Hanwha Vision

Network Camera

Online help

TID-A800

Monitoring

You can check the live screen to view what is being captured by the camera and control screen capture, and other features. When you click the button on the screen, the live screen will appear.

You can move to the live screen, playback screen or setup screen by clicking the buttons at the top.

- (Live): Check the live screen to view what is being captured by the camera and control a variety of camera features.
- (Playback): Search and playback a recorded image from an SD card (or microSD card) or NAS.
- (Setup): Change the camera settings.

The following information can be found in the upper right corner of the web viewer.

- **Model name**: Displays the camera model name. Clicking the model name opens detailed version information.
- **Account name**: Displays the name of the account that accessed the camera, such as 'admin' or 'user 1'. To log out from the web viewer, click the account name and then click **[Logout]**.
- **Apps**: Opens a list of all applications installed on the camera. Click **[Go App]** button to access the settings screen for a specific application. (May not be displayed depending on account permissions.)
- **Help**: Opens the Online Help in a new window, providing detailed information about the features of the camera web viewer. Click **[Protocol]** to view the list of SUNAPI APIs requested on the current page. The most recently requested API appears at the top, and the API address can be copied using the copy button next to each item. The list is cleared upon leaving the page. The filter function is available to display only APIs matching a specific SUNAPI action.
- **Theme switch**: You can set the theme color of the camera web page. Choose and apply the preferred theme (White or Black) according to your preference or the ambient brightness.

> **Note**
>
> - If you click the icon at the top right of the live page, you can see the connected IP address and the authentication status. If successfully authenticated, the icon will be colored in green. If failed to be authenticated, it will be colored in red. If authentication is irrelevant due to the use of HTTP connection, dash (-) will be displayed.
> - The VoIP call status will be displayed together with an icon in the upper-right of the live page. The call status will be displayed in one of three statuses: [Waiting], [Calling], and [Busy].
> - When playing a video on the live page, ghosting might occur under one of the following cases:
>   - When the resolution changed after changing the profile
>   - When the data transfer is delayed due to network delay after changing the profile
>   - When the size or location of the web browser window changed

---

Icons

The icons at the bottom of the live screen provide the following functions (Some functions may not work with certain browsers or codecs.):

Icon	Description of function
Call	You can have a two-way conversation by transmitting audio to and from the camera in real time. • When initiating a call from the web page

Icon	Description of function
	• Click the call button to start a two-way call. • When the call is connected, the call button displays the elapsed connection time and a "Pause" button, and an "End call" button appears. • Click the "Pause" button to pause audio transmission to the camera; click it again to resume transmission. • Click the "End call" button to end the call and return to the initial call button state. • When receiving a call request from the camera • The call button changes to an "Take call" button and an "End call" button appears. • Click the "Take call" button to start the call; the button displays the elapsed connection time and a "Pause" button. • Click the "Pause" button to pause audio transmission to the camera; click it again to resume transmission. • Click the "End call" button to end the call and return to the initial call button state. Two-way call can only be used by one user at a time. If another user is already on a call, a notification message will be displayed. If the video frame rate is below 30 IPS, video update may be delayed by up to 30 seconds depending on the frame rate.
Door	Controls a connected alarm output device (e.g., electronic door lock) to open a door or send an alarm signal. Clicking the button sends a signal to "Alarm output 2". While the signal is being output, the button is displayed in an active state.
Video setup	You can check or change the profile applied to the current live screen. You can also change the display settings of the live screen.

Icon	Description of function
ⓘ Status	Check the connection information for each profile and for connected users at the same time. It is also possible to display streaming information on the video screen.
Privacy area	The Privacy area setting window will appear. Specific functions related to privacy mask areas can be controlled, including setting the use of the privacy mask area feature or designating a privacy mask area. For more information on privacy mask areas, refer to **[Setup]**>**[Video & Audio]**>**[Video setup]**.
Full screen	View the live screen in full screen. To return to the size of the previous web browser, click the icon in full screen mode or press the **[Esc]** key on the keyboard.
Size option	The size changes to the next size each time you click it. • (Fit): Fit the camera image to the size of the web browser. • 1:1(Original Size): View the camera image at its actual resolution. • (Aspect Ratio): View the live screen in the web browser by zooming in or out, while maintaining the aspect ratio of the camera image.
Capture	Capture and save the live screen as a PNG image file. A captured image file is saved in the default recording path of each browser.
REC Record	You can record and save the live screen to a PC. Click the Record icon to start recording; click the icon again to stop recording. Recorded files are saved in .avi format and can be saved in the default path of the browser or a file path can be set in the 'Save as' window. To protect your video files with password, select ZIP from the list of the video recording file format and enter a password. You need to enter

Icon	Description of function
	the password to play back downloaded videos. The password setup function for recorded videos is not available in some camera models.
⬚ Pixel count	On the live screen, you can see the number of horizontal/vertical pixels in the area selected with the mouse. Click the Pixel count icon and click and drag the desired area with the mouse. The selected area will be displayed and the number of pixels in the image will be displayed. When you click the Pixel count icon again, the Pixel count function ends.
 Microphone	Use the microphone function. Microphone function can be used only when accessed in HTTPS mode.
 Alarm output	When you click a desired alarm output number, the alarm will be outputted as previously set. The alarm can be set from the **[Setup]**>**[Event]**>**[Alarm output]** page. The number of alarm outputs varies depending on the camera.
 Speaker	Adjust the audio volume of the live screen. Click the icon to activate the audio and adjust the volume. To use the Speaker function, the **[Audio in]** function should be activated for the relevant profile. To activate the audio input function, select **[Enable]** from **[Setup]**>**[Basic]**>**[Video profile]**>**[Audio in]**.
▷/■ Audio play/Audio stop	You can play or stop an audio clip of your choice after selecting it from the audio clip list. You can play audio of your choice while monitoring the live video. Go to **[Setup]**>**[Video & Audio]**>**[Audio setup]**>**[Audio clip]** to register an audio clip.

To capture image

- In the scene to capture, click the capture icon(📷).
- When the captured image is saved, a notification message will pop up. The capture image is saved to the path specified in each browser.

To record video

- Click the Record icon(⏺).
- To end the manual recording, click the Record icon(⏺) again.

The manual recording can be saved as an .avi file in your PC. Specify the path and save the video.
To protect video recordings with password

- You can select ZIP as the recording format and click the "REC" icon to set the password.

Your video recordings will be saved as .zip in your PC. You need to enter the password to play back the videos. (The password setup function for recorded videos is not available in some camera models.)

To switch to full screen

- Select the Full screen icon(⛶) to change the viewer mode to full screen.
- To exit the full screen mode, click the Full screen icon(⛶) again or the [Esc] key on the keyboard.

To use microphone

- Click the microphone icon(🎙).

If no sound is heard when connecting or disconnecting the audio jack from the PC while playing the audio, click the microphone icon(🎙) and enable it.
The sound output from the camera may be inconsistent depending on the microphone device settings. If the sound is not well heard, turn off the improvement function of the microphone properties in the PC where the web viewer is operating, or adjust the microphone device volume.

To use speaker

- Click the Speaker icon(🔊).

To count the number of pixels

- Click the Pixel count icon(⬚).
- Set the area by dragging the mouse on the image. The number of horizontal/vertical pixels of the area will be displayed on the screen.

To play an audio clip

- Click the Play icon (▷) after selecting an audio clip of your choice from the audio clip list.
- To stop playing it, click the Stop icon (■).

Video setup

Profile

The name and detailed information of the Video profile applied to the current live screen will be displayed. When you press the **[Profile]** drop-down icon, a Video profile list that can be used from the current web viewer will appear; when you select the desired Video profile, it will be applied to the live screen

immediately. You can check the resolution, codec, frame rate and target bitrate of the selected Video profile.

Display

Set the contrast, brightness, sharpness, etc. of the live screen; when you enter the setting, it will be applied to the live screen immediately. Click the ↻ button if you want to reset all the display settnigs. (The **[Display]** function is not supported on some camera models.)

Status

Profile access

Check the connection status of all currently-set profiles or check the status of currently-connected users.

Current users

You can check the applied profile for each user, bitrate (kbps), network connection status and IP address of all users currently connected to the camera.

Stream info

Display video information (resolution, video codec, frame rate, bitrate) and audio information (audio codec, sampling rate) in real time on the live video.

Playback

You can import and playback a recorded image from an SD card (or microSD card) or NAS.
When you click the ▶ button on the screen, the playback screen will appear. A time bar will appear at the bottom of the playback screen and an image recorded according to the set schedule or by an event is displayed on the time bar. When you click **[Refresh]**, the recorded image information in the time bar is updated to the latest.
You can search for a recorded image by event type or date, and capture or save it to a PC. Also, if the time on the camera system has been adjusted and thus resulted in overlapping time, the video recorded during that overlapping hour can be searched. If there are overlapping sections, the **[Overlapped section]** option will appear next to the **[All]** button.

You can move to the live screen, playback screen or setup screen by clicking the buttons at the top.

- 🖥(Monitoring): Check the live image being captured by the camera and control various camera functions.
- ▶(Playback): Search and playback a recorded image from an SD card (or microSD card) or NAS.
- ⚙(Setup): Change the camera settings.

> **Note**
>
> - A video needs to be recorded first on the **[Live]** page before being able to play it.
> - Connecting to the web viewer via Chrome, the record playback screen feature can be securely used.

Playback icons

The icons at the bottom of the playback screen provide the following functions:

Icon	Description of function
▷/II Playback/Pause	Playback or pause an image.
▷▷ Speed	Play the video at 2x speed.
🔊 Speaker	Adjust the audio volume of the playback screen. Click the button to activate the audio and adjust the volume.

Playback a recorded image through event search

You can search for a recorded image by event type.

To search by event and play back

1. Click the Show button on the Playback screen. If there is any video taken on the day of searching, it will be displayed on the time bar.
2. To search by event type, click the **[All]** button at the top of the time bar and select an event you want.
3. Click the **[Apply]** button to display the searched events on the time bar.

4. Click the Playback button.
5. To stop the playback, click the Pause button.

Playback a recorded image through time search

Search for a recorded image by selecting a date and time on the calendar. When you click the **[Today]** button on the time bar, only images recorded today will be searched.

To search by time and play back

1. Click a date on the time bar, select the date you want on the calendar, and set the start and end time.
   - When you select **[All day]**, the start and end time will be set automatically from 00:00:00 to 23:59:59.
2. Click the **[Apply]** button.
3. Click the Playback button. The video of the selected time will play back.
   - If the video is already playing, the recorded time of the current video is displayed.
   - Move the button along the time bar to play back the video of the desired time.

Recorded video save

Recorded videos can be saved to files.

To save a video

1. Click the **[Export]** button.
2. In **[Time]**, set the Start time and End time for the video to save.
3. From **[Type]**, select the file type you want.
   - AVI: Saves in .avi.
   - ZIP: Saves in .zip. You can set a password for your files. You need to enter this password to unzip those files in order to play videos. (The password setup function for recorded videos is not available in some camera models.)
4. Click the **[OK]** button.

Video profile

The user can add or delete a video profile, and change the profile properties. Set the video profile, frame rate and codec as 'Video profile' in advance and later change the video profile to stream or play back an image. When you finish the setting, click **[Apply]** at the bottom of the page.

Select channel

After selecting your camera channel, you can set the details of Video profile for each channel.
Click **[Info]** to see a summary of the channel condition.

Adding a channel

You can add a virtual channel to show a zoomed view of the face area on the front of the intercom.

1. In **[Select channel]**, click **[Add]**. Channel number is automatically assigned.
2. Check the **[View mode]**.
   - **Face zoom**: Moves and zooms (DPTZ) the video to the intercom user's face area.
3. Click **[Apply]**.

Video profile

Users can select a video profile according to the service environment and circumstances of product use. In addition to the profiles provided by default, users can add a new profile or delete an existing one. You can set the codec, profile type, resolution, frame rate, and other settings for each profile.

Profile list

The profile list is provided by default; all profiles added by the user are also displayed.
Copy the RTSP URL for each profile from the **[RTSP URL]** column.

Adding a video profile

1. Click **[Add]**. A new item will be added to the profile list.
2. Enter the name of profile in the **[Name]** field. The entered name will appear in the profile list.
3. Set the profile items, including **[Codec]**, **[Profile type]** and **[Resolution]**.
4. Click **[Apply]** at the bottom of the page.
5. When the confirm window appears, click **[OK]**. The new profile will be added.

Changing a video profile property

1. Select the profile which you wish to change from the profile list.
2. Change the relative settings, including **[Codec]**, **[Profile type]** and **[Resolution]**.
3. Click **[Apply]** at the bottom of the page.
4. When the confirm window appears, click **[OK]**. The settings of the selected profile will change.

Deleting a video profile

1. Select the profile which you wish to delete from the profile list.
2. Click **[Delete]**.
3. When the confirm window appears, click **[OK]**. The selected profile will be deleted.

Name

The name of the profile selected from the profile list will be displayed. You can enter a new profile name if creating a new profile.

Codec

Select the codec which you wish to apply to the profile. The profile properties may vary according to the selected codec type.

Profile type

Select a profile type to apply. The selected profile type will be displayed in the **[Type]** column of the profile list. The setup items may vary according to the selected codec type.

- **Default profile**: This is the default profile applied for streaming a live camera image. 'Default' is displayed in **[Type]** in the profile list.
- **Email/FTP profile**: A video profile that is used when sending a capture image of the event to email and FTP servers, or when sending video clips to the FTP server. (Video clips can be sent to FTP only if the **[Codec]** is set to **[H.264]** or **[H.265]**.) [Event] will be displayed in the **[Type]** column.
- **Edge recording profile**: This profile is applied for recording an image on an SD card or NAS. 'Record' is displayed in **[Type]** in the profile list.
  If multiple channels and profiles have set [Edge recording profile], the video is recorded using the profile that has most recently set the [Edge recording profile] option. For example, if both "profile 1" of Channel 1 and "profile 2" of Channel 2 have set the [Edge recording profile] option, and "profile 2" has most recently been set, "profile 2" will be used for video recording.
- **Frame Lock profile**: This is a profile applied to guarantee a certain level of video frame rate. 'FrameLock' is displayed in **[Type]** in the profile list. This 'Frame Lock profile' option appears only when **[Codec]** is set to **[H.264]** or **[H.265]**.
- **VoIP Profile**: This is a profile dedicated to VoIP. This is displayed as 'VoIP' in **[Type]** of the profile list. **[Codec]** is locked to **[H.264]**. If Codec is changed, the VoIP profile is deselected.

Audio in

When the camera has an internal microphone or an external microphone is connected, you can set external sounds to be inputted in the image.
To use the Speaker function on the **[Live]** page, **[Enable]** should be selected for **[Audio in]**.

Profile properties

Set the details for the current video profile.

Resolution

Set the resolution of the camera image.

> **Note**
>
> - In order to stream a high-resolution image smoothly, it is recommended to connect to the web viewer using Google Chrome.

Frame rate

Set the number of frames per second.
The range of frame rates available varies according to the frame rate value selected from **[Video & Audio]** > **[Camera setup]** > **[Sensor]**.

Maximum bitrate

Set the maximum bitrate of the image when **[Bitrate control]** is **[VBR]**.

Target bitrate

Fix the amount of image data to be sent if **[Bitrate control]** is **[CBR]**.

Advanced

If either **[H.264]** or **[H.265]** is set for **[Codec]** of the profile, all advanced setup items will be displayed. If **[MJPEG]** is selected for **[Codec]** of the profile, only the **[Encoding priority]** item will be displayed.

Bitrate control

Set how to adjust the amount of image data.

- **CBR**: Constant Bitrate is for sending full-frame data of a constant size. When CBR is selected, the size of data to be sent is set by setting the target bitrate. CBR has a constant data size, making it is easy to predict the data size for the whole system, enabling the system to be operated stably.
- **VBR**: Variable Bitrate is for sending an image within the maximum bitrate without fixing the data size of the frame. VBR can use storage space capacity or bandwidth efficiently while maintaining the quality, but if an image suddenly becomes more complex, it may cause a strain on the network.

> **Note**
>
> - When the Bitrate control is set to 'CBR (fixed bitrate)' and the priority on image quality mode is selected, the actually transferred frame rate may be different from the set frame rate in order to guarantee the best image quality under the set bitrate in consideration of the complexity on screen.

Video compression

You can set the video compression ratio.
The **[Compression]** option of **[Profile properties]** sets the priority of encoding when [Bitrate control] is set to [CBR]. The **[Video compression]** option sets sets

the priority of encoding, which affects the amount of data transmission and video quality based on the video compression rate for VBR action.
The higher the value of [Video compression], the better the video compression rate. As the video compression rate increases, the amount of video data transmission decreases, but the video quality might be degraded as a result. If the video compression rate is lowered by setting a low value to [Video compression], the video quality improves, but the amount of video transmission could increase.
[Video compression] is activated if either **[H.264]** or **[H.265]** is selected for **[Codec]** of the profile, and **[VBR]** is set for **[Bitrate control]**.

