M001 Starting and stopping of memory card control module [info]

Description	%1 sdctrl (M001)
%1	Starting or stopping
Meaning	The memory card control module (sdctrl) has started or stopped.

M002 Valid management information inserted [info]

Description	Valid db information (%1)(%2)(%3) was inserted (M002)
%1	Name of management information file with inserted valid information
%2	Directory number of valid information
%3	File number of valid information
Meaning	Added to management information as it appears to be a valid video file.

M003 Started/finished recreation of management information [info]

Description	%1 updating management file (%2)(M003)
%1	Start | Finish
%2	Management information identification number
Meaning	Process to recreate management information finished.

■ ONVIF notification (RTP)

R001 Startup of RTP distribution module [info]

Description	starting media_plane (R001)
Meaning	RTP distribution module started.

R002 Stopping of RTP distribution module [info]

Description	stopping media_plane (R002)
Meaning	RTP distribution module stopped.

R003 RTSP PLAY request received [info]

Description	PLAY received: client_IP=%1, profile=%2, num_of_sessions=%3(V=%4, A=%5, M=%6,BC=%7) (R003)
%1	Client IP address
%2	Profile name of requested PLAY
%3	Total number of client sessions
%4	Total distribution count of Video stream
%5	Total distribution count of Audio stream
%6	Total distribution count of Metadata stream
%7	Total distribution count of AudioBackChannel
Meaning	RTSP PLAY request was received.

R004 RTSP TEARDOWN request received [info]

Description	TEARDOWN received: client_IP=%1, profile=%2, num_of_sessions=%3(V=%4, A=%5, M=%6,BC=%7) (R004)
%1	Client IP address
%2	Profile name of requested TEARDOWN
%3	Total number of client sessions
%4	Total distribution count of Video stream
%5	Total distribution count of Audio stream
%6	Total distribution count of Metadata stream
%7	Total distribution count of AudioBackChannel
Meaning	RTSP TEARDOWN request was received.

R005 Starting multicast [info]

Description	start multicast: profile=%1, num_of_sessions=%2(V=%3, A=%4, M=%5,BC=%6) (R005)
%1	Client IP address
%2	Profile name of requested MulticastStreaming START
%3	Total distribution count of Video stream
%4	Total distribution count of Audio stream
%5	Total distribution count of Metadata stream
%6	Total distribution count of AudioBackChannel
Meaning	Multicast was started.

R006 Stopping multicast [info]

Description	stop multicast: profile=%1, num_of_sessions=%2(V=%3, A=%4, M=%5,BC=%6) (R006)
%1	Client IP address
%2	Profile name of requested MulticastStreaming STOP
%3	Total distribution count of Video stream
%4	Total distribution count of Audio stream
%5	Total distribution count of Metadata stream
%6	Total distribution count of AudioBackChannel
Meaning	Multicast was stopped.

List of Viewer Messages

Messages Shown in the Information Display

Messages shown in the information display of the Camera Viewer are classified into the following three types.

Icon	Category	Explanation
	Information Message	Displays help messages related to various buttons, pull-down lists, etc., as well as frame rate and other information.
	Warning Message	Displays a message urging caution to the user when camera control privileges cannot be obtained, the audio session stops, etc.
	Error Message	Displayed when a system error occurs in the viewer.

Warning Message

Message	Explanation
The camera is busy.	The connection limit was exceeded.
Failed to get camera control privileges.	The request for camera control privileges was denied because the camera was being used by the administrator, etc.
You are not connected to the camera.	An attempt was made to operate the camera when the camera was not connected.
Please get camera control privileges.	An attempt was made to operate the camera without camera control privileges.
Another user is already connected as an administrator.	The administrator is already connected to the camera.
No audio device.	The [Audio Reception] button was clicked while the computer audio device was unavailable or disabled.
Insufficient memory card capacity.	An attempt was made to manually record to a memory card with insufficient capacity.
Recording to memory card is not allowed.	Recording to the memory card failed because [Memory Card Operations] > [Operation Settings] was not set to [Save Logs and Videos].
You cannot control the camera unless you exit Digital PTZ and Viewer PTZ.	The video display area was clicked with the Digital PTZ or Viewer PTZ enabled.
Start Digital PTZ or Viewer PTZ.	You clicked the pan/tilt slider, zoom slider, or video display area with the Digital PTZ and Viewer PTZ disabled.
Waiting for control privileges.	A general user is waiting to obtain control.
Recreating video management information.	The video management information on the memory card is being recreated.
User authentication failed.	User authentication failed.
Failed to initialize the ActiveX plug-in.	When the ActiveX plug-in is not installed after starting the Camera Viewer, the Camera Viewer waits 10 seconds for the plug-in to be installed, but the plug-in was not installed after 10 seconds.
JavaScript is not available or disabled on your web browser.	JavaScript could not be used in the web browser.
Currently in the process of starting or ending audio transmission and receiving.	Attempted to start or stop audio transmission while already processing starting or stopping of audio transmission and reception.
You do not have video reception permission.	A user without video reception privileges tried to connect to the camera.