Encoding priority

Set the priority between frame rate and image quality if the amount of image data exceeds the target bitrate. (Supported options may vary depending on camera specifications.)
If **[Codec]** of the profile is **[MJPEG]**, you can select between **[Frame rate]** and **[Bitrate]**.

GOV length

GOV (Group of Video) is a group of image frames for H.264/H.265 video compression; it means the group of frames from one I-frame to the next I-frame. GOV contains both I-frame and P-frame. I-frame is the frame which becomes the basis of compression (also called the key frame); it has data for one complete image. P-frame has information of the changed area only, based on the front frame. For this reason, the number of I-frames is fewer as the GOV length is longer, making the image size small, while the number of I-frames is more as the GOV length becomes shorter, making for a larger image size. The maximum value of the GOV length varies according to the **[Frame rate]** in **[Profile properties]**.

Profile

This menu becomes active only when the codec of the profile is H.264. The profile can be considered as a bundle of various compression technologies. The profiles supported in the Hanwha Vision cameras include **[Baseline]**, **[Main]** and **[High]**. The compression performance becomes higher and the quality becomes better as you move from Baseline to High, but a lot of system resources are used for compressing and decompressing and may create a strain on the playback equipment. (Supported options may vary depending on camera specifications.)

Dynamic GOV

To apply the Dynamic GOV function to the current profile, select **[Enable]**.
Dynamic GOV is the function whereby the GOV length is changed automatically according to the image situation. In a video where little or no motion is detected, GOV operates based on the value set for **[Dynamic GOV]** by user, decreasing the bitrate of the whole video. Once motion is detected, I-frame is displayed immediately. Then, until the motion is not detected anymore, GOV operates based on the value set for **[GOV length]**.

- Enter the maximum GOV length to apply when there is no motion in the image. The range of input value is displayed next to **[GOV length]**. The input value in **[GOV length]** becomes the minimum value, while the maximum value is 480; it varies according to the **[Frame rate]** in **[Profile properties]**.

> **Note**
>
> - When the WiseStream function is used, if the dynamic GOV and dynamic FPS functions are used, the WiseStream performance is optimized. The WiseStream can be set in the **[Video & Audio]** > **[WiseStream]** menu.

Dynamic FPS

Select **[Enable]** to apply the Dynamic FPS function to the profile currently being set.
Dynamic FPS is a function that automatically changes FPS settings, from the minimum FPS setting to frame rate setting depending on the screen situation. In a nearly motionless video, FPS will function using the minimum FPS setting, which in turn reduces the overall screen bitrate. When a motion is detected, FPS will use an increased FPS value.

Minimum FPS

Enter the minimum FPS value to be applied when Dynamic FPS is enabled.
The **[Minimum FPS]** option cannot be configured if the FPS value is set as 1.

> **Note**
>
> - When the WiseStream function is used, if the dynamic GOV and dynamic FPS functions are used, the WiseStream performance is optimized. The WiseStream can be set in the **[Video & Audio]** > **[WiseStream]** menu.
> - Dynamic FPS is enabled only when **[Codec]** is set to **[H.264]** or **[H.265]** and **[Bitrate control]** is set to **[VBR]**.

Multicast

Multicast is the method used to send data in one instance from the camera to multiple pieces of equipment. Set whether or not to use RTSP (Real Time Streaming Protocol) on the current profile and enter the detailed information.

Multicast (RTSP)

To send an image by using RTSP, select **[Enable]**.

IP address

Enter an IPv4 address that can be connected from the IPv4 network. The range of multicast IP address is anywhere between 224.0.0.0 and 239.255.255.254. However, 255 cannot be used at the end.

Port

Set the port that controls sending of the image. The range of multicast RTSP ports is from 1024 to 65534, and only even numbers are allowed. (The 3702 port however, cannot be used.)

TTL

You can set the TTL of the RTSP packet. A value between 0 and 255 can be entered for the TTL value.

User

You can manage the user accounts connecting to the camera. You can change the administrator password and guest settings, authentication setup and setting of current users. When you finish the setting, click **[Apply]** at the bottom of the page.

Change administrator info

You can change the administrator account ID and password. To reinforce security, create a password by combining random English uppercase and lowercase letters, numbers and special characters.

ID

View or change the administrator ID that is currently used.

> **Note**
>
> - Administrator ID must contain only alphanumeric characters with a maximum length of 8 characters.
> - The default guest ID "guest" or the default user ID "user1", "user2"..."user10" cannot be used as the administrator ID.

Current password

Enter the current password. To prevent the password from being changed by someone else, the administrator password can be changed only after entering the previous password.

New password

Enter a new password.

Confirm new password

This is the confirmation procedure to prevent incorrect input of a new password. Enter the new password again.

> **Note**
>
> - It is recommended to change the password every three months.
> - The password restrictions are as follows:
>   - After the factory reset, both the admin and user passwords will reset, and you need to create them again.
>   - When you access the camera web viewer for the first time, or access it after the initialization, you will be moved to the password setting menu.
>   - To use the web viewer menu, you need to set the new password in the password change menu and log in to the web viewer again with the changed password.
>   - When changing the admin password, if the current password is not matched, then you cannot set the new password.
>   - After changing the password, if there is a camera connected to a client, such as CMS or NVR, then you need to register the changed password before use. If you

maintain the same connection, the client will use the previous password for authentication, so the account can be locked.

- When logging in to the web viewer, if you entered incorrect password more than five times, it will be locked for 30 seconds and you won't be able to access the web viewer.
- If connection is made from various places with the same ID, or the password is changed while a number of Internet browsers are open, the Internet browsers may malfunction. It is recommended that a password be changed only from one location or only through one Internet browser.

Admin login timeout

If there are no activities for a certain period of time after accessing the camera web viewer with the administrator account, the web viewer login will be disconnected. Enter the timein minutes to automatically disconnect the admin login when the administrator is not active.

Note

- This **[Admin login timeout]** function is not supported in Safari.

Guest settings

When you select **[Allow guest access]**, a guest can connect to a web viewer screen. When you connect with a guest account, you can see only the live screen on the web viewer. Guest ID and password are 'guest/guest' and these cannot be changed.

Authentication setup

When you select **[Allow RTSP connection without authentication]**, you can access the camera video using RTSP (Real Time Streaming Protocol) without the login authentication.

Current users

You can set the connection information for user accounts other than the administrator, and set use permissions including audio in, audio out, alarm output and profile.
When a registered user logs in, only the functions set for that user are enabled.
10 current user accounts are set by default; you can add or delete an account.
Up to 10 current IP user accounts can be used.

Note

- If you want to select the configured user that can use ONVIF, the use of the function may be restricted depending on the permission level set.

Use

Select the check box to enable the selected user account.

Name

Enter the ID

Password

Enter the password. The password setting rule is same as the administrator password setting rule.

Admin privilege

Authorize the selected users with admin privileges. Normal users can use only functions that their administrator allowed, but administrators can access and set any functions they want. However, even if admin privileges are given to users, they cannot change their admin ID or password.

Profile setup

Grant access to the selected user to control the detailed settings for video profiles.

Video setup

Grant access to the selected user to control detailed settings related to a video output.

Camera setup

Grant access to the selected user to control detailed settings related to camera video.

Audio in

Grant access to the entered audio to the selected user. If users with audio input access sign in to the camera web viewer with their account, they can check the video screen along with the audio. If the user does not have access to audio input, they can see the screen only.

Audio out

Grant access to the audio output to the selected user. The users with audio output access can transmit audio through microphones and other devices.

Alarm output

Grant access to the alarm output to the selected user. The users with alarm output access can transmit alarms.

Log

Grant the selected user permission to access logs (access log, system log, event log, remote log transmission).

Profile access

Set the type of video profiles the selected user can choose on live mode. If set to **[Default]**, the user can only check videos through the default profile. If set to **[All]**, the user can check videos through all profiles.

Playback

Grants the selected user the right to search and play the recorded video. When a user with playback permission accesses the web viewer, the ▶(playback) icon is activated at the top.

Open platform

Grant the selected user permission to access the app installed on the camera and check the detailed information of the app. The installed app information can be checked in the **[Open platform]** menu.

Inputting a current user

1. Select the row of the current user account you wish to use. The current user account is changed to a status where input is available.
2. Select the check box in the **[Use]** column.
3. Enter the ID and password in the **[Name]** and **[Password]** columns.
4. Select a function to allow in the **[Audio in]**, **[Audio out]** and **[Alarm output]** columns respectively, and select the type of profile to allow in the **[Profile]** column. (Some cameras do not support setup of **[Audio in]**, **[Audio out]**, and **[Alarm output]**.)
5. When the input of the current user account is completed, click **[Apply]** at the bottom of the page.
6. When the confirm window appears, click **[OK]**.

Note

- If the number of current user accounts is less than 10, you can add a current user account by clicking **[Add]**.

Modifying a current user

1. Select the row of the current user account you wish to modify.
2. Change the function settings and click **[Apply]** at the bottom of the page.
3. In the confirmation dialog, click **[OK]**. Then the information of the user will be changed.

Deleting a current user

1. Select the row of the current user account you wish to delete and click **[Delete]**.
2. Click **[Apply]** at the bottom of the page.
3. In the confirmation dialog, click **[OK]**. Then the information of the selected current user will be deleted.

Date & Time

You can check the current system time of the camera, change the time setting according to the local time zone, or set the system time through synchronization with the PC time or NTP server.

Current system time

The current system time of the camera is displayed. The previously set system time is displayed.

Time zone

The camera time is set based on standard time (GMT).

Time zone

The user can select the time zone.

Daylight saving time

When an area where daylight saving time is used is selected, the **[Daylight saving time]** menu will be displayed. The start and end time for daylight saving time in the selected time zone are displayed. When **[Enable]** is selected for **[Daylight saving time]**, a time which is one hour ahead of the standard time of the relevant zone is displayed.

> **Note**
>
> - Only when **[Daylight saving time]** is set to **[Enable]** will the time appearing on the timeline of the **[Playback]** screen be displayed according to daylight saving time.
> - If the clock function of the PC is set to automatically apply daylight saving time, the daylight saving time option is automatically selected in the camera web viewer, and cannot be changed by the user.

System time setup

The user can set the camera time manually or by synchronizing it with an NTP server.

Manual

The user can enter the current time manually for the camera or synchronize it with the time of the PC with which it is currently being used.

- Set the system time by entering the time in **[Y - M - D]** and **[h: m: s]**.
- When **[Synchronize with PC viewer]** is selected, the time of the PC viewer is synchronized with the system time. When **[Synchronize with PC viewer]** is selected, the same time zone should be separately set for both the PC and the camera.

Synchronize with NTP server

The NTP (Network Time Protocol) server time is synchronized with the system time. 5 NTP server addresses are entered by default. You can change an NTP server address by clicking the address input field.

IP & Port

Enter IP address and port. You can set IPv4 and IPv6 on the **[IP address]** tab. You can set the port for each protocol on the **[Port]** tab. When you finish the setting, click the **[Apply]** button at the bottom of the page. When you click the **[Apply]** button, you will need to reconnect to the web viewer.

IPv4 setup

You can check or change the IP type, MAC address, IP address, subnet mask, gateway, and DNS information used for the network communication using the IPv4 type.

IP type

Select the IP connection type. If a fixed IP address is used, set **[Manual]** and enter the information. If a dynamic IP is used, set **[DHCP]** and enter the DNS address only.

- **Manual**: Enter and set the IP address, subnet mask, gateway, DNS1 and DNS2 directly.
- **DHCP**: Set DNS1 and DNS2.

MAC address

The MAC address of the camera is displayed.

IP address

The current IPv4 address is displayed. You can change the IP address by setting **[Manual]** for **[IP type]**.

Subnet mask

The subnet mask of the current IP address is displayed. You can change the subnet mask by setting **[Manual]** for **[IP type]**.

Gateway

The gateway of the current IP address is displayed. You can change the gateway by setting **[Manual]** for **[IP type]**.

DNS setting by DHCP

This is displayed when **[DHCP]** is set for **[IP type]**. If you select **[Use]**, the DNS address is automatically assigned.

DNS1/DNS2

The address of the DNS (Domain Name Service) server is displayed.

Host name

Host name is the name to retrieve the host name which is used in ONVIF GetHostname command. The first character must be alphabetic and only alphabetic characters, numbers, hyphen(-), and the '.' symbol can be entered. Hyphen(-) and the '.' symbol cannot be at the beginning or end of the host name. Up to 63 characters can be entered. Name of the camera is input as default; does not need to be set as it is not a required value.

> **Note**
>
> - If you choose **[Change host name]** option under **[Network]**>**[HTTPS]**>**[Secure connection system]**>**[HTTPS (Use a secure connection)]**, the host name will be changed to the common name set in the certificate.

MTU

Set the maximum transmission unit (MTU) at which data can be transferred from the network interface. The MTU value can be set from 1280 octets to 1500 octets. If the value is set too low, the video playback may be delayed. Therefore, the MTU value should be set according to the user's network environment.

Vendor class

You can type the DHCP vendor class identifier up to 127 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (-_~!@[],.?). A blank space cannot be used.

ICMP (Timestamp)

Select **[Enable]** to use the Internet Control Message Protocol (ICMP) timestamp request message. You can use the timestamp to calculate the round-trip time or time difference between the two systems. The ICMP (Timestamp) option is enabled by default.

IPv6 setup

IPv6 is a next-generation Internet address system with data processing speed, concurrent data processing capacity and Internet address system which are more expanded than IPv4. To use IPv6, select **[Enable]**. You can set the IP type, IP address, Prefix and gateway. When you select a camera model from the IP installer, you can select either IPv4 or IPv6 address and connect by entering the appropriate address directly in the web browser.

IP type

Select the IP connection type. The default value is **[Default]**. If DHCP is not detected, the value will automatically be changed to the previous setting.

- **DHCP**: The IPv6 address assigned through DHCP is displayed.
- **Manual**: The user can enter an IPv6 address of choice.
- **Default**: The current IPv6 address is displayed.

> **Note**
>
> - After changing the setting, click the **[Apply]** button to close the web browser window. After a moment, access the changed IP address again.

IP address

Enter the IPv6 address.

Prefix

This value sets the IP range. If **[IP type]** is **[Default]**, **[Prefix]** value is 64. If it is **[Manual]**, you can change the **[Prefix]** value.

Gateway

Gateway is displayed when **[Manual]** is set for **[IP type]**. The user enters the gateway address directly.

Port

A port is the location used for sending and receiving data Click **[Port]** tab, set the relevant items, and then click the **[Apply]** button at the bottom of the page. It is recommended to use HTTPS and RTSP to reinforce image security.

> **Note**
>
> - When setting the port number, you cannot use 3702, 49152 or any number between 0 and 1023.

HTTP

The HTTP port is used for connecting to the camera using a web browser. The default value is 80 (TCP). The available range is between 1024 and 65535. When the HTTP port is changed, the web browser window will be closed. Enter the new HTTP port at the end of the IP address to reconnect. If the HTTP port is 80, the port number can be omitted. (e.g.: Camera IP address: 192.168.1.100, HTTP port In case of 8080 -> http://192.168.1.100:8080)

HTTPS

HTTPS has increased security over HTTP. This can be used when HTTPS mode is set in SSL, and the default value is 443 (TCP). The available range is between 1024 and 65535.

RTSP

This is the port for sending an image in RTSP (Real Time Streaming Protocol); the default value is 554. The available range is between 1024 and 65535.

Time out

To use the time out, select the **[Time out]** checkbox. If there is no response for a certain period of time when connection is made in RTSP, reset the port connection.

Call setup

You can set up SIP.
The Session Initiation Protocol (SIP) is used for VoIP calls. By using a network intercom where an SIP is activated, the user can make calls.
SIP can be set using either P2P method or PBX server. The P2P method is used if users are directly communicating over the same network and do not need to use functions provided by the PBX server. The PBX server method is used to communicate with users inside and outside of the IP network.
Once the setup is complete, click the **[Apply]** button at the bottom of the page.

Call setup

Ringtone

You can select the audio clip to play on the speaker when attempting to call the receiver.
You can add audio clips in **[Video & audio]**> **[Audio setup]**> **[Audio clip]**.

Calling time out

You can set up the maximum period of time to try connection when requesting an SIP call.
If the receiver does not receive the call request by the specified time, the call request automatically ends.

Status LED

If **[Enable]** is selected, LED is turned on to display current status depending on the intercom status.
If **[Enable]** is not selected, LED is turned off, and the status is not displayed.
The intercom status of each LED light is as follows:

Status	LED color	LED behavior
Standby	Blue	Turned on
Call button pressed and waiting on hold	Blue	Blinking
On the phone	Blue	Blinking slowly
Alarm output 2	Green	Turned on
Booting	Red	Turned on
Call error	Red	Blinking
Firmware update	White	Turned on

LED off during idle status

If **[Enable]** is selected, the LED status indicator is automatically turned off during idle status. It the status changes, the LED displays the current status.
If an event occurs in the touchless sensor while **[LED off during idle status]** is set to **[Enable]**, the LED status indicator is turned on for five seconds in blue.
To use the **[LED off during idle status]** function, **[LED off during idle status]** should be set to **[Enable]**.

End call request

If you select **[Enable]** and press the call button while you are in a status that is requesting a call from the intercom, the call request will be stopped. If you do not select [Enable], the proceeding call will not stop even when you press the call button while requesting a call and the call request will continue for the duration of the time that is set in [Calling time out].

Test call event

You can test whether the Call request event is received correctly by the VMS and web viewer.
Click the **[Test]** button to send a call request event. You can then verify the call request event on the VMS or web viewer that is connected to the live video and receiving events.

Microphone operation

If you want a microphone mounted on a camera to operate only on SIP or VMS calls, select **[During call only]**. If you want a microphone to always operate even when not on SIP or VMS calls, select **[Always]**.

> **Note**
>
> - If you want to operate the VMS call function, the **[Audio in]** option must be enabled in **[Basic]** > **[Video profile]**.

Video setup

You can set a privacy area in the camera's image or flip it in reverse directions (vertically or horizontally). In addition, you can display an analog image or change the video output type. (Depending on the camera model, privacy area, video screen flip/mirror function, or video output function might not be supported.)

Privacy area

To prevent a possibility of privacy invasion in the camera's image, you can set a privacy area. To use the privacy area function, click **[Enable privacy area]**. To deactivate a privacy area, deselect **[Enable privacy area]**, then you can check the full camera's image without anything hidden due to privacy. The set privacy areas are not deleted, and they can be checked in the privacy area list.

Pattern

Select the mosaic pattern to apply to a privacy area. Select **[Solid]** to apply the color set in the privacy area window. If you select the pattern, it will be applied to all the areas.

Setting a privacy area (PTZ camera)

1. Select **[Enable privacy area]** and click **[OK]** in the confirmation dialog.
2. Click on 4 corners with the mouse on the camera video screen.
3. In the **[Privacy area]** window, set the following:
   - Drag the icon ⊕ to place the desired video screen on a privacy area by adjusting the camera pan/tilt.
   - Enter the name of the privacy area in **[Name]**, select the color to cover the image in **[Color]**.
   - Select whether to enable **[Zoom threshold]** . The function ensures that a privacy area is used only if the image is magnified to higher than a zoom ratio set in [Set zoom threshold]. In other words, if the image is reduced below the zoom ratio, the privacy area is deleted from the image.
4. In the **[Privacy area]** window, click **[OK]**.
5. In step 3, if you select **[On]** in **[Zoom threshold]**, the **[Set zoom threshold]** window will appear. After setting the desired zoom ration, click **[OK]**.
6. A new privacy area is added to the list of privacy areas. The privacy area to which zoom threshold is applied will be marked as '[Zoom]' in the list of privacy areas. The color set in the camera's image screen is used to display the privacy area.

Setting a privacy area (zoom camera)

1. Select **[Enable privacy area]** and click **[OK]** in the confirmation dialog.
2. Drag with the mouse on the camera video screen to set the privacy area.
3. In the **[Privacy area]** window, set the following:
   - Enter the name of the privacy area in **[Name]**, select the color to cover the image in **[Color]**.
   - Select whether to enable **[Zoom threshold]** . The function ensures that a privacy area is used only if the image is magnified to higher than a zoom ratio set in [Set zoom threshold]. In other words, if the image is reduced below the zoom ratio, the privacy area is deleted from the image.
4. In the **[Privacy area]** window, click **[OK]**.
5. In step 3, if you selected **[On]** for the **[Zoom threshold]** option, then the **[Set zoom threshold]** window will appear. After setting the desired zoom ration, click **[OK]**.
6. A new privacy area is added to the list of privacy areas. The privacy area to which zoom threshold is applied will be marked as '[Zoom]' in the list of privacy areas. The color set in the camera's image screen is used to display the privacy area.

Setting a privacy area (except for a zoom or PTZ camera)

1. Select **[Enable privacy area]** and click **[OK]** in the confirmation dialog.
2. Drag the mouse on the camera video screen to set the privacy area.
3. In the **[Privacy area]** window, set the following:
   - Enter the name of the privacy area in **[Name]**, select the color to cover the image in **[Color]**.
4. In the **[Privacy area]** window, click **[OK]**.
5. A new privacy area is added to the list of privacy areas. The color set in the camera's image screen is used to display a privacy area.

Note

- When entering the name of a privacy area, you can enter only English letters, numbers, dash (-), and period (.).

Changing a privacy area

- You can change the size of a privacy area by moving a corner of the privacy area.
- To create a polygon (N-gon), first select and create a quadrilateral. When a [+] sign appears, click it to add another point. You can add up to 4 additional points to create a polygon of your choice.
- To delete a vertex, hover over the vertex you want to delete. Then the [-] sign appears on the point. Clicking the [-] sign deletes the vertex.
- To move a privacy area, click and drag the relevant area with the mouse.

Deleting a privacy area

1. Select a privacy area to delete from the list of privacy areas. The selected area is displayed on the camera's image screen.
2. Click **[Delete]** to delete the selected area.

Changing the order of privacy areas

You can change the order where each privacy area is saved.

1. Click **[Order]**.
2. In the **[Order]** dialog box, select a privacy mask area to change its order, and then select an option you would like.
   - Click **[Top]** to move to the very first order.
   - Click **[Up]** to move to the previous order.
   - Click **[Down]** to move to the next order.
   - Click **[Bottom]** to move to the last order.
3. Click **[OK]** in the **[Order]** dialog.

Video rotation

If the screen is displayed upside down after installing the camera, you can correct this using the flip mode and mirror mode functions.

Note

- If you change the video rotation setting, the video will be flipped in four directions or changed. To help you analyzing the changed video and accumulate the statistics, change the analysis and statistics setting. The settings can be changed in the [Analytics] and [Statistics] menus. (Some camera models do not support [Analytics] or [Statistics].)

Flip

Select **[On]** to flip the camera image upside down.

Mirror

Select **[On]** to mirror the camera image.

Audio setup

You can connect a microphone and speaker to a network camera and listen to the sound at a remote location where the camera is installed, or output audio from the camera to the location. When you complete the setting, click **[Apply]** at the bottom of the page.

Audio in

You can input audio into an image through a microphone connected to the camera. Input audio by selecting a source that fits the usage environment.

Source

Select an audio input type. (Supported options may vary depending on camera specifications.)

- **Internal microphone**: This is the internal microphone included with the camera.

Codec

Select an audio codec. (Supported options may vary depending on camera specifications.)

- **G.711**: An ITU standard audio codec that uses 64 kbps pulse code modulation (PCM) voice coding, enabling digital voice transmission over PSTN or through PBX.
- **G.726**: An ITU audio codec that uses Adaptive Differential Pulse Code Modulation (ADPCM) voice coding to compress 64 kbps PCM to variable bit rates of 40/32/24/16 kbps.
- **AAC**: Short for Advanced Audio Coding, AAC is the international standard that succeeds MP3. It enables the use of audio of a higher sampling rate than is the case when using the previous G.711 and G.726 codecs.
- **OPUS**: A royalty-free, open-source lossy audio codec. The [OPUS] codec is not supported when audio is input from IOBox to the camera. Additionally, if it is set to the OPUS codec, audio won't be recorded when you record on the SD card or NAS.

Sampling rate

This refers to the number of samplings per second when an analog sound source is converted to a digital sound source; as this value is higher, the sound quality is better. The sampling rate is fixed for each audio codec, and cannot be changed by the user. The sampling rate of the G.711 and G.726 codecs is 8 kHz, while the sampling rate of the AAC codec and OPUS codec is 16 kHz.
(Supported [Codec] options may differ depending on the camera specifications.)

Bitrate

This value represents the compression ratio of audio data. Settings differ depending on the codec. The bitrate of the G.711 codec and OPUS codec is 64

kbps and cannot be changed. The bitrate of the G.726 codec is 16, 24, 32 and 40 kbps; the compression ratio can be changed. Only 48 kbps can be selected for the AAC codec. (Supported [Codec] options may differ depending on the camera specifications.)

Gain

Sets the amplification value of audio in. If the input sound is too low, you can increase the gain value to amplify the input audio signal. The range of gain value is from 1 to 10; a larger value means higher amplification.

Noise reduction

Select Noise Reduction if the surrounding noise is too strong to hear the sound of interest.
Noise reduction may not work properly if noise is indistinguishable from the surrounding voice sound, or if the sound pressure is high.

- **Sensitivity**: You can set the noise reduction sensitivity based on the level of ambient noise.

Audio out

You can output audio through the built-in speaker.

Gain

Set the amplification value of audio out. If the output sound is too low, you can increase the gain value to amplify the output audio signal. The range of gain value is from 1 to 10; a larger value means a louder audio out.

> **Note**
>
> - The maximum sound pressure level supported varies depending on the camera's power supply method (PoE or DC 12V). As a result, the actual output sound level may differ based on the power environment, even if the same gain value is set.
>   - PoE: Up to 81 dB at 1 m distance
>   - DC 12V: Up to 84 dB at 1 m distance

> **Note**
>
> - If an excessive audio level or gain value is set, a deterioration of sound quality or a howling sound may occur.

Auto audio out gain

Analyzes the noise level of the surrounding environment and automatically adjusts the audio output volume.

Calibration

Measures the ambient noise.

- **Manual**: Click the **Manual** button to measure the ambient noise.

- **Auto**: Automatically measures the ambient noise at the interval set in **[Period]**.

Period

Set the interval at which to measure the ambient noise. (1 to 24 hours, configurable in 1-hour increments)

Results

Displays information about the measured noise.

- **Ambient noise**: Displays the measured noise level (unit: dB).
- **Calibrated gain level**: Displays the volume value automatically adjusted based on the measured noise environment.
- **Last calibration**: Displays the time of the last noise measurement. (YYYY-MM-DD HH:MM:SS)

Equalizer

You can optimize sound quality by adjusting the characteristics of each frequency band of the speaker output.

Preset

You can select a preset value configured for each purpose.

- **Flat**: Sets all frequency bands to 0 and outputs the original sound as-is.
- **Bass Boost**: Boosts the low frequency bands to enhance bass.
- **Mid Boost**: Boosts the mid frequency bands around 1 kHz to make the human voice clearer.
- **Treble Boost**: Boosts the high frequency bands to enhance clear and sharp sounds.
- **Custom**: The user manually adjusts each frequency band. (Setting range: -12 to 12)

Health check

Diagnoses whether the microphone and speaker connected to the camera are operating normally.

Check

Checks the operation of the microphone and speaker.

- **Manual**: Click the **[Manual]** button to immediately check the microphone and speaker.
- **Auto**: Periodically checks the device status according to the configured schedule.

Schedule

Set the day of the week and time to perform automatic checks.

- **Daily**: Performs a check every day at the set time (HH:MM).

- **Weekly**: Performs a check every week on the set day of the week and time (HH:MM).

Results

Displays the check results.

- **Last checked**: Displays the time of the last check. (YYYY-MM-DD HH:MM:SS)
- **Status**: Shows the check result.
  - Microphone and speaker are functioning properly
  - Microphone error
  - Speaker error
  - Failed to generate test tone

> **Note**
>
> - The status check function operates normally in environments where ambient noise is 70 dB or lower.

Audio clip

You can register or delete an audio clip file. You can also set up the schedule to play the audio clip only at a specific time.
You can upload up to 5 audio clips. If the total number of audio files added reaches 5, or the maximum allowed capacity is exceeded, the **[Upload]** and **[Record]** buttons will be deactivated.
You need to click **[Apply]** after file registration to display the audio file in the audio clip list on the **[Live]** or **[Event rule]** page.
After registering your audio clips, you can set a clip of your choice to be triggered by an event or play the clip by selecting it while monitoring camera video on the **[Live]** screen.

Upload

Register an audio file. The supported file formats are .wav and .mp3. (Some cameras support only .wav format.)
Click **[Upload]** and select a file to upload. Then the file will be added to the list.

> **Note**
>
> - Sampling rate of 48,000 kHz or less is recommended.
> - For bits per sample (bps), 8/16 bit is recommended.
> - Only PCM (process control monitoring) data is supported.

Record

Recorded audio can be registered as an audio clip.

Recording audio

1. Click **[Record]**.
2. In the **[Record]** dialog, do the following:
   1. Enter a name for the audio clip file in the **[Name]** field. You can enter up to 63 characters including English letters (a-z, A-Z) and numbers (0-9). If you click

[Start] and **[Stop]** without entering a file name, "myRecording" will be auto-filled in the box.
2. Click **[Start]** to start audio recording.
3. To stop recording, click **[Stop]**. Then the time available for recording and the length of the recorded audio are displayed.
4. Click **[Play]** to listen to the recording. The audio pre-listening feature works regardless the set gain value since the pre-listening is played on the PC.
5. Upon completion of the recording, select the audio clip file type in **[Format]**. The audio clip is generally recorded in .wav format. If you select **[MP3]**, it may take a while to convert the .wav file to .mp3 format.

3. In the **[Record]** dialog, click **[OK]**.

Note

If audio recording does not work, check the following:

- Check if your camera web viewer is connected using HTTPS secure connection mode. To access using the HTTPS secure connection mode, select **[Network]** > **[HTTPS]**> **[Secure connection system]** and then select **[HTTPS (Use a secure connection)]**.
- Check if your microphone is properly working in your PC.
- Check if your browser allows access to the microphone.

There's no session timeout during the recording of an audio clip.

Delete

After selecting the radio button of a clip to delete in the audio clip list, click **[Delete]** to delete the selected audio clip.

Audio clip list

Displays the list of registered audio clips.
To select a clip, click its radio button.

- **Name**: You can check or edit the name of the audio clip. You can enter up to 63 characters including English letters (a-z, A-Z) and numbers (0-9).
- **Play**: Plays and previews the audio file.
- **Gain**: Set the audio output amplification value. If your sound output is not loud enough, you can raise the gain value to amplify the audio signal output. The higher the value, the louder the audio output.
- **Download**: Download an audio clip file.

Schedule

You can set the schedule for your registered audio clips to play automatically.
You can set a different schedule for each audio clip.
You need to register an audio clip first to activate the **[Schedule]** option.

Setting the schedule for audio clip playback

1. Select an audio clip from the audio clip list to play it at a specific time.
2. Check the **[Enable]** box under **[Schedule]**.
3. Specify the time to play.
   - If you want to play it daily at a specific time, select **[Daily]** and the specific time you want.
   - If you want to play it on a day of the week at a specific time, select **[Weekly]** and the specific day of the week and time you want.

Camera setup

You can change the camera settings to capture the best image in the environment where the camera is installed. Image presets suitable for various environments are provided by default; you can also specify camera settings directly. You can check on the camera preview screen how the camera image is displayed according to the settings. When you complete the setting, click **[Apply]** at the bottom of the page. If the time-out time (240 seconds) has passed without clicking **[Apply]** after changing the setting, the previous setting will be restored.

Comparison view

You can see the videos of before and after changing camera video setting values all at once in the **[Before]** and **[After]** panels.

Sensor mode

Set how many frames per second the CMOS sensor of the camera will capture.

> **Note**
>
> - Changing the sensor mode will reset the whole camera setting. (Depending on camera specifications, settings may not be reset.)
> - Sensor mode value cannot be set differently for each image preset. Frame rate applies identical to all image presets.
> - The maximum value of **[Basic]**>**[Video profile]**>**[Frame rate]** varies according to the number of frames set for the sensor mode.
> - Any changes to the Sensor mode options are equally applied to all the other channels.
> - The [50 fps] or [60 fps] options under sensor mode can be selected only when **[Backlight]** mode is set to **[Off]**. (Available sensor mode options may vary depending on the camera specifications.)
> - If **[Backlight]** is set to [WDR] under **[Image preset mode]** > **[User preset]**, the **[Sensor mode]** cannot be set to [50 fps] or [60 fps] in that user preset. (Available sensor mode options may vary depending on the camera specifications.)

Image preset mode

Various image presets are provided for specific purposes. Select an image preset that best suits your camera environment. (Supported options may vary depending on camera specifications.)

- **User-defined preset 1**: Used for displaying the image as you set.
- **User-defined preset 2**: Used for displaying the image as you set.
- **Outdoor daytime**: Used to display a clear and smooth video taken outdoor in daytime.
- **Outdoor night time**: Used to reduce the level of noises for video taken outdoor at night with low brightness and lighten up dark areas.
- **Indoor backlight**: Used to display a video where indoor and outdoor are both identifiable with indoor backlight.
- **Indoor bright scenes**: Used to provide clear picture quality and reduce flickering in an illuminated indoor environment.
- **Number plates**: Used to improve the ability to identify the license plate of a car in daytime and at night.