Message	Explanation
Audio reception is restricted.	You clicked the audio reception button when [Server] > [Audio Server] > [Audio Transmission from the Camera] was set to [Disable].
Your web browser is not supported.	You started the Camera Viewer with an unsupported web browser.
ActiveX is disabled.	ActiveX is disabled in the web browser settings or system functions cannot be accessed from ActiveX due to security settings. Even though ActiveX is enabled, if this message is displayed in the environment where the proxy server is used, select [Control Panel] > [Network and Internet] > [Internet options] > the [Connections] tab > [LAN settings] > the [Use a proxy server for your LAN] checkbox in [Proxy server] > select [Advanced] > specify the camera IP address in [Exceptions].
Cannot control focus. Please check the lens.	You tried to operate the focus (P. 47) when the camera was mounted with no lens or an incommunicable lens, or when the focus mode switch on the lens was set to MF (manual).
Cannot use One-shot AF because the shutter speed is too slow.	You clicked ONE SHOT when [Camera] > [Camera Settings] > [Camera Mode] was set to [Manual], [Tv], or [AGC], and also [Camera] > [Camera Settings] > [Shutter Speed] was set to [1/7] or slower.
Cannot display video because color bars are being output.	You started the Camera Viewer with color bars being output. Color bars began to be output while the camera was connected.
Cannot control ND Filter because Infrared is in use.	You tried to operate the ND filter (P. 49) when using the infrared mode.
Cannot control iris. Please check the lens.	You tried to operate the iris (P. 48) when the camera was mounted with no lens or an incommunicable lens, or when the iris switch on the lens was set to manual.
Camera was adjusted.	You performed a certain operation with the [Camera Operation] menu displayed, by which the change of an element in the [Camera Operation] menu should be triggered.
Cannot use One-shot AF because the lens does not support it.	You clicked ONE SHOT when ONE SHOT was unavailable because the camera was mounted with a lens which did not support the one-shot AF.

Restoring Factory Default Settings

If you have forgotten the settings and want to set the camera from the beginning, restore the factory default settings first. It is recommended that you use [Maintenance] > [Backup / Restore] on the Setting Page to create a backup file before restoring the factory default settings (P. 160).

Important

If you restore default settings, you will become unable to connect to the camera because the administrator account is also initialized. Use the Camera Management Tool to configure the initial settings.

Note

- Settings can also be backed up using the Camera Management Tool. For details on using the Camera Management Tool, please refer to "Camera Management Tool User Manual".
- For factory default settings, please refer to P. 186.

Restoring the Initial Settings from a Web Browser

Use [Maintenance] > [General] > [Initialization] > [Network Settings] > [Do not save] on the Setting Page (P. 158).

Restoring Factory Default Settings with the Reset Switch on the Camera

If you have forgotten or do not know the IP address of the camera or your Administrator password, you cannot operate the camera via the network. In this case, press the reset switch to reset the camera.
For information on how to initialize the camera using the reset switch on the camera, please refer to "Setup Guide".

List of Factory Default Settings

Item	Setting
• LAN	
LAN Interface	Auto
Maximum Packet Size	1500
• IPv4	
IPv4 Address Settings Method	Auto (DHCP)
IPv4 Address	192.168.100.1
Subnet Mask	255.255.255.0
IPv4 Default Gateway Address	
AutoIP	Enable
IPv4 Address (AutoIP)	
• IPv6	
IPv6	Enable
Auto (RA)	Enable
Auto (DHCPv6)	Enable
IPv6 Address (Manual)	
Prefix Length	64
IPv6 Default Gateway Address	
IPv6 Address (Auto)	
• DNS	
Name Server Address 1	
Name Server Address 2	
Set Name Server Address Automatically	Use DHCP/DHCPv6
Host Name	
Host Name Registration with DDNS	Do Not Register
Search Domain	
Search Domain List	
• mDNS	
Use mDNS	Enable
• Administrator Account	
Administrator Name	
Password	
• User Authority	
Authorized User Camera Control	Video distribution and Privileged Camera control
Guest User Camera Control	No access privileges
Authorized User Audio Distribution	Yes
Guest User Audio Distribution	No
• Current Date and Time	