- **Vivid video**: Used to improve color and clarity.

> **Note**
>
> - After selecting an image preset mode, change the detailed settings of camera image, such as white balance and night/day modes, and click **[Apply]** to save the changed value as the image preset value. To reset it to default, click **[Reset]**.
> - When **[User preset]** is selected and **[Backlight]** is set to **[WDR]**, **[Sensor mode]** cannot be set to [50 fps] or [60 fps]. (Available sensor mode options may vary depending on the camera specifications.)
> - If **[Sensor mode]** is set to [50 fps] or [60 fps], setting **[Backlight]** to **[WDR]** in **[User preset]** disables the corresponding preset. (Available sensor mode options may vary depending on the camera specifications.)

SSDR

SSDR is a function that improves the visibility of dark areas by increasing the brightness of dark areas in environments where there is significant contrast between dark and bright areas.

SSDR

To use SSDR, select **[Enable]**.

Shadow level

You can adjust the shadow level.
Increasing the level enhances the characteristics of shadows but also increases noise in shadows of the video.
To adjust the shadow level, the SSDR feature must be enabled. Select **[Enable]** in **[SSDR]**.

Highlight level

You can adjust the highlight level.
Increasing the level enhances the characteristics of highlights but also increases noise in highlights of the video.
To adjust the highlight level, the SSDR feature must be enabled. Select **[Enable]** in **[SSDR]**.

D-Range

Select the amplitude area of the dynamic range.

- **Narrow**: The camera's default mode which prioritizes image quality.
- **Wide**: A mode that improves discrimination. It darkens the bright area to visualize the saturated area clearly and brightens the dark area to improve discrimination. Setting the mode as **[Wide]** improves discrimination on videos with similar brightness levels, but may decrease their expressiveness.

White balance

You can make corrections to show the color white correctly and other colors normally, in any lighting environment.

Mode

Select the white balance mode according to the environment where the camera is being used. (Supported options may vary depending on camera specifications.)

- **Manual**: You can adjust red gain and blue gain manually. If more red color is shown, lower the red gain, and if more blue color is shown, lower the blue gain. If more green color is shown, raise both the red and the blue values.
- **ATW**: Corrects the camera color automatically.
- **NarrowATW**: Auto-corrects camera color in 2800 K ~ 9000 K environment. **[ATW]**The color temperature range is narrower than Mode.
- **Outdoor**: The colors of the camera are corrected to be optimized for an outdoor environment.
- **Indoor**: Correction is made to optimize colors for an indoor environment.
- **AWC**: Screen correction is made to optimize the colors for the current lighting environment. When you aim the camera at white paper and click **[Set]**, the red gain and blue gain will be adjusted and applied to the image. The white balance value continues to be applied to the currently displayed video. If the environment changes, this should be adjusted again.
- **MERCURY**: Screen correction is made to optimize the colors for the mercury lighting environment.
- **SODIUM**: Screen correction is made to optimize the colors for the sodium lighting environment.

Red gain

Adjust the red gain. If the red gain is high, more red color is shown on the screen. If too much red is shown, lower the red gain.

Blue gain

Adjust the blue gain. If the blue gain is high, more blue color is shown on the screen. If too much blue is shown, lower the blue gain.

> **Note**
>
> - In any of the following cases, white balance may not operate normally. In such case, adjust the white balance through the **[AWC]** mode.
>   - If the surrounding environment exceeds the color temperature correction range, such as a clear sky or sunset
>   - If the surrounding environment is dark
>   - If the camera faces directly toward a fluorescent light or if there is a significant illumination change.

Backlight

An image captured against the light can be corrected. Select from among Off, BLC, HLC, or WDR in **[Mode]** and change the setting according to the selected backlight mode.

BLC

The BLC (Back Light Compensation) mode selects and corrects a specific area on a dark image captured against the light, to show an object in a selected area more clearly.

BLC level

Move the slide bar to adjust the BLC level. The higher the level, the brighter the set area.

HLC

The HLC (High Light Compensation) mode blocks strong lighting such as a streetlight or the headlights of a vehicle, to prevent failures to detect a neighboring object, such as a car license plate, due to saturation of strong lights.

HLC level

Set the level of exposures and adjust the highlight areas.
The higher the level, the higher the correction and the bigger the difference is for highlight-blocked area.

Mask

Select whether or not to apply the mask.

- **Off**: Does not create blocked area.
- **On**: Always blocks areas of brightness above a certain level.
- **Night only**: Blocks areas until it gets really dark.
- **All day**: Blocks areas except during very bright or dark time.

Mask color

Sets the color of the blocked area.

Mask tone

Sets the tone of the blocked area.

> **Note**
>
> - At night, it only operates when the size of a highlight goes over the threshold in a dark environment.
> - At night, HLC does not operate when it is overall too bright or dark. In daytime, HLC does not operate when it is too dark.
> - When setting up HLC, there are minimum and maximum sizes to prevent malfunction of HLC.

WDR

The WDR (Wide Dynamic Range) mode shows both a dark area and a bright area clearly in a backlight environment. This method captures once with a fast shutter to show a bright area clearly and again with a slow shutter to show a dark area clearly, using the dual shutters of the camera, and then combines only the parts shown clearly from the two images into one image. If the WDR mode is used, noise may occur between the bright area and the dark area.



WDR mode off



WDR mode on

WDR level

Adjusts the intensity of backlight correction.

WDR control

Sets the WDR action option. (Supported options may vary depending on camera specifications.)

- **Always on**: the WDR mode is enabled at all times.
- **Turn off in low light**: The WDR mode is automatically turned off in a low-light environment.
- **Turn off in B/W**: The WDR mode is automatically turned off when the B/W mode operates.

Motion artifact reduction

If **[Enable]** is selected, motion artifacts are reduced that occur during the process of composing moving objects in WDR video.

> **Note**
>
> - When WDR mode is selected, the shutter value will be reset. The screen will become bright and then become dark.
> - When WDR mode is used, the frame rate is reduced by half.
> - It is recommended to use the WDR mode when a camera is installed indoor and there is very strong backlight.
> - If the WDR mode is used, noise may occur between the bright area and the dark area.
> - If the WDR mode is used, noise may occur in the motion detection area.
> - Please turn off the WDR mode because, depending on the lighting condition in WDR mode, the following problems could occur:
>   - When there are unnatural color changes and/or unnatural symptoms on the screen.
>   - When there is noise on the bright part of the screen.
> - The WDR performance may vary depending on the size of bright areas on the screen, so adjust the installation angle properly for the best WDR performance.
> - If you set the WDR level too high, the screen may exhibit unnatural symptoms.

Exposure

Change the exposure according to the environment of the camera. If the background is darker than the subject, the subject will be shown normally only when the exposure is decreased. Conversely, if the background is brighter than the subject, the subject will be shown normally only when the exposure is increased.

Brightness

The brightness of the screen can be adjusted. The higher the number, the brighter the screen.

Minimum shutter

The shutter can set the sensor exposure automatically according to the environment; the electronic shutter operates at a range of between minimum shutter and maximum shutter. Minimum shutter means the minimum value of the possible range for exposure time and sets a long exposure time.
If the selected minimum shutter value is smaller than the fps value of **[Sensor]** mode, the frame rate can be reduced in the dark.

Maximum shutter

Maximum shutter means the maximum value of the possible range for exposure time and sets a short exposure time.

Prefer shutter

Set the proper exposure time that has a high priority in operation within the range of exposure time.

Anti flicker

Prevents screen flickering that occurs due to inconsistency in the lighting in the capturing environment.

Anti flicker shutter speed

Set the shutter speed to prevent flickering. The available values for the anti flicker shutter speed vary depending on the settings configured in the [Sensor mode] and [Anti flicker].

SSNR

Remove noise from the image. (Supported options may vary depending on camera specifications.)

- **On/Off**: Sets whether or not to use the SSNR function. When **[On]** is selected, the SSNR level can be adjusted.
- **WiseNR**: When a moving object is in the image, the noise reduction level is adjusted automatically to improve object discrimination.
- **WiseNRII**: When there is a movement of a person or vehicle in the image, it will automatically adjust the noise reduction level to reduce the tailing effect of moving objects to improve distinction.

SSNR 2D level

SSNR 2D reduces noise on the image using adjacent pixels in one frame. Set the SSNR 2D level. The level can be set when **[On]** or **[WiseNR]** is selected for

[SSNR].
Noise will be reduced when you raise the level, but the picture may become less clear.

SSNR 3D level

SSNR 3D reduces noise on the image using the pixels of various frames. Set the SSNR 3D level. The level can be set when **[On]** or **[WiseNR]** is selected for **[SSNR]**.
The higher the level, the less the noises, but then the video might lag.

AGC

AGC (Auto Gain Control) adjusts the brightness by controlling the sensitivity of image gain when capturing an object in dim light.

- **Off**: Disables the AGC function that brightens dark image by amplifying gain from video signal.When this option is selected, **[SSNR]** and **[Day/Night]** do not work.
- **Manual:**: Manually adjusts the AGC value.
- **Max gain**: Sets the max gain that can be auto-controlled depending on the brightness of the surrounding.

Level (Manual)

Sets the AGC level value manually as desired. The higher the level value, the higher the gain value, which results in a brighter screen even in a dark environment.
If **[Manual]** is selected under **[AGC]**, **[Level (Manual)]** is enabled.

Level (Max gain)

Sets the max gain value. : Controls the max gain that is set based on the brightness of the surrounding. The higher the level value, the higher the max gain.
[Level (Max gain)] is enabled if **[Max gain]** is selected under **[AGC]**.

> **Note**
>
> - The screen exposure can be saturated depending on the max/min range of shutter settings.
> - It may take a while until the effect is applied or canceled after setting the WiseNR mode (SSNR 2D and SSNR 3D).
> - The level of noise might go up despite the improved video detection ability after setting the WiseNR mode (SSNR 2D and SSNR 3D).
> - In the bright environment with less noises, the effect of WiseNR (SSNR 2D and SSNR 3D) can be little.
> - Since the motion detection function is used internally when the WiseNR (SSNR 2D and SSNR 3D) is enabled to detect motion in video, it is detected according to the operational condition of motion detection event. For the detailed motion detection settings, go to **[Analysis]** > **[Motion Detection]**.
> - As the usage of AGC increases, the SSNR 3D value for SSNR also increases, which could lead to stuttering in the video.
> - AGC action increases screen noise.
> - If AGC mode option is set to **[Off]** or **[Manual]**, or if [Max gain] value is set to below 30 db, **[Day/Night]** cannot be set to **[Auto]**.

Day/Night

Change the image to color or b/w according to the camera's environment.
When the dwell time is set, the image can be changed to color or b/w according to preference.
When switching to Day/Night, a motion detection event or image analysis event cannot be detected.

Mode

Selects the mode which changes the camera to color or b/w. (Supported options may vary depending on camera specifications.)

- **Color**: Outputs an image in color.
- **B/W**: Outputs an image in b/w.
- **Auto**: Switch to color mode during the daytime and b/w at night or in low light.
  However, if **[AGC]** under **[Exposure]** is set to **[Off]** or **[Manual]**, or if **[Max gain]** is set below "below 30 dB", **[Day/Night]** cannot be set to **[Auto]**.
- **External**: When an alarm input terminal is linked with external equipment, color and b/w can be controlled.
- **Schedule**: Day/Night is changed to the schedule set from **[Activation time (Color)]**.

Dwell time

Changes to color or b/w when **[Auto]** is selected for Day/Night and the brightness condition is maintained for the set dwell time.

Duration

Sets the time interval when switching to color or b/w occurs.
When **[Customize]** is selected, you can manually set the ambient brightness level that determines the Day/Night mode switching threshold within a range of 0-100. The left slider with the Sun icon sets the threshold for switching from b/w to color, while the right slider with the Moon icon sets the threshold for switching from color to b/w. Entering a lower value in the left input field causes the image to switch to color in brighter conditions, while entering a higher value in the right input field causes the image to switch to b/w in darker conditions. The sliders are only active when [Day/Night mode] is set to [Auto]. If the [Level(Max gain)] value under [Exposure] > [AGC] is set below 30 dB, or if [AGC] is set to [Off] or [Manual], the sliders will be disabled and [Day/Night mode] will automatically switch to [Color].

Alarm input

Set the image to color or b/w according to the opening and closing status of the alarm sensor.

Activation time (Color)

Sets the schedule for operation in color mode. When **[Everyday]** is selected and the time is set, color mode is activated at the relevant time every day, and b/w mode is activated at all other times. If you wish to not have color mode set for the same time every day, you can deselect **[Everyday]** and set the activation time to Mon., Tue., Wed., Thu., Fri., Sat. or Sun., respectively.

Note

- When switching between night and day modes, the motion detection event will not take place. In other words, even if you 'Enable' the motion detection event, it will not detect when switching between night and day modes occurs. You can enable or disable the motion detection event in **[Analytics]** > **[Motion Detection]**.

Special

You can adjust an image for sharpness, contrast, color level, etc.

DIS

When the camera is shaking due to external impacts, such as wind, DIS (Digital Image Stabilization) corrects the video automatically and stabilizes the screen.

Sharpness

Adjust the overall sharpness of the image.

Sharpness level

Adjust the overall sharpness of the image. You can set the sharpness level by setting **[On]** for **[Sharpness]**.
The higher the sharpness level is, the stronger and clearer the video sharpness is.

Gamma control

When set to **[On]**, the brightness distribution of video is analyzed and its brightness level is adjusted.

Gamma

Adjust the contrast of the image. This means the gap between the brightest part and the darkest part in an image; a higher gamma value means a clearer display of the difference in brightness.

Contrast

Adjust the shade contrast of the image.

Contrast adaptive level

Adjust the contrast difference that will be applied in the video. This option enhances the contrast by preventing the distribution of specific brightness levels from being skewed in the 4x4 divided areas. In environments with many dark areas, highlights become brighter, increasing the contrast difference, while in environments with many bright areas, shadows become darker, also increasing the contrast difference. Moreover, in environments with both dark and bright

areas, highlights become brighter, shadows become darker, and the contrast difference increases.
As the **[Contrast adaptive level]** increases, the contrast intensity increases, and as the level decreases, the contrast intensity decreases.
In low-light environments, setting the **[Contrast adaptive level]** value to 2 - 50 may result in less noticeable effects. Therefore, you need to be careful when adjusting settings in low-light environments.

Local contrast

Local contrast feature maintains the overall brightness difference (global contrast) of the video while amplifying subtle contrast differences by making brighter areas brighter and darker areas darker within small regions, such as tree textures, faces, and floor patterns.
This feature enhances delicate textures and surface details, making fine boundaries and patterns that were previously hard to see more visible. As a result, the video appears more realistic and vivid.

Local contrast level

To enable, set **[Local contrast]** to **[On]**.
Increasing the local contrast level enhances texture. However, it may also create unnatural white or black borders around object edges, making the image look rough. In low-light conditions, video noise becomes more visible and can reduce image quality.

Color level

Adjust the intensity of color in the image.

Chromatic aberration correction

You can enable or disable the **[Chromatic aberration correction]** feature.
Chromatic aberration is a phenomenon where colors are separated due to differences in refractive index based on the wavelength of light through the lens, which can result in unexpected colors, such as purple, appearing along the edges of objects. If this phenomenon occurs in the lens, it can be improved through chromatic aberration correction.

> **Note**
>
> - Depending on the focus distance of the object being captured, the effect of chromatic aberration correction may not be noticeable in environments where chromatic aberration doesn't occur.
> - When an object has thin borders in primary colors, its color may seem washed out or faded due to chromatic aberration.
> - The higher the chromatic aberration correction level, the more noticeable the phenomenon of color removal may be.
> - Colors may be excessively removed depending on the distribution or size of the color components. Therefore, it is not recommended to use the chromatic aberration correction function in environments with many thin borders of primary colors outdoors, such as lawns.

Correction level

You can adjust the chromatic aberration correction level. A higher value applies more correction.
This option is enabled only when you select **[Chromatic aberration correction]** > **[On]**.

Defog

Correct the image when it is foggy or cloudy. When **[Auto]** is set, the surrounding environment is detected and the image is corrected automatically. When **[Manual]** is set, you can see the surrounding environment and set the correction level directly. (Supported options may vary depending on camera specifications.)
The default value is set to **[Off]**.

Defog level

Activated when **[Manual]** is set for **[Defog]**; it adjusts the defog level. A higher defog level displays the image more clearly. If the fog level is low and a high defog level is set, the screen may look darker.

> **Note**
>
> - If you set the Defog mode to **[Auto]**, as the amount of fog decreases, the level of defog function is also lowered. If you want to maintain the same effect of the function despite a decrease in the fog, then set the Defog mode to **[Manual]**.
> - If the fog level is low and a manual high defog level is high, the screen may look darker.