Item	Setting
• Settings	
Settings Method	Set manually
Set NTP Server Settings Automatically	Disable
NTP Server	
Synchronization Interval (minutes)	5
Last Sync Time	
Time Zone	(GMT+09:00) Osaka, Sapporo, Tokyo
Daylight Saving Time	Disable
• JPEG	
Video Quality: 480 x 270	6
Video Quality: 960 x 540	6
Video Quality: 1920 x 1080	6
Video Quality: Digital PTZ	6
Video Size: video Transmission	1920 x 1080
Maximum Frame Rate: Video Transmission	15.0
Video Size: Upload / Memory card	480 x 270
• H.264(1)	
Video Size	1920 x 1080
Bit Rate Control	Use bit rate control (constant bit rate)
Target Bit Rate (kbps)	3072
Video Quality	6
Frame Rate (fps)	15
I Frame Interval (sec)	1
• H.264(2)	
H.264(2)	Disable
Video Size	480 x 270
Bit Rate Control	Use bit rate control (constant bit rate)
Target Bit Rate (kbps)	1024
Video Quality	6
Frame Rate (fps)	15
I Frame Interval (sec)	1
• General	
Default Page	Display Settings Page
• Viewer Settings	
User Authentication	Authenticate
H.264 for Guest Users	Disable

Item	Setting
• Camera Name	
Camera Name (alphanumeric characters)	ME20F-SHN
• System Settings	
System Frequency	59.94 Hz
System Frame Rate (59.94 Hz)	29.97P
System Resolution	1920 x 1080
Tele-converter	Disable
3G/HD-SDI Terminals	Enable
HDMI OUT Terminals	Enable
Buttons/Remote Controller	Enable
• Installation Conditions	
LED Setting	Turn On
Scan Reverse	Disable
Peripheral Illumination Correction	Disable
EF-S Lens	Disable
• Camera Position Control	
Camera Position without Control	Do not return to Home Position
• External Input Device	
Device Name (alphanumeric characters)	
• External Output Device	
Device Name (alphanumeric characters)	
• Camera Settings	
Camera Mode	Auto
AE Shift	0
AGC Limit	Off (75dB)
Auto Slow Shutter	On
Iris Increment	1/2 stop
AF Frame Position	Center
White Balance	Auto
White Balance Fine Adjustment	0
Color Temperature	5500
Infrared	Disable
ND Mode	Auto
Light Metering	Standard
Flicker Reduction	Disable
Custom Picture	Crisp Img
• Custom Picture	
Base Custom Picture	
Gamma	Normal 1
Master Pedestal	0

Item	Setting
Master Black Red	0
Master Black Blue	0
Black Gamma	0
Knee	On
Knee Slope	0
Knee Point	95
Sharpness	0
Noise Reduction	Off
R Gain	0
B Gain	0
• Register Preset	
Digital PTZ Position	Register
Camera Settings	Do Not Register
Preset Name	preset 1
Show in Viewers	Enable
• Specified Area	
Area 1 (Pink)	Disable
Area 2 (Purple)	Disable
Area 3 (Blue)	Disable
Area 4 (Cyan)	Disable
Area 5 (Green)	Disable
Area 6 (Yellow)	Disable
Area 7 (Orange)	Disable
Area 8 (White)	Disable
• ADSR	
Enable in H.264(1)	Disable
Enable in H.264(2)	Disable
Data Size Reduction Level	High
• On-screen display	
Date display	Disable
Position of date display	Upper left
Format of date display	YYYY/MM/DD
Time display	Disable
Position of time display	Upper left
Text display	Disable
Position of text display	Upper left
Text string display	
Common Settings	
Color of text	White
Background color	Black
Color depth of text and background	Fill text and background color