OSD

Display the camera title or the date and time, and set the location, size, color and transparency of the characters.

Camera title

Sets whether or not to display the camera title. When **[Enable]** is selected, the **[Add]**/**[Delete]** buttons will be activated.
When you click the **[Add]** button, a field where a camera title can be entered will be added to the list.
The initial position of the camera title is the top-left corner of the video screen. Moving the orange cursor to the desired position changes the location of the camera title on the video screen. (For some cameras, clicking **[Add]** adds a camera title field for entering a title and X,Y coordinate fields for positioning.)
To preview how the camera title is displayed on the screen after entering it, enter the camera title and click **[Preview]**.
Up to 5 camera titles can be added.
To delete a camera title, select the title to delete and click **[Delete]**.

Date & Time

To display the date and time on the screen, select **[Enable]**. To display the days of the week, select the check box under **[Weekday overlay]**. Select the date format in **[Format]** and set its location on the preview video screen. (For some

cameras, you can set the coordinates where the date and time are displayed in the **[X]** column and **[Y]** column.)

System info

To display the IP address of the camera and MAC information on the screen, select each corresponding item. The location of the IP address and MAC information can be moved using the cursor.

Size

Adjust the size of OSD.

Color

Set the color of OSD.

Transparency

Set the transparency of OSD.

Overlay image

You can display the image you want on the screen. Use the **[Upload image]** menu to upload images.

Upload image

[...]button can be clicked to search files in bitmap format. Click **[Upload]** to upload image files. To delete image files applied to the screen, click **[Remove]**. Image file should be 16 bits (RGB565 not supported), 24 bits, or 32 bits bitmap file. Image size can be up to 300 x 300 px and file size should be no more than 400 KB.
For certain cameras, the image specifications may vary. The image file should be an 8-bit bitmap (RGB565 is not supported). The image size can be up to 288 x 288 pixels (width must be a multiple of 32, and height must be a multiple of 4), and the file size should not exceed 400 KB.

Note

- In case of the item with a location that can be adjusted (camera title, date & time, overlay image, and system info), if it overlaps with other fixed OSD items, the screen may fail to display it properly. (Some cameras do not support **[Overlay image]** or **[System info]** option.)

LED light

Mode

Configure the detailed settings of the LED light that only emits white light.
If you select **[Supplement light]** or **[Light alarm]**, you cannot change the mode under **[Day/Night]**. (Supported options may vary depending on camera specifications.)

- **Supplement light**: Use the LED light as a supplement light. Then, the **[Light alarm]** option will be disabled.
  - **Auto**: Detects screen brightness and switches the LED light on and off automatically. When the ambient environment becomes darker, the LED light lights up; when the ambient environment becomes brighter, the LED light goes out. For the LED light to light up or go out, the environmental change must remain longer than the time you set in **[Minimum duration]**.
  - **Schedule**: Only turns on the LED light during the scheduled time.
- **Light alarm**: Use an LED light as a light alarm that emits light when the set event occurs. You can set the event settings in **[Event]**>**[Event rule]**.
  - **Constant**: Keeps the LED light on during the time you set in **[Duration]** when the event occurs.
  - **Flashing**: Flashes the LED light every 0.5 seconds for the time set in **[Duration]** when the event occurs.
- **Off**: Disables the LED light feature.

Duration

This option is enabled when you select **[Mode]**>**[Light alarm]**.
Set the duration of LED lighting or flashing. Then the LED light will stay on or flash during the set duration.

Level

When you select **[Supplement light]** or **[Light alarm]** under **[Mode]**, set the brightness of the LED light. The larger the number, the brighter the LED light.

> **Note**
>
> - If the LED light works as a supplementary light:
>   - The LED light may not be turned off if the surroundings does not get brighter enough. It is recommended you set the amount of time when to turn on the LED light.
>   - If the camera is installed in a dark indoor environment or in a shady area, the LED may not go out even during the day.
>   - The light alarm may not go off even if the event occurs.
> - If the LED light works as a light alarm:
>   - If the mode is set to **[Flashing]**, the screen brightness may be unstable since flashing is designed to warn pedestrians.
>   - If the light alarm runs while the camera mode is b/w mode, the LED light alarm may start flashing late or the video screen may be unstable due to camera auto-adjustment.

Activation time

The camera always operates at a specific preset time. Set and use a desired image preset at the desired time.

Off

The camera operates at the time selected in the image preset.

Only scheduled time

You can execute a desired image preset at a specific time. Select an image preset and set the start and end time. Set the image preset for each hour according to the usage of the camera.
The date from Sunday to Saturday, based on the current camera time, is displayed on the time table shown when **[Only scheduled time]** is selected. You can set the time by clicking or dragging on the time table with the mouse. The set activation time is executed repeatedly on the relevant weekday and time.
You can change the time view unit by clicking **[1 min]**, **[30 min]** or **[1 h]**. When you click **[Reset]**, all set event activation times will be deleted. To confirm or change the camera time, refer to **[Basic]**>**[Date & Time]**.

WiseStream

WiseStream effectively reduces data size while maintaining video quality by analyzing the complexity of the video.
WiseStream primarily operates based on motion detection. If there is minimal motion in the camera video, it increases the compression rate to reduce the size of the video data and save bandwidth. When motion is detected again, it reverts to the original state to prevent loss of video data.
If an AI app is installed on the camera, the **[AI-based WiseStream]** option becomes available. **[AI-based WiseStream]** operates based on the areas for AI object detection. In short, if the size of the area with objects detected is small, it increases the compression rate to reduce the size of the video data and save bandwidth. If the size of the area increases, it reverts to the original state.

Mode

You can choose how much to compress the video with WiseStream.

- **Off**: Does not use the WiseStream feature.
- **Low to High**: Select the degree of bitrate reduction to apply using the WiseStream feature.

> **Note**
>
> - The **[WiseStream]** feature can be set for camera channels, not by profile.
> - **[WiseStream]** only works when **[Codec]** is set to **[H.264]** or **[H.265]** and **[Bitrate control]** is set to **[VBR]**. You can set the **[Codec]** and **[Bitrate control]** options in **[Basic]** > **[Video profile]**.
> - When the **[AI-based WiseStream]** option is not used, the occurrence of a screen transition (such as large movements directly in front of the camera) may result in more severe image quality degradation (e.g., block noise) compared to video without [WiseStream] applied.
> - When the **[AI-based WiseStream]** option is used, areas where objects are not detected may experience relative image quality degradation (e.g., block noise).

DDNS

If you use DDNS (Dynamic Domain Name Service), you can set the IP address of the camera to be changed to a general host name which can be easily remembered by the user. If the IP address of the camera is 198.160.0.100, you can connect to the camera by entering a host name such as http://ddns.hanwha-security.com/camera1 instead of the IP address. It is convenient since the user can connect to the camera with the DDNS address even if the IP address of the camera is changed.
The exclusive Wisenet DDNS for Hanwha Vision or public DDNS can be used for DDNS. Enter the desired DDNS information and click the **[Apply]** button at the bottom of the page. If the connection to the selected DDNS is made, 'Successful' message will be displayed, and if the connection is not made, 'Failed' message will be displayed.

Note

- To use the DDNS service, the setup of port forwarding for the DDNS and the router need to be done together.
- For the port forwarding setup method for the router, see the instruction manual shipped together with the product.
- When UPnP discovery funtion is enabled, DDNS cannot be used. UPnP discovery will be activated when the **[UPnP discovery]** option is set to **[Enable]** on **[Network]**>**[Auto IP configure]**.

DDNS

Off

Select if you wish not to use DDNS.

Wisenet DDNS

Select when you use DDNS server provided by Hanwha Vision. To use Wisenet DDNS, sign up for the membership at the Wisenet DDNS homepage (http://ddns.hanwha-security.com) and register the product at **[My DDNS]**> **[Register Product]**.

- **Server**: Enter DDNS server name which you intend to use.
- **Product ID**: Enter ID of the product registered on Wisenet DDNS server. If **[Quick connect]** is selected when a router which supports the UPnP (Universal plug and play) function is used, it supports automatic opening of the port in case of connection from the outside.

Note

- If the router does not support the UPnP function or to use DDNS server without using **[Quick connect]**, set manual for the port forwarding of the router. For the port forwarding setup method for the router, refer to the instruction manual included in the product.

Public DDNS

Select it when you use DDNS server provided by a public website. Use it after signing up for the service at the relevant website.

- **Server**: Select public DDNS server which you intend to use.
- **Host name**: Enter a host name registered on DDNS server.
- **Username**: Enter the user name for DDNS server.
- **Password**: Enter the password for DDNS server.

IP & MAC filtering

You can allow or deny access for a specific IP and MAC and add IP and MAC addresses to give or block access. IPv4 and IPv6 addresses are managed separately.

Filtering mode

You can choose whether to block or allow access to specific IPs or MAC addresses. If you change the filtering mode, all previously registered IP or MAC addresses will be removed. For example, if you select **[Block]**, register an IP or MAC address, and then select **[Allow]**, all IP or MAC addresses previously registered for access restriction will be removed from the list.

- **Block**: Access is restricted for the registered IP or MAC. Add IP or MAC addresses for which you want to block access.
- **Allow**: Access is only granted to the registered IP or MAC. Add IP or MAC addresses for which you want to allow access. The IP address (either IPv4 or IPv6) of the device currently accessing the camera is auto-filled, and can be removed if desired.

IPv4

You can add or delete IPv4 addresses. Up to 10 IP addresses can be added.

Adding IPv4 addresses

1. Click **[Add]**.
2. In the **[Add]** dialog, enter the following details:
   - **IP**: Enter the IPv4 address. You can only enter numbers from 0 to 255 and the '.' symbol.
   - **Prefix**: A value that determines the scope of the IP. The prefix ranges from 1 to 32.
   - **Filtering range**: The filtering range is auto-filled based on the provided IP address and prefix.
3. Click **[OK]**.

The IPv4 type IP address is registered. Only the IP selected in the **[Use]** column will be activated.

Deleting IPv4 addresses

1. Select an IPv4 address to delete and click **[Delete]**.
2. In the confirmation dialog, click **[OK]**. Then the IPv4 address will be deleted.

IPv6

You can add or delete IPv6 addresses. Up to 10 IP addresses can be added.

Adding IPv6 addresses

1. Click **[Add]**.
2. In the **[Add]** dialog, enter the following details:
   - **IP**: Enter the IPv6 address. You can only enter the hexadecimal number, ranging from 00 to FF and the ':' symbol.

- **Prefix**: A value that determines the scope of the IP. The prefix ranges from 1 to 128.
- **Filtering range**: The filtering range is auto-filled based on the provided IP address and prefix.

3. Click **[OK]**.

The IPv6 type IP address is registered. Only the IP selected in the **[Use]** column will be activated.

Deleting IPv6 addresses

1. Select an IPv6 address to delete and click **[Delete]**.
2. In the confirmation dialog, click **[OK]**. Then the IPv6 address will be deleted.

MAC

You can add or delete MAC addresses. Up to 10 IP addresses can be added.

Adding MAC addresses

1. Click **[Add]**.
2. In the **[Add]** dialog, enter the MAC address in the box. You can enter numbers (0-9), characters (a-f, A-F), and symbols (: , -). The length of a MAC address is 17 characters, and the format would be "XX:XX:XX:XX:XX:XX" or "XX-XX-XX-XX-XX-XX".
3. Click **[OK]**.

The MAC address is registered in a format of "xx:xx:xx:xx:xx:xx". Only the MAC enabled in the **[Use]** column will be activated.

Deleting MAC addresses

1. Select a MAC address to delete and click **[Delete]**.
2. In the confirmation dialog, click **[OK]**. Then the MAC address will be deleted.

HTTPS

You can select a secure connection system or install a public certificate.

Secure connection system

Select an appropriate secure connection system in consideration of the security level. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) sends and receives data through the process of encoding/decoding users' page requests over SSL sub layer under hypertext transport agreement layer. Therefore, this mode is safer than HTTP mode in terms of security.

HTTP (Do not use a secure connection)

Select this to send data without HTTP encryption.

HTTPS (Use a secure connection)

Select this to connect in HTTPS secure connection mode.

Certificates

A list of registered certificates is displayed. Select the certificate to use for HTTPS connection.
Certificates can be registered in **[Network]**>**[Certificate management]**, and only certificates with non-encrypted key files are displayed on the list.

Change host name

Selecting **[Change host name]** option changes the camera's host name to the common name in the certificate. Some security check tools may see that the product's security is vulnerable if the camera's host name is different from the common name set in the certificate.
You can view the host name under **[Basic]**>**[IP & Port]**>**[IP address]**>**[IPv4 setup]**>**[Host name]**.
[Change host name] can be set only when **[Device certificate]** is selected in **[Certificates]**.

Mutual authentication

To proceed with mutual authentication for enhanced security, select**[Mutual authentication]**.
As you proceed with mutual authentication, you can choose an option for allowing access.

- **[Allow all connections]**: All access attempts that tried mutual authentication are allowed for connection regardless of the success/failure of mutual authentication. This means that even without mutual authentication, camera access is granted.

- **[Allow only mutually authenticated connections]**: Camera access is granted upon the success of mutual authentication only.
- **[Allow only mutually authenticated connections (including Device ID authentication)]**: Access is allowed only when the client's device ID information is verified and certified to verify integrity of mutual authentication.

[Mutual authentication] can be set only when **[Device certificate]** is selected in **[Certificates]**.

TLS settings

Sets Cipher mode or TLS version to use for encrypted communication.

Cipher mode

Provides cipher suites by combining various algorithms to use for TLS-encrypted communications, such as key exchange, authentication, and encryption.

- **Secure cipher suites only**: Uses only cipher suites with a high level of security.
- **All compatible cipher suites**: Uses cipher suites for backward compatibility although less secure. **[All compatible cipher suites]** includes both secure and not secure cipher suites.

Version

Selects the TLS protocol version to use for encrypted communication.

CORS policy

CORS (Cross-Origin Resource Sharing) allows web pages to access resources from different origins. By selecting **[Same origin only]** and clicking **[OK]**, the server will only allow requests coming from the same origin and block requests from different origins. If you select **[Same origin only]**, you need to restart the web service, causing the web page to refresh in the process.
If you select **[Same origin only]** under **[CORS policy]**, the camera may not be compatible with some VMSes.

802.1x

You can select whether or not to use the 802.1x protocol when connecting to a network, and install the certificates. When you complete the setting, click the **[Apply]** button at the bottom of the page.

IEEE 802.1x setup

IEEE 802.1x

To use IEEE 802.1x protocol for connecting to the network, select **[Enable]**. IEEE 802.1x is a part of the network protocol group called IEEE 802.1 and is the IEEE standard regarding port-based Network Access Control (PNAC). IEEE 802.1x is mainly used for reinforcing security in a wireless LAN (Wi-Fi) environment.

EAP Type

EAP (Extensible Authentication Protocol) is a protocol that allows easier extension using the authentication method defined by wireless network and Point-to-Point Protocol. It is recommended to be used only in an environment where EAP-TLS, PEAPv0/MSCHAPv2 cannot be used since LEAP is an insecure authentication method.

- **EAP-TLS**: EAP-TLS (Transport Layer Security) carries out mutual authentication that requires a client certificate with the server; a dynamic WEP key is used for security after connection is made.
- **LEAP**: LEAP (Lightweight Extensible Authentication Protocol) does not require certificates and uses only a dynamic WEP key, so a strong password should be used.
- **PEAPv0/MSCHAPv2**: PEAP/MSCHAPv2 (Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) authentication performs authentication based on the ID and password of user through an EAP-TLS session generated from the server-side authentication only.

EAPOL version

Select **[1]** or **[2]** for the version of the **[EAPOL]** (EAP over LANs) used in the network switch.

ID

Enter your client certificate ID for **[EAP-TLS]** and enter your user ID for **[LEAP]** and **[PEAPv0/MSCHAPv2]**.

Password

Enter your client private key for **[EAP-TLS]** and enter your user password for **[LEAP]** and **[PEAPv0/MSCHAPv2]**. This is not necessary if an unencrypted key is used in **[EAP-TLS]**.

Note

- If the connected network equipment does not support 802.1x, it may not operate properly even if **[Enable]** is set for 802.1x.

Certificates

CA certificates

Select the CA certificate you want from the certificate list.
The CA certificate displayed is the one registered in **[Network]**>**[Certificate management]**>**[CA certificate]**.

Client certificate

Select the client certificate you want from the certificate list. The client certificate is a certificate created/applied and used by users.
The client certificate displayed is the one registered in **[Network]**>**[Certificate management]**>**[Client certificate]**.

QoS

QoS (Quality of Service) is the function that sets the priority of data transmission and secures the data transmission quality according to set priorities when overload (simultaneous traffic increase, network failure, etc.) occurs on the network. A QoS IP address can be entered in IPv4 or IPv6. When you finish the setting, click the **[Apply]** button at the bottom of the page.

IPv4

A QoS IP address can be added or deleted in IPv4. The default values are 32 for Prefix and 63 for DSCP.

- **Prefix**: This value can set the IP range, and a value from 1 to 32 can be set in IPv4.
- **DSCP**: The QoS priority is DSCP (Differentiated Services Code Point). A value of 0 to 63 can be set for the DSCP value; as the value gets closer to 0, the priority becomes lower.

Adding an IPv4 address

1. Click the **[Add]** button. A field where an IPv4 address can be entered will be created.
2. Enter the IP, Prefix and DSCP information.
3. QoS can be applied to the relevant IPv4 address only after the **[Use]** check box is selected.
4. Clicking the **[Apply]** button at the bottom of the page will save all information added to the list.

Deleting an IPv4 address

1. Select an IPv4 address you wish to delete.
2. Click the **[Delete]** button.
3. Click the **[OK]** button on the delete confirm window. The IPv4 address will be deleted.

IPv6

A QoS IP address can be added or deleted in IPv6. The default values are 128 for Prefix and 63 for DSCP.

- **Prefix**: This value can set the IP range; a value from 1 to 128 can be set in IPv6.
- **DSCP**: The priority for QoS is DSCP (Differentiated Services Code Point). A value of 0 to 63 can be set for the DSCP value; as the value gets closer to 0, the priority becomes lower.

Adding an IPv6 address

1. Click the **[Add]** button. A field where an IPv6 address can be entered will be created.
2. Enter the IP, Prefix and DSCP information.
3. QoS can be applied to the relevant IPv6 address only after the **[Use]** check box is selected.
4. Clicking the **[Apply]** button at the bottom of the page will save all information added to the list.

Deleting an IPv6 address

1. Select an IPv6 address you wish to delete.
2. Click the **[Delete]** button.
3. Click the **[OK]** button on the delete confirm window. The IPv6 address will be deleted.

SNMP

SNMP (Simple Network Management Protocol) is a network management protocol which can collect information from the equipment on the network, and manage the network. When you finish the setting, click the **[Apply]** button at the bottom of the page.

SNMP v1/v2c

SNMP v1 protocol is not encrypted and has almost no security function. It also tends to use excessive bandwidth, so if there is much equipment, it may be difficult to manage the network. An algorithm has been added to SNMP v2c protocol for data and authentication security, allowing for more efficient bandwidth than with SNMP v1.

SNMP v1/v2c

To use SNMP v1/v2c, select **[Enable]**.

Read community

Enter the read-only community name to access SNMP information.

Write community

Enter the write-only community name to access SNMP information.

SNMP v3

SNMP v3 authentication has stronger security than v1 and v2c; transmission without data transformation is possible. The packet is also encrypted to block unauthorized users from accessing data.

SNMP v3

To use SNMP v3, select **[Enable]**.

Password

Set the user password for SNMP v3. Passwords must be between 8 and 16 characters. The default password is weak, so changing it to a new password is highly recommended immediately after installing the product. Users are responsible for security and other issues due to continued use of the default password.

> **Note**
>
> - To use SNMP v3, the 'Secure connection system' needs to be set to '[HTTPS]' mode. Go to **[Network]** > **[HTTPS]**> **[Secure connection system]** and then select **[HTTPS**

(Secure connection mode using a unique certificate)] or **[HTTPS (Secure connection mode using the public certificate)]**.

- To use SNMP v3, the 'Secure connection system' needs to be set to '[HTTPS]' mode. Go to **[Network]** > **[HTTPS]**> **[Secure connection system]** and then select **[HTTPS (Use a secure connection)]**.
- Failure to use SNMP v3 may result in security issues.

SNMP traps

The SNMP traps is a function that delivers specific events in the equipment on the network to the management system.

SNMP traps

To use SNMP traps, select **[Enable]**.

Community

Enter the name of the trap community that receives the message.

IP address

Enter the IP address of the user sending the message.

- **Authentication failure notification**: Set whether or not to deliver an event to the management system when community information is incorrect.
- **Network connection notification**: Set whether or not to deliver an event to the management system when the disconnected network is reconnected.

Setup

Configure SIP settings.
SIP (Session Initiation Protocol) is used for VoIP calls. You can make calls with users using a network intercom with SIP enabled.
SIP setup supports two methods: P2P and PBX server. Use the P2P method when users communicate directly on the same network and there is no need to use features provided by a PBX server. Use the PBX server method when communicating with users both inside and outside the IP network.
Once the setup is complete, click the **[Apply]** button at the bottom of the page.

Enable SIP

Enable SIP

Select **[Enable]** to activate the SIP function. When a call request event occurs while the function is activated, it attempts to connect to the VoIP client via the configured SIP.

> **Note**
>
> - To use the SIP call function, both the account and recipient must be configured.

Allow incoming SIP calls

If you select **[Enable]**, a VoIP client can request an SIP connection to connect to the camera. When a VoIP phone requests a connection while incoming calls are allowed, the camera sends the video via the SIP connection. Connections from all users are allowed regardless of whether a recipient is registered.

> **Note**
>
> - To use this function properly, the camera's SIP account must be configured and connected to the server.

Port setup

You can set the port to use for the SIP service.

SIP port

Enter the port number to activate the SIP service. The port is used in P2P mode.
The setting range is 1024 to 65535, and the default value is 5060.

SIP TLS port

Enter the port number to activate the SIP TLS service. The port is used in P2P mode.
The setting range is 1024 to 65535, and the default value is 5061.

RTP start port

Enter the start number of the RTP port to use when connecting media.
The setting range is 1024 to 65535, and the default value is 4000.

> **Note**
>
> - Port setup is only activated when **[Enable SIP]** is selected.
> - If the configured RTP start port is already in use, a port of 4000 or higher is selected randomly.
> - Ports 3702 and 49152 are used by the system and cannot be used as SIP ports.

NAT traversal

NAT traversal is used if the intercom camera is connected to the network behind the NAT router. You can set detailed options for the camera's SIP connection inside NAT.
An STUN server and a TURN server should be installed in advance.
If the connection cannot be made with the camera installed inside NAT, setting STUN, TURN, and ICE allows you to connect to the camera video.

ICE

Determines the priority of connection candidates collected using the STUN service.
To use ICE, STUN must also be enabled.

STUN

Collects the intercom's IP, NAT's IP and public IP for P2P connection.
Select **[Enable]** to use the STUN server.

Server address

Enter the STUN server address. You may enter up to 63 characters, including alphabet, numbers, and the following special characters: -, . / _ :

TURN

Provides relay connection in an environment where a P2P connection is unavailable.
Select **[Enable]** to use the TURN server.

Server address

Enter the TURN server address. You may enter up to 63 characters, including alphabet, numbers, and the following special characters: -, . / _ :

Username

Enter the ID to access the TURN server. You can enter up to 31 characters, including alphabet, numbers, and the following special characters: ~`!@$^()_-|{}[];,./?

Password

Enter the password to access the TURN server. You can enter up to 31 characters, including alphabet, numbers, and the following special characters: ~`!@$^()_-|{}[];,./?

Advanced

Auto UDP-TCP switch

Select **[Enable]** to temporarily auto-switch the transfer protocol from UDP to TCP.

Contact rewrite

Select **[Enable]** to automatically update the transfer address and contact information header for a register request if the change in the public IP address is detected.

Call duration limit

Select **[Enable]** to set the maximum length of SIP call time. If the specified maximum call time exceeds, the call ends automatically.
Even if the call duration limit option is disabled, the call will automatically end after the maximum setting time of 60 minutes for system protection.

Maximum

Enter the maximum length of SIP call time. It is enabled only if you select **[Enable]** for **[Call duration limit]**.

Registration interval

Sets the interval of attempting to register to the registrar server.
If the camera requests for registration to the SIP server but fails to register, it tries to request for registration again to the SIP server according to the interval set in **[Registration interval]**. On registration failure, the retry is performed after adding the 'failure detection time' and the 'configured registration interval'. For example, if the detection time is 60 seconds and the configured value is 300 seconds, a retry will be attempted 360 seconds after the initial request.

Audio direction

You can select between a two-way call or a one-way call.
If **[Send and receive]** is selected, the call becomes two-way communication that sends and receives a call. If you select **[Receive only]** or **[Send only]**, the call becomes one-way communication that only receives or sends a call.

Account

You can register, modify, or delete accounts used in SIP.
If you change the account setup, the SIP will be terminated and restarted.
Once the setup is complete, click the **[Apply]** button at the bottom of the page.

Account list

You can check the name, ID, server address, type, and connection status of the currently configured accounts. Click the **[Refresh]** button to renew the account list.
When the connection is successful, "Available" is displayed along with the connected server address (Peer-to-Peer displays the camera IP). When the connection fails, "Unavailable" is displayed along with the domain name.
Among the added accounts, only the account selected in the **[Use]** column is used for SIP communication. Only one account can be selected from the registered accounts, and a newly registered account is automatically activated.

> **Note**
>
> - At least one account must be registered in the system, and a maximum of five accounts can be registered.
> - A Peer-to-Peer account is automatically created when the camera is assigned an IP.
> - To delete a Peer-to-Peer type account, at least one account must be registered, and the camera must be factory reset to recreate it after deletion.
> - Modifying the account settings will restart the SIP connection.

Adding an account

1. Click the **[Add]** button.
2. Enter information related to the account from the **[Add account]** dialog box. You can enter up to 31 characters using letters, numbers, and special characters (* ~`!@$^()_-|{}[];,./?).
   - **Name**: Enter the name of the new SIP account. You can enter 1 to 20 characters using letters, numbers, and special characters (~`!@$^()_-|{}[];,./?).
   - **User ID**: Set the same ID as the Authentication ID. You can enter 1 to 31 characters using letters, numbers, and special characters (~`!@$^()_-|{}[];,./?).
   - **Authentication ID**: Enter the ID to log in to the domain server. You can enter 1 to 31 characters using letters, numbers, and special characters (~`!@$^()_-|{}[];,./?).
   - **Password**: Enter the password to log in to the domain server. You can enter 1 to 31 characters using letters, numbers, and special characters (~*`!@#$%()^_-+=|{}[].?/).
   - **Domain name**: Enter the server name that the SIP account has access to. You can enter 1 to 63 characters using letters, numbers, and special characters (-.:).
3. Enter additional information by clicking **[Advanced setup]** in the **[Add account]** dialog box. You do not need to enter all the information below.
   - **Caller ID**: The ID of the caller displayed to the recipient after the call connects. You can enter 1 to 31 characters using letters, numbers, and special characters (~`!@$^()_-|{}[];,./?).
   - **Backup domain name**: Enter the backup server that you will access if there is an error in the domain server. You can enter 1 to 63 characters using letters, numbers, and special characters (-.:).
   - **Registrar address**: Enter a registrar server if there is an additional registrar server. You can enter 1 to 63 characters using letters, numbers, and special characters (-.:).
   - **Backup registrar address**: Enter the server that you will access if there is an error with the registrar server. You can enter 1 to 63 characters using letters, numbers, and special characters (-.:).

- **Transport mode**: Select the transport protocol that the SIP is using. You can select UDP, TCP, or TLS.
- **Proxy address**: Enter a proxy server if there is a proxy server. You can enter 1 to 63 characters using letters, numbers, and special characters (-.:).

4. Click the **[OK]** button in the **[Add account]** dialog box.

If communication is possible as the account registration information is successfully registered to the server, **[Available]** will be displayed in the **[Status]** column of the account list.
When adding an account, enter the **User ID**, **Authentication ID**, **Caller ID**, and **Domain name** fields in compliance with RFC3621 Section 19.1 and 25.1.

Modifying an SIP account

1. Select an item to modify from the **[Name]** column.
2. Change the information you want in the **[Add account]** dialog box and click the **[OK]** button.

If you modify the account setup, SIP is reconnected.

Deleting an SIP account

1. Select an item to delete from the **[Select]** column.
2. Click the **[Delete]** button.

Video profile

You can check the current setup information of the VoIP-specific video profile information. If no VoIP profile is set up, “No profile set” message is displayed. You can set the video profile information in **[Basic]**>**[Video profile]**.

Note

- If you delete a profile or change the settings during a video call, the video call will be terminated.

Recipient

You can set the recipients of an SIP Call.
Once the setup is complete, click the **[Apply]** button at the bottom of the page.

Call request

Call request

You can select a call request mode. You must first set a recipient in **[Recipient list]** before the **[Call request]** option is activated.

- **Single**: You can set one person from the recipient list as the recipient, and a call request will be sent to the specified recipient.
- **Group (Parallel forking)**: You can set a recipient group from the recipient list as the recipient, and a call request will be sent to all recipients in the specified group.

Test call

Test call

You can test whether the call settings are configured correctly. The result is displayed in one of three states: Failed, Succeeded, or Calling. The status information disappears 10 seconds after the test call.
Make sure to enable SIP and enter all call settings, account, and recipient information before running the test call. If the SIP setup is not complete, the test result will be displayed as failed. SIP activation and call settings can be configured in the **[Network]** > **[SIP]** > **[SIP Setup]** menu, account information in the **[Network]** > **[SIP]** > **[Account]** menu, and recipient information in the **[Network]** > **[SIP]** > **[Recipient]** menu.

Recipient list

You can add, change, or delete SIP call recipients.
Duplicate entries with the same name or SIP address cannot be configured. Also, if your own account ID is set as a recipient, single calls are not available, and that recipient will be excluded during group calls.

Group

You can only check the group selected from the list. For example, if you select **[1]**, you can filter and see only the list of recipients assigned to Group 1.

Adding a recipient

You can add up to 30 recipients and assign up to 10 recipients to each group.

1. Click the **[Add]** button.
2. Enter the following in the **[Add recipient]** dialog box.
   - **Name**: Enter the name of the recipient. You can enter 1 to 20 characters, including alphabet, numbers, and special characters (~`!@$^()_-|{}[];,./?).
   - **Type**: Select the SIP address type.

- **SIP address**: Enter the SIP address. You can enter 7 to 100 characters, including alphabet, numbers, and special characters (~`!@$^()_-|{}[];,./?).
  - If **[Registrar]** is selected for **[Type]**, enter in the format “sip:UserID@Domain”.
  - If **[Peer-to-peer]** is selected for **[Type]**, enter in the format “sip:IP address”.
- **Group**: To assign to a group, select the desired group. Select **[None]** to add as an individual recipient.

3. Click the **[OK]** button in the **[Add recipient]** dialog box.

Modifying recipient information

1. Select an item to modify from the **[Name]** column.
2. Change the desired information in the **[Add recipient]** dialog box and click the **[OK]** button.

Assigning a recipient to a group

You can assign a recipient to a group or change the assigned group. A recipient can be assigned to multiple groups.

- To assign a recipient to a group, select the group to assign the recipient to from the **[Group]** column.
- To exclude a recipient from a group, deselect the group from the **[Group]** column.

Deleting a recipient

- To delete only the selected recipient, select the item to delete from the **[Select]** column and click **[Delete]**.
- To delete all recipients at once, click **[Delete all]**.

DTMF

You can add or delete DTMF codes.
DTMF codes are used by SIP devices to remotely unlock a door or trigger specific events using DTMF (Dual-Tone Multi-Frequency) signaling.

DTMF

Enable DTMF code reception

If **[Enable DTMF code reception]** is selected, the DTMF code reception function configured in **[Code]** is activated. When a configured DTMF code is received, the action preset in the event rule is performed. Event rules can be configured in the **[Event]** > **[Event rule]** menu.
You can register and manage up to 10 DTMF codes.

Adding a DTMF code

1. Click the **[Add]** button.
2. Enter a name to identify the DTMF code in the **[Name]** field. You can enter 1–20 characters, including letters, numbers, and special characters. Spaces are not allowed.
3. Enter the digits to be input via the actual phone keypad in the **[Code]** field. Only numbers with up to 4 digits can be entered.
4. Click the **[OK]** button.

Deleting a DTMF code

1. Select the checkbox of the code you want to delete from the code list.
2. Click the **[Delete]** button.

Audio codecs

Configure the audio codecs to use in SIP calls.
After completing the settings, click the **[Apply]** button at the bottom of the page.

Audio codecs

Audio codecs

You can view the list of codecs supported by the SIP device and configure whether to use them.
Selecting a checkbox in the list enables the corresponding codec.
The supported audio codecs and sampling rates are as follows.

- PCMU(8000/1)
- PCMA(8000/1)
- opus(48000/2)
- G722(16000/1)
- L16(44100/1)

Setting audio codec priority

Codecs positioned higher in the list have higher priority. You can optimize call quality and bandwidth by adjusting the order of the enabled codecs.

- **[Up]**: Increases the priority of the selected codec by one level.
- **[Down]**: Decreases the priority of the selected codec by one level.