Item	Setting
• Mask area	
Area	Enable
• All privacy masks	
Color	Black
• General Audio	
MIC Power	Disable (dynamic microphone)
• HTTP Server	
Authentication Method	Digest Authentication
HTTP Port	80
HTTPS Port	443
• SNMP Server	
Use SNMP v1 and v2c	Disable
Use SNMP v3	Disable
Administrator Contact Information	
Administration Function Name	ME20F-SHN
Installation Location	
• SNMP v1 and v2c Server	
Community Name	
• SNMP v3 Server	
User Name	
Security Level	No authentication and no encryption
Authentication Algorithm	MD5
Encryption Algorithm	DES
• FTP Server	
Use FTP Server	Disable
User Name	
• WS-Security	
Check Time on Authentication	Check
• Video Server	
Maximum Number of Clients	30
Camera Control Queue Length	30
Maximum Connection Time (sec.)	0
Camera Control Time (sec.)	20
• Audio Server	
Audio Transmission from the Camera	Disable
Voice Activity Detection	Disable
• RTP Server	
RTP	Enable
RTSP Authentication Method	Digest Authentication
RTSP Port	554

Item	Setting
• Audio Multicast	
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
• RTP Stream 1	
Video Size	480 x 270 JPEG
Frame Rate	5
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
Audio Transmission	Disable
• RTP Stream 2	
Video Size	480 x 270 JPEG
Frame Rate	10
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
Audio Transmission	Disable
• RTP Stream 3	
Video Size	480 x 270 JPEG
Frame Rate	15
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
Audio Transmission	Disable
• RTP Stream 4	
Video Size	480 x 270 JPEG
Frame Rate	30
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
Audio Transmission	Disable
• RTP Stream 5	
Video Size	H.264(1)
Frame rate	5
Multicast Address	0.0.0.0
Multicast Port	0
Multicast TTL	1
Audio Transmission	Disable
• Video Record Settings	
Video Record Action	Record to Memory Card

Item	Setting
• General Upload	
Upload	Upload Disabled
Video Format	JPEG
Frame Rate	1
Pre-event Buffer (number of frames)	0
Post-event Buffer (number of frames)	0
Pre-event Buffer (sec)	0
Post-event Buffer (sec)	0
• HTTP Upload	
Notification	Notification Only with HTTP
URI	
User Name	
Proxy Server	
Proxy Port	80
Proxy User Name	
Parameter (query string)	
• FTP Upload	
Notification	Video data upload with FTP
FTP Server	
User Name	
PASV Mode	Enable
File Upload Path	
File Naming	YYYYMMDDHHMMSSms
Maximum Number of Loops	0
Subdirectory Name to Create	
File Name to Create	image.jpg
File Name to Create	video.mov
• E-mail Notification	
Notification	Text Only
Mail Server Name	
Mail Server Port	25
Sender (From)	
Recipient (To)	
Authentication	None
User Name	
POP Server	
Subject	
Message Body	

Item	Setting
• External Device Output	
Operation Mode	Normally Open
Active Output Format	Continuous
Pulse Output Time (sec)	1
• External Device Input	
External Device Input Event	Enable
Operation Mode	Normally Open
Active Event Operation	Disable
Inactive Event Operation	Disable
Ongoing Active Event Operation	Disable
Preset	None
Video Record	Disable
E-mail Notification	Disable
External Device Output for Active Event	Disable
External Device Output for Inactive Event	Disable
Infrared Switching	Disable
• Timer 1	
Timer Event	Disable
24-Hour Continuous Settings	Disable
Start Time	00:00
End Time	00:00
Repeat Interval	None
• Operation	
Start Time Preset	None
Video Record	Disable
E-mail Notification	Disable
External Device Output	Disable
Infrared Switching	Disable
• Timer 2	
Timer Event	Disable
24-Hour Continuous Settings	Disable
Start Time	00:00
End Time	00:00
Repeat Interval	None
• Operation	
Start Time Preset	None
Video Record	Disable
E-mail Notification	Disable
External Device Output	Disable
• Timer 3	
Timer Event	Disable