Auto IP configure

You can set the camera IP automatically. You can assign an IP address that can connect to an additional camera on the same local network or set the camera IP to check for a camera connected to the network on Windows or Mac OS. When you finish the setting, click the **[Apply]** button at the bottom of the page.

Link-Local IPv4 address

You can assign an additional IP that can connect to a camera from the same local network.

Auto configure

To use auto configuration of a Link-local IPv4 address, select **[Enable]**.

- **IP address**: The assigned IP address is displayed.
- **Subnet mask**: The subnet mask of the assigned IP address is displayed.

UPnP discovery

You can search for a camera automatically from clients and OS that support the UPnP (Universal Plug and Play) protocol.

UPnP discovery

To use UPnP discovery, select **[Enable]**.

- **Friendly name**: The camera name is displayed. The friendly name is displayed in order of WISENET - model name - MAC address.

Bonjour

You can search for a camera automatically from clients and OS that support the Bonjour protocol. Connected cameras are displayed on the Bonjour bookmark of the Safari web browser on Mac OS, which supports Bonjour by default.

Bonjour

To use Bonjour, select **[Enable]**.

- **Friendly name**: The camera name is displayed. The friendly name is displayed in order of WISENET - model name - MAC address.

Certificate management

You can add or delete certificates. You can manage CA certificate and client certificate separately.
CA certificate is signed by the Certificate Authority (CA), and client certificate is created, applied, and used by person.

Client certificate

You can install or delete a user certificate. If you have a certificate file and key file, you can register the certificate. You can also create a certificate file by filling out the certificate information.
Our device certificate is provided by default, which cannot be deleted. Clicking the button ⓘ shows the certificate information.

Adding a client certificate

1. Click **[Add]**.
2. If you have a Client certificate file, select **[Client]** from the **[Type]** options in the **[Add certificate]** dialog, and perform the following:
   - **Name for the certificate**: Enter the certificate name. You can enter up to 31 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space cannot be used.
   - **Certificate file**: Click [...] and select the certificate file.
   - **Key file**: Click [...] and select the auth key file.
3. If you want to create a certificate manually, select **[Self-Signed]** from the **[Type]** options in the **[Add certificate]** dialog, and perform the following: A certificate can also be created simply by filling out the required fields marked with an asterisk (*).
   - **Name for the certificate**: Enter the certificate name. You can enter up to 31 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space cannot be used.
   - **Common name (CN)**: Enter the common name of the certificate. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only *_-[.). A blank space also can be used.
   - **SAN**: Enter the certificate subject alternative name (SAN) information. You can enter up to 198 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only *_-[.,). A blank space cannot be used.
   - **Valid thru**: Select the expiry date of the certificate.
   - **Country (C)**: Enter the country information. Only two alphabet letters are allowed.
   - **State/Province (ST)**: Enter the state or province information. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space also can be used.
   - **Organization (O)**: Enter the organization information. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space also can be used.
   - **City/locality (L)**: Enter the locality information. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space also can be used.
   - **Organizational unit (OU)**: Enter the information on the organization unit. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only _-[]). A blank space also can be used.
   - **E-mail**: Enter the e-mail address. You can enter up to 63 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (only ~!@_-[],.?). A blank space cannot be used.
4. If you have a certificate file in PKCS #12 format, select **[PKCS #12]** from the **[Type]** options in the **[Add certificate]** dialog, and perform the following:
   - **Name for the certificate**: Enter the certificate name. You can enter up to 31 characters, including English uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and special characters (only _-]), but no spaces.
   - **Certificate file**: Click [...], then select a certificate file. You can only upload a *.p12 or *.pfx extension.

- **PKCS#12 password**: Enter the password to use when decrypting files in p12 or pfx format. If it is entered incorrectly, the file will not be created. Leaving it blank will proceed without a PKCS#12 decryption key.
- **Private key passphrase**: A password used to encrypt the private key extracted from the PKCS#12 file. If you enter no value and leave it blank, it is generated unencrypted.

5. In the **[Add certificate]** dialog, click **[OK]** to save the entered information in the list.

Deleting a client certificate

1. Select the client certificate to delete.
2. Click **[Delete]**.

CA certificate

You can install or delete a CA certificate. CA certificate is issued by the Certificate Authority (CA).
Our root CA certificate is provided by default, which cannot be deleted. Clicking the button ⓘ shows the certificate information.

Adding a CA certificate

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

Deleting a CA certificate

1. Select the CA certificate to delete.
2. Click **[Delete]**.

Event rule

You can create rules that make the camera perform a particular action when a specific event occurs.

Event rule

You can register detailed event rules of when the camera will perform a specific action when a specific event occurs. Also, you configure conditions for activating the event rules.

Adding event rules

After clicking the **[Add]** Button, configure the event rules in the setup window.

1. In **[Rule name]**, enter the desired name of event rules. Up to 15 characters can be entered.
2. After selecting **[Add]** in the **[Event trigger]** panel, select both the channel number where the event occurs and the trigger type to create the event.
3. Click **[Invert]** if you want the event trigger to be triggered when the event ends rather than when it occurs. For example, if you select **[Invert]** in **[Motion detection]**, the event trigger will operate as soon as the camera ends detecting motion after detecting motion. A list of sub-rules will appear for a specific trigger depending on your settings. After selecting a sub-rule, you can choose an **[Invert]** option.
4. In **[Duration]**, set up the minimum time for the event to occur before performing the action. For example, if the **[runtime]** is set to **[60]**, an event operation will be executed in case all the event triggers occur within 60 seconds.
5. In the **[Event action settings]** panel, select the desired event action to perform when an event occurs. (The supported event actions vary depending on the camera specification.)
   - **FTP**: To capture the video screen and send it via the FTP server when an event occurs, select **[Enable]**. Detailed FTP settings can be configured in **[Event]**>**[FTP/E-mail]**.
   - **E-mail**: To capture the video screen and send it via e-mail when an event occurs, select **[Enable]**. Detailed e-mail settings can be configured in **[Event]**>**[FTP/E-mail]**.
   - **Record**: To record the video when an event occurs, select **[Enable]**. Detailed record settings can be configured in **[Event]**>**[Storage]**.
   - **Handover**: When an event occurs, the receiver camera moves to a preset position or performs a specific action. Select a registered receiver camera from the dropdown list. If a name is set, the name is displayed; otherwise, the index number is displayed. When **[Off]** is selected, the handover function will not work, even when an event occurs. Detailed receiver camera settings can be configured in **[Event]**>**[Handover]**.
   - **Audio clip**: This function plays the configured audio clip when an event occurs. If you select **[Off]**, the audio clip will not play even when an event occurs. You can register an audio clip in **[Video & Audio]**>**[Audio setup]**>**[Audio clip]**.
   - **Alarm output**: To output an alarm when an event occurs, select the output time. If **[Always]** is selected, the alarm will continue to be output until it is stopped by the user. To disable the alarm when an event occurs, select **[Off]**. Detailed alarm output settings can be configured in **[Event]**>**[Alarm I/O]**.
   - **MQTT**: When an event occurs, it publishes a notification message to the MQTT client. If you want to add or edit the MQTT message to be published, go to the **[Event]**>**[MQTT]**>**[Publication/subscription]**>**[Publication]** tab.
   - **Light alarm**: An LED light constantly emits light during a time period set or flashes with an interval of 0.5 seconds when an event occurs. You can specify the settings for LED light operation in the **[Video & Audio]**>**[Camera setup]**>**[LED light]** tab.
   - **SIP**: When an event occurs, a SIP call is made. This works only if the SIP function is enabled and the account and recipient settings are configured.
6. Configure the schedule of event action from **[Activation time]**. In other words, an event action is performed only at the set time when an event occurs. It is possible to select a preset option so that an event action is performed either all the time or only during weekdays/weekends. Moreover, it is possible to configure a new event

action schedule after clicking the calendar-shaped icon.
The camera's system time can be checked in **[Basic]**>**[Date & Time]**.

7. Click **[OK]**.

Added event rules will be displayed. You can check if the event rules and their details are valid or invalid. For example, if "motion detection" is registered as an event trigger condition while the "motion detection" function of the camera is disabled, it is displayed as "invalid."

To change the event rules, double-click the rule you want from the list of event rules. When the event rules window opens, you can change the details.
To disable the event rules, select **[Off]** from the list of the event rules.

Deleting an event rule

- Select a event rule on the list and then click the **[Delete]** button.

Note

- Selecting **[Network disconnection]** in the event trigger options limits the options of event triggers and event actions that can be combined.

Handover

Handover is a function that, when an event occurs, delivers the configured action (performing an action, sending a CGI command, etc.) to the receiver camera so that the camera performs a specific action.

Receiver

You can add, modify, or delete receiver cameras. Up to 32 receiver cameras can be registered.

Adding a receiver camera

1. Click **[Add]**.
2. In the **[Add Camera]** dialog, enter the camera information to receive the handover.
   - **No.**: Set the receiver camera number.
   - **Name**: Set a name for handover identification.
   - **IP type**: Select the IP address type between IPv4 and IPv6 or select **[Domain name]** to set the camera information using a domain name.
   - **Type: Select the mode of communication among HTTP, HTTPS, and TCP.**
   - **Action**: Select the action for the receiver camera to perform when the event occurs.
     - **Preset**: Move to a specific preset position. (Can be set when **Type** is **HTTP** or **HTTPS**)
     - **Custom**: Send a request with the configured query string.
   - **Server address**: When you select **[Domain name]** in **[IP type]**, enter the domain name of the camera. You can enter up to 63 characters, including English uppercase (A-Z) and lowercase (a-z), numbers(0-9), and special characters (only.-). However, the first and last characters must be letters or numbers.
   - **IP address**: Enter the IP address of the receiver camera.
     - When you select **[IPv4]** in **[IP type]**, enter it in the format of four numbers separated by dots, ranging from 0 to 255. (However, addresses between 223.255.255.255 and 255.255.255.255 cannot be set, and addresses ending in 255 cannot be set.)
     - When you select **[IPv6]** in **[IP type]**, enter an address in the format of eight 16-bit, 4-digit hexadecimal numbers separated by a colon (:), ranging from 0 to ff (hexadecimal). Consecutive zeros can be abbreviated as a double colon (::). (The :: can only be used once in the address).
   - **Port**: Enter the port number of the receiver camera.
   - **User**: Enter the access ID to access the receiver camera.
     This can be set only when **[HTTP]** or **[HTTPS]** is selected for **[Type]**.
   - **Password**: Enter the password to access the receiver camera.
     This can be set only when **[HTTP]** or **[HTTPS]** is selected for **[Type]**.
   - **Preset no.**: Enter the preset position number to which the receiver camera will move. The preset number should be set in advance in the PTZ camera for reception. In the handover menu, enter the preset PTZ number.
     This can be set only when **[HTTP]** or **[HTTPS]** is selected for **[Type]** and **[Preset]** is selected for **[Action]**.
   - **TCP message**: Enter the message to send to the TCP recipient. This can be set only when **[TCP]** is selected for **[Type]**. You must enter at least 1 character and can enter up to 255 characters.
   - **Verification of server certificate**: Selecting **[Enable]** will verify the integrity and authenticity of the certificate sent from the server. A specific CA certificate to use for certificate verification can be selected in **[CA certificates]**.
     This appears only when **[HTTPS]** is selected in **[Type]**.
   - **CA certificates**: Select a desired certificate from the list of CA certificates installed on the camera. TLS/SSL connection is available only when selecting the CA certificate used to sign the certificate sent from the server. The indicated CA certificate is the one registered in **[Network]**>**[Certificate management]**>**[CA certificate]**.
     This can be set only when **[HTTPS]** is selected in **[Type]**.
   - **Query string**: Enter the query string of the URL. This can be set only when **[HTTP]** or **[HTTPS]** is selected for **[Type]** and **[Custom]** is selected for **[Action]**. You must enter at least 1 character and can enter up to 255 characters.

- **Info**: Displays URL complete with the entered information.

3. Click **[OK]**.

Modifying a receiver camera

1. In the receiving camera list, select the checkbox next to the camera you want to modify to select it.
2. Click the **[Modify]** button.
3. When the **[Add Camera]** dialog box appears, modify the options and then click **[OK]**.

Deleting a receiver camera

1. Click a checkbox in the list of receiver cameras, and select the camera you want to delete.
2. Click **[Delete]**, and in the confirmation dialog, click **[OK]**.

Note

- If the type is set to **[HTTP]**, the receiver camera will receive both HTTP and HTTPS. If the type is set to **[HTTPS]**, the receiver camera will only receive HTTPS.
- You cannot set the same preset number, query string, TCP message, etc. for the same IP address.

FTP / E-mail

When an event is created while the camera is capturing an image, the captured image can be sent to an FTP server or by e-mail. Also, video files can be sent to an FTP server. Enter the appropriate FTP server and e-mail configuration information to be used.
When you enter FTP server or e-mail server information and click the **[Apply]** button at the bottom of the page, an FTP server connection test or an e-mail test will be carried out. If an incorrect FTP server address or e-mail server address is entered, a message saying 'Failed' will be displayed. If the test is succesfully done, the message saying 'Successful' will be displayed

---

FTP configuration

Protocol

Select a communication protocol used for the transfer of image files when an event occurs. You can choose between the File Transfer Protocol (FTP) and the Secure File Transfer Protocol (SFTP) that is more secure than FTP.

Login type

The login-type option appears when you select **[SFTP]** in **[Protocol]**. You can choose between **[Password]** and **[Key file]** for authentication to access the server. Select **[Password]** to authenticate with your ID and password; select **[Key file]** to authenticate with a key file.

Server address

Enter the IP address for the FTP server where an event creation image will be sent. You can enter from 1 to 64 characters.

ID

Enter the ID for the FTP server login account. Special characters such as #%&+=₩:<>"' are not allowed, and you can enter from 1 to 30 characters.

Password

Enter the password for the FTP server login account. Special characters such as #%&+=₩:<>"' are not allowed, and you can enter from 1 to 30 characters.

Private key file

The private-key-file option appears when you select **[SFTP]** in **[Protocol]** and then select **[Key file]** in **[Login type]**.
Click **[Import]** to import a private key file to use for authentication to access the server. In the **[Import private key file]** dialog box, type a name in the **[Key name]** box and click **[...]** to choose a key file to import. If the key file is encrypted, select **[Enable]** in the **[Key passphrase]** area and then type the Key passphrase in the box to decrypt the file. If you close the **[Import private key**

file] dialog box, the key name that you typed in the **[Key name]** box appears in the **[Private key file]** box.
You can delete the registered private key file by clicking **[Delete]**.

Upload directory

Enter the directory of the FTP server where an event creation image will be recorded. You can enter up to 60 characters using alphabets, numbers, and/or special characters (/~`!@#$%^&()_-=+{}[];',.).

Port

Enter the port value of the FTP server. The default port value of the FTP server is 21, which can be changed according to the FTP server settings. The port can be changed within a range of 1 to 65535.

Passive mode

Select **[Enable]** when connection in passive mode is necessary due to firewall or FTP server configuration.

File type

Select the file type to be sent to the FTP server when an event occurs.

- **Image**: If **[Image]** is selected, the camera will send the captured image to FTP when an event occurs. At this point, the image file is sent with the information set in [E-mail/FTP profile]. Detailed settings for [E-mail/FTP profile] can be viewed in **[Basic]**>**[Video profile]**.
- **Video clip**: If **[Video clip]** is selected, when an event occurs, the video is sent for the set duration determined by **[Pre event duration]** and **[Post event duration]** based on the time of the event occurrence. For example, if [Pre event duration] is set to [1] second and [Post event duration] is set to [10] seconds, the video of which range includes 1 second before the event and 10 seconds after the event is sent to the FTP server based on the time of the event occurrence. So, if an event occurs at 12:30:10 PM, the video from 12:30:09 PM to 12:30:20 PM will be sent to the FTP server.
  Video clips are processed in parallel up to a maximum of 3 across the entire system. For example, if FTP, SMTP (e-mail), and handover request simultaneously, each file is created and transmitted. However, if 4 or more requests occur simultaneously, the excess requests will be processed as errors.

File name

You can preset the file name format that will be used for the file transmitted via FTP when an event occurs.
Select **[IP address]** to include the IP address in the file name. If you select **[YY]**, **[MM]**, **[DD]**, **[hh]**, **[mm]**, and **[ss]**, respectively, the file name will include the date of event occurrence, including the year, month, day, hour, minute, and second information. Also, if you select **[Rule index]**, the event rule number will be included in the file name. The channel name is automatically inserted right before the file name extension.

Select **[Enable]** to generate the file name using the format you set when files are transferred via FTP.

E-mail configuration

Server address

Enter the e-mail SMTP server address for sending an event creation image by e-mail. You can enter from 1 to 64 characters.

Verification of server certificate

Selecting **[Enable]** will verify the integrity and authenticity of the certificate sent from the email server. A specific CA certificate to use for certificate verification can be selected in **[CA certificates]**.