Item	Setting
24-Hour Continuous Settings	Disable
Start Time	00:00
End Time	00:00
Repeat Interval	None
• Operation	
Start Time Preset	None
Video Record	Disable
E-mail Notification	Disable
External Device Output	Disable
• Timer 4	
Timer Event	Disable
24-Hour Continuous Settings	Disable
Start Time	00:00
End Time	00:00
Repeat Interval	None
• Operation	
Start Time Preset	None
Video Record	Disable
E-mail Notification	Disable
External Device Output	Disable
• Display Options	
Detection Area/Line	Selected Detection Settings Only
Non-detection Area	Only enabled non-detection areas
Detection Results	Selected Detection Settings Only
• Infrared Switching	
Preset when Switching to Normal Capture	None
Preset when Switching to Infrared	None
• IPv4 Host Access Restrictions	
Apply Host Access Restrictions	Disable
Default Policy	Authorize Access
Network Address / Subnet	01: / 32 Yes
	02: / 32 Yes
	03: / 32 Yes
	04: / 32 Yes
	05: / 32 Yes
	06: / 32 Yes
	07: / 32 Yes
	08: / 32 Yes
	09: / 32 Yes
	10: / 32 Yes
	11: / 32 Yes
	12: / 32 Yes
	13: / 32 Yes
	14: / 32 Yes
	15: / 32 Yes
	16: / 32 Yes
	17: / 32 Yes
	18: / 32 Yes
	19: / 32 Yes
	20: / 32 Yes
• IPv6 Host Access Restrictions	
Apply Host Access Restrictions	Disable
Default Policy	Authorize Access
Prefix / Prefix Length	01: / 128 Yes
	02: / 128 Yes
	03: / 128 Yes
	04: / 128 Yes
	05: / 128 Yes
	06: / 128 Yes
	07: / 128 Yes
	08: / 128 Yes
	09: / 128 Yes
	10: / 128 Yes
	11: / 128 Yes
	12: / 128 Yes
	13: / 128 Yes
	14: / 128 Yes
	15: / 128 Yes
	16: / 128 Yes
	17: / 128 Yes
	18: / 128 Yes
	19: / 128 Yes
	20: / 128 Yes
• Certificates	
Certificate Status	Not Installed
Country (C)	
State/Province (ST)	
Locality (L)	
Organization (O)	
Organizational Unit (OU)	
Common Name (CN)	

Item	Setting
Validity Period Start Date	
Validity Period End Date	
• Encrypted Communications	
HTTPS Connection Policy	HTTP
• 802.1X Authentication	
802.1X Authentication	Disable
Authentication Status	Stop
• Authentication Method	
Authentication Method	EAP-MD5
User Name	
• IPsec	
IPsec	Auto Key Exchange
• Auto Key Exchange Settings	
IPsec SA Encryption Algorithm	AES->3DES
IPsec SA Authentication Algorithm	HMAC_SHA1_96
IPsec SA Validity Period (min)	480
ISAKMP SA Encryption Algorithm	AES->3DES
ISAKMP SA Authentication Algorithm	SHA1
DH Group	Group 14->Group 5->Group 2
ISAKMP SA Validity Period (min)	480
• IPsec Set 1	
IPsec Set	Disable
IPsec Mode	Tunnel Mode
Destination IPv4 Address	
Destination IPv6 Address	
Source IPv4 Address	
Source IPv6 Address	
IPsec Protocol	ESP
Security Gateway IPv4 Address	
Security Gateway IPv6 Address	
Destination Subnet Mask Length	16
Destination Prefix Length	16
IKE Pre-Shared Key	
SA ESP Encryption Algorithm	AES
SA ESP Authentication Algorithm	HMAC_SHA1_96
SA ESP Encryption Key (outbound)	
SA ESP Authentication Key (outbound)	
SA ESP SPI (outbound)	
SA ESP Encryption Key (inbound)	
SA ESP Authentication Key (inbound)	
SA ESP SPI (inbound)	
SA AH Authentication Algorithm	HMAC_SHA1_96
SA AH Authentication Key (outbound)	
SA AH SPI (outbound)	
SA AH Authentication Key (inbound)	
SA AH SPI (inbound)	
• IPsec Set 2	
IPsec Set	Disable
IPsec Mode	Tunnel Mode
Destination IPv4 Address	
Destination IPv6 Address	
Source IPv4 Address	
Source IPv6 Address	
IPsec Protocol	ESP
Security Gateway IPv4 Address	
Security Gateway IPv6 Address	
Destination Subnet Mask Length	16
Destination Prefix Length	16
IKE Pre-Shared Key	
SA ESP Encryption Algorithm	AES
SA ESP Authentication Algorithm	HMAC_SHA1_96
SA ESP Encryption Key (outbound)	
SA ESP Authentication Key (outbound)	
SA ESP SPI (outbound)	
SA ESP Encryption Key (inbound)	
SA ESP Authentication Key (inbound)	
SA ESP SPI (inbound)	
SA AH Authentication Algorithm	HMAC_SHA1_96
SA AH Authentication Key (outbound)	
SA AH SPI (outbound)	
SA AH Authentication Key (inbound)	
SA AH SPI (inbound)	
• IPsec Set 3	
IPsec Set	Disable
IPsec Mode	Tunnel Mode
Destination IPv4 Address	
Destination IPv6 Address	
Source IPv4 Address	

Item	Setting
Source IPv6 Address	
IPsec Protocol	ESP
Security Gateway IPv4 Address	
Security Gateway IPv6 Address	
Destination Subnet Mask Length	16
Destination Prefix Length	16
IKE Pre-Shared Key	
SA ESP Encryption Algorithm	AES
SA ESP Authentication Algorithm	HMAC_SHA1_96
SA ESP Encryption Key (outbound)	
SA ESP Authentication Key (outbound)	
SA ESP SPI (outbound)	
SA ESP Encryption Key (inbound)	
SA ESP Authentication Key (inbound)	
SA ESP SPI (inbound)	
SA AH Authentication Algorithm	HMAC_SHA1_96
SA AH Authentication Key (outbound)	
SA AH SPI (outbound)	
SA AH Authentication Key (inbound)	
SA AH SPI (inbound)	
• IPsec Set 4	
IPsec Set	Disable
IPsec Mode	Tunnel Mode
Destination IPv4 Address	
Destination IPv6 Address	
Source IPv4 Address	
Source IPv6 Address	
IPsec Protocol	ESP
Security Gateway IPv4 Address	
Security Gateway IPv6 Address	
Destination Subnet Mask Length	16
Destination Prefix Length	16
IKE Pre-Shared Key	
SA ESP Encryption Algorithm	AES
SA ESP Authentication Algorithm	HMAC_SHA1_96
SA ESP Encryption Key (outbound)	
SA ESP Authentication Key (outbound)	
SA ESP SPI (outbound)	
SA ESP Encryption Key (inbound)	
SA ESP Authentication Key (inbound)	
SA ESP SPI (inbound)	
SA AH Authentication Algorithm	HMAC_SHA1_96
SA AH Authentication Key (outbound)	
SA AH SPI (outbound)	
SA AH Authentication Key (inbound)	
SA AH SPI (inbound)	
• IPsec Set 5	
IPsec Set	Disable
IPsec Mode	Tunnel Mode
Destination IPv4 Address	
Destination IPv6 Address	
Source IPv4 Address	
Source IPv6 Address	
IPsec Protocol	ESP
Security Gateway IPv4 Address	
Security Gateway IPv6 Address	
Destination Subnet Mask Length	16
Destination Prefix Length	16
IKE Pre-Shared Key	
SA ESP Encryption Algorithm	AES
SA ESP Authentication Algorithm	HMAC_SHA1_96
SA ESP Encryption Key (outbound)	
SA ESP Authentication Key (outbound)	
SA ESP SPI (outbound)	
SA ESP Encryption Key (inbound)	
SA ESP Authentication Key (inbound)	
SA ESP SPI (inbound)	
SA AH Authentication Algorithm	HMAC_SHA1_96
SA AH Authentication Key (outbound)	
SA AH SPI (outbound)	
SA AH Authentication Key (inbound)	
SA AH SPI (inbound)	
• Video Record Settings	
Video Record Action	Record to Memory Card
• Memory Card Operations	
Operation Settings	Save Logs and Videos

Item	Setting
Video Format	JPEG
Pre-event Buffer (number of frames)	0
Post-event Buffer (number of frames)	0
Pre-event Buffer (sec)	0
Post-event Buffer (sec)	0
Overwrite videos	Enable
Auto Video Delete	Disable
Days Saved	30
Delete Time	00:00
• Initialization	
Network Settings	Save
• Backup / Restore	
Save Destination	Memory Card
• Update Firmware	
Restore Default Settings	Do Not Restore
• Log Notifications	
Use log notifications	Disable
Notification Level	Error
Mail Server Name	
Mail Server Port	25
Sender (From)	
Recipient (To)	
Authentication	None
User Name	
POP Server	
Subject	

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

BIE-7257-000