CA certificates

Install the CA certificate to use for email server authentication from the list of CA certificates installed on the camera. To establish a TLS/SSL connection, you must select the CA certificate that was used to sign the certificate sent by the server.

Authentication

Select whether or not to authenticate with an ID and password each time an e-mail is sent.

Encryption

Choose between **[SSL]** and **[StartTLS]** for the SMTP TLS security option. If you don't want to use SMTP TLS security, select **[None]**.

ID

Enter the ID for the login account connected to the e-mail SMTP server. Special characters such as #%&+=₩:<>"' are not allowed, and you can enter from 1 to 32 characters.

Password

Enter the password for the login account connected to the e-mail SMTP server. Special characters such as #%&+=₩:<>"' are not allowed, and you can enter from 1 to 32 characters.

Port

Enter the port value of the email SMTP server. The default port value of the email server is 25; the port value will be automatically changed and entered based on the TLS option selected in **[Encryption]** if TLS security is not set for the email SMTP server.

Recipient

Enter the email address of the e-mail recipient. You can enter from 1 to 64 characters.

Sender

Enter the email address of the e-mail sender. If the address of the sender is not correct, the intended recipient may not receive the e-mail. You can enter from 1 to 64 characters.

Subject

Enter the subject of the e-mail to be sent when an event is created. Special character ₩ is not allowed, and you can enter from 1 to 60 characters.

Message

Enter the body information for the e-mail to be sent when an event is created. When an event is created, the captured image will be sent as an e-mail attachment. Special character ₩ is not allowed, and you can enter from 1 to 255 characters.

Storage

You can select a device to capture a camera image and set the recording conditions. When you complete the setting, click **[Apply]** at the bottom of the page.

Storage action setup

Selecting a recording device and selecting **[On]** allows you to change the setting for the relevant device.
When **[On]** is set for an SD card and NAS at the same time, NAS is processed by priority.

- **SD Card**: You can set whether or not to use an SD card. When an SD card is recognized, the free space, total capacity and status are displayed. To format the SD card, click **[Format]**.
- **NAS**: You can set whether to use NAS (Network Attached Storage). When a connection to NAS is established, the free space, total capacity and status are displayed. To format the default folder on NAS, click **[Format]**.

> **Note**
>
> The **[Status]** column shows the status of the recording device.
>
> - **None**: There is no recording device, or the recording feature is inactive.
> - **Ready**: Waiting to record
> - **Recording**: Able to record
> - **Formatting**: The recording device is being formatted
> - **Full**: The recording device does not have enough free space
> - **Error**: A problem occurred, and further recording is not possible.
> - **No profile available**: The selected edge recording profile is inactive (The edge recording profile can be selected at **[Basic]** > **[Video profile]**)
> - **Profile error**: An error occurred in the selected edge recording profile (The edge recording profile can be selected in [Basic] > **[Video profile]**)
> - **Password error**: The SD card password does not match the camera's set SD card password (The SD card password can be changed in **[Encryption]**)

Overwrite

Sets whether or not to use the overwrite function of an SD card or NAS. When the device capacity has been reached, new data will be recorded over the oldest data. When the device capacity has been reached, a message saying 'Full' is displayed in **[Status]** in the device list.

Auto delete

Sets whether or not to use the auto delete function. The most recent data for the set number of days is kept and the rest will be deleted. The number of auto delete days can be set from 1 to 180. The **[Auto delete]** function is activated only when **[Enable]** is set for **[Overwrite]**.

> **Note**

- When 'Error' is displayed in **[Status]** in the device list, check whether the recording device is connected properly, whether the file system of the recording device is damaged or not, and whether the recording device is physically damaged. If the 'Error' message persists after checking the recording device, format or replace the device.
- Recording may not be possible due to temporary network disconnection when NAS is used, so it is recommended to use an SD card also.
- When resolution, bit rate and frame rate are set at high, the amount of image data also increases. If the amount of data increases, a frame skip may occur even if set to full frame. If frame skipping occurs, then at least one image is saved per second.
- Before removing the (Micro) SD card, first switch to **[Off]**. If you remove it on your own or power up the camera with a unstable source of electricity without switching to **[Off]**, it can damage the (Micro) SD card.
- If you use the (Micro) SD memory card below the recommended speed, it can cause frame skipping. If you use the (Micro) SD memory card with too large capacity, it can slow down the format speed.
- If you use NAS, auto deletion is supported only when the NAS capacity is above the recommended specifications.
- Deleted data cannot be restored.

SD File System

This menu is displayed only when **[SD Card]** is selected in the **[Device]** column of **[Storage action setup]**, allowing you to select the file system on the SD card. SD cards support VFAT and EXT4 file systems, so select the file system according to the SD card of the camera you are using. If the file system of the SD card is EXT4, Windows OS can recognize it only when a separate application is installed.

Type

Select either VFAT or EXT4 for the file system of the SD card. When the setting is changed, all existing data will be formatted. Be sure to back up data before changing the setting.

Note

- High Endurance SD Cards are recommended. For detailed information, refer to the Hanwha Vision website.
- It can take up to 10 minutes to format the (Micro) SD card with the EXT4 file system.

Encryption

SD card encryption allows you to save video data in your encrypted SD card (or microSD card). This keeps your SD card safe and secured even when you lost it. The SD card encryption option appears when you select **[SD]** for **[Device]** under the **[Storage action setup]** column.

Note

- If you change the SD card setting to encrypt or decrypt it, all of its data will be deleted and the SD card will be formatted.

SD card encryption

Selecting **[Enable]** encrypts the SD card while deselecting **[Enable]** decrypts it.

Encrypting SD card

1. Select **[Enable]** under **[Encryption]**.
2. Enter your **[New password]** in the text box, and enter the same password again in the **[Confirm new password]**.
3. Click **[Apply]** at the bottom of the page.
4. If SD card encryption is working properly, the 'Encrypted' message will appear.

Decrypting SD card

1. Deselect **[Enable]** under **[Encryption]**.
2. Click **[Apply]** at the bottom of the page. If SD card encryption is disabled, so the SD card data is not encrypted, 'Unencrypted' message will appear.

Changing password

You can change the password for SD card encryption.
If the password of the encrypted SD card and the password you entered do not match, 'Password error' message will appear in the **[Status]** column of **[Storage action setup]**.

1. Click **[Change password]**.
2. Enter the current password in the **[Current password]** text box.
3. Enter the new password in the **[New password]** and **[Confirm new password]** text boxes.
4. Click **[Apply]** at the bottom of the page.

NAS connection setup

This menu is displayed only when **[NAS]** is selected in the **[Device]** column of **[Storage action setup]** and NAS access information is entered. Enter the NAS information and click **[Test]** to check the connection. If the connection is made, a 'Successful' message appears; otherwise, a 'Failed' message is displayed.

Server address

Enter the NAS IP address or domain name.
You can enter up to 63 characters, including English uppercase (A-Z) and lowercase (a-z), numbers (0-9), and special characters (only.-). However, the first and last characters must be English letters or numbers.

ID

Enter the ID for the account registered on NAS.
You can enter up to 31 characters, including English uppercase (A-Z) and lowercase (a-z), numbers (0-9), and special characters (only_-.).

Password

Enter the password for the account registered on NAS.
You can enter up to 31 characters, including English uppercase (A-Z) and lowercase (a-z), numbers (0-9), and special characters (only~!@^*_-[]./?).

Default folder

Designate the default folder where NAS will record image data.

You can enter up to 31 characters, including English uppercase (A-Z) and lowercase (a-z), numbers (0-9), and special characters (only/_-.). For example, you can use a special character (/) as a directory separator like "Directory1/Directory2".

SMB version

Select the version of the NAS file sharing protocol.
SMB v2.0 or v3.0 shows the capacity allocated to a specific account from the total NAS capacity. However, SMB v1.0 does not support this feature, so v1.0 shows the total NAS capacity, while v2.0 or v3.0 shows only the capacity allocated to the account.

Note

- If a failure message is displayed when you test after entering NAS information, check the following items:
  - Check if the IP address, ID, password, and default NAS folder are entered correctly.
  - Check if the IP address type of NAS and the IP address type of the camera are identical. (e.g.: The default value of NAS and the camera is 255.255.255.0. If the IP address is 192.168.20.32, the NAS IP address should be between 192.168.20.1 and 192.168.20.255.)
  - For the NAS default folder, only one folder should be used in one camera, with no duplication.
  - Check if the device is recommended NAS equipment. Refer to 'Recommended NAS specifications' in the user's manual.
  - Check if the SMB version of NAS is set to 3.0. (Not applicable to some camera models.)
- If **[Overwrite]** in the storage setup for NAS is not used and the free space for NAS is less than 20%, images will be recorded on the SD card.
- If an SD card which was used in another camera is inserted while data is being recorded on NAS, images may not be recorded.
- If the NAS setup is changed while data is being recorded on NAS, the change will not apply immediately.
- If NAS equipment is removed or the network connection is terminated while data is being recorded on NAS, the NAS recording action may be terminated.
- When resolution, bitrate and frame rate are set at high, the amount of image data also increases. If the amount of data increases, a frame skipping may occur even if set to full frame rate. If frame skipping occurs, then at least one image is saved per second.
- Check if you are trying to access as another user without formatting the default folder that is saved or used already.

Record

Record setup

Edge recording profile

The name of the video profile which will be used for recording is displayed. The profile set as 'Edge recording profile' from **[Basic]**>**[Video profile]** > **[Profile type]** is displayed.

Continuous recording

Sets for normal recording with no event; Video is saved with a fixed frame rate at all times in an ordinary situation without an event.

- **None**: No camera image is recorded.
- **I-Frame**: Records I-Frame only for continuous recording.
- **Full frame**: Records full frame for continuous recording.

Event recording

Sets the recording type when an event occurs.

- **None**: No camera image is recorded when an event occurs.
- **I-Frame**: Records only I-Frame when an event occurs.
- **Full frame**: Records full frame when an event occurs.

Pre event duration

Sets the image recording time before an event occurs. An image can be recorded at 1 second, 3 seconds and 5 seconds prior to the occurrence of an event.

Post event duration

Sets the image recording time span after an event. An image can be recorded for 5 seconds, 10 seconds, 30 seconds, 60 seconds or 120 seconds after the occurrence of an event.

Record file type

Sets the file format for recording an image. When the file recording format is changed, the existing data will be erased.

- **STW**: This is the unique file type for Hanwha Vision.
- **AVI**: This is an AVI file.

> **Note**
>
> - Any changes to the Record file type options are equally applied to all the other channels.

Continuous recording schedule

You can set the time to record an image on the recording device.

Always

Always records an image on the recording device.

Only scheduled time

Records an image only at the scheduled time. The date from Sunday to Saturday, based on the current camera time, is displayed on the time table shown when **[Only scheduled time]** is selected. You can set the time for recording by clicking or dragging on the time table with the mouse. The set time is executed repeatedly on the relevant weekday and time.
You can change the time view unit by clicking **[1 min]**, **[30 min]** or **[1 h]**. When you click **[Reset]**, all set event activation times will be deleted. To confirm or change the camera time, refer to **[Basic]**>**[Date & Time]**.

Alarm I/O

The I/O port of a camera can be set either as an input or output port as desired.
After selecting it to be either an input or output port, you can set the details of each Alarm I/O.

> **Note**
>
> If you use all alarm ports as output, the **[External]** mode of **[Day/Night]** will be disabled. If it is already set to **[External]**, it will be changed to the **[Auto]** mode. You can select **[Video & Audio]**>**[Camera setup]**>**[Day/Night]** to check the External mode of Day/Night.

Alarm I/O

If **[Input]** is selected, **[Input device setup]** can be set. If **[Output]** is selected, **[Alarm output]** can be set.
The number of supported alarm inputs/outputs may differ by camera.

Input device setup

Sets whether or not to use an alarm input device and the type to activate an alarm event when an alarm input is given.

Input device setup

To use an alarm input device, select **[Enable]**.

Type

Select the alarm input type.

- **N.O. (Normal Open)**: The alarm input sensor is open by default; when it is closed, an alarm input event is created.
- **N.C. (Normal Close)**: The alarm input sensor is closed by default and when it is open, an alarm input event is created.

Alarm output

Sets how to control an alarm when an alarm is outputted by the user or when an event is created.
When changing the type of alarm output, the Alarm output button on the Live page and the type of alarm output in the Event setup are changed.

Type

Selects the alarm output type.

- **N.O. (Normal Open)**: The alarm output sensor is open by default and when it is closed, an alarm is outputted.
- **N.C. (Normal Close)**: The alarm output sensor is closed by default and when it is open, an alarm is outputted.

Mode

Sets the control type when an alarm is outputted.

- **Pulse**: An alarm is outputted for the time set in **[Duration]** and the alarm turns off automatically.
- **Active/Inactive**: When you press the alarm output button on the monitoring screen, an alarm will turn on; when you press the button again, the alarm will turn off.

Duration

Sets the alarm output time when **[Pulse]** is selected in **[Mode]**.

Time schedule

A time schedule event is a function for generating events at set intervals. When you complete the setting, click the **[Apply]** button at the bottom of the page.

Event setup schedule To use the event setup schedule, select **[Enable]**.

Transfer interval This sets the event occurrence interval. Click the drop-down menu and select a number and a unit.

> **Note**
>
> - The transfer interval should be set lower than the operation interval in the event action settings.

Device alarm

You can set alarms to go off when the network is physically disconnected or when the camera's external cover case is opened.

> **Note**
> You can change the option settings on the **[Device alarm]** page only when you are logged in as an administrator.

Device alarm

You can set whether to trigger an alarm in the event of network disconnection or the opening of the camera's case.

Network disconnection

To trigger an alarm when the network is disconnected, select **[Enable]**.

Case tampering

To trigger an alarm when the camera's external cover case is opened, select **[Enable]**.

MQTT

MQTT (Message Queueing Telemetry Transport) is a messaging protocol based on Publication/Subscription. As it is designed to transmit lightweight messages, it is ideal for connecting remote devices that require a small code space or minimal network bandwidth.
Communicating through the MQTT protocol enables the camera to easily send and receive data to and from multiple devices. For example, if a camera's client sends a notification of a camera event, multiple clients subscribing to that notification can receive it through a broker. Also, the camera's client can receive notifications from several clients and control the camera's motion. For example, you can receive a notification from another client and start recording with the camera, or you can send a notification back to another client that you received the notification.

MQTT

Enable MQTT

Select **[Enable MQTT]** to connect to the set broker.

Status

Shows the connection status to the broker. Click the refresh button to update the connection status to the broker.

Client setup

Set MQTT client information. Enter the MQTT broker information where the camera's client will be connected.
An MQTT broker brokers messages on the topic received from the publisher when a client sends a declaration to the broker that it will subscribe to the messages of a specific topic.

Address

Enter the broker's domain and IP address. **[Address]** and **[Port]** are required entries and are marked with an asterisk (*).

Port

Enter the port number to connect to the broker. **[Address]** and **[Port]** are required entries and are marked with an asterisk (*).

Username

Enter the client ID.

Password

Enter the client password.

Transport protocol

Choose between TCP, TLS, WebSocket, and WebSocketSecure.

Basepath

If using WebSocket and WebSocketSecure, you can set the basepath as well as the broker address and port. In this case, the URL of the final broker will be Address:port/basepath.

ALPN

Enter the ALPN supported by the broker.

Verification of server certificate

If connecting via TLS or WebSocketSecure, select **[Enable]** to verify a server certificate.

CA certificates

Selects the one you want from the list of certificates installed on the camera. To add a CA certificate, go to **[Network]**>**[Certificate management]**>**[CA certificates]**.

Client certificate

Selects the one you want from the list of certificates installed on the camera. To add a client certificate, go to **[Network]**>**[Certificate management]**>**[Client certificate]**.

Custom client ID

To use a client ID defined by the user when connecting to a broker, select **[Enable]** and enter the desired ID in the **[Client ID]** field. If there is no input entered in the **[Client ID]** field, it will be connected using a random ID.

Keep Alive interval

Enter the time in seconds. Checks if the broker is connected every set interval time.
If you set both **[Keep Alive interval]** and **[Connection timeout]** together, make sure to set the **[Connection timeout]** value higher than the **[Keep Alive interval]** value.

Connection timeout

Enter the time in seconds. If there is no response from the broker for the set period of time, it will be disconnected from the broker.

If you set both **[Keep Alive interval]** and **[Connection timeout]** together, make sure to set the **[Connection timeout]** value higher than the **[Keep Alive interval]** value.

Auto reconnect

If you select **[Enable]**, it will automatically try to connect every minute if the previously connected broker is disconnected.

Clean session

If **[Enable]** is selected, all information (e.g., client ID or messages designated to be retained) previously retained is to be deleted from the client and broker when connecting them. If **[Enable]** is not selected, the information remaining in the previous session is to be retained. For example, if there is a topic you subscribed to in the previous session, the client can receive messages on that topic even if you do not subscribe to it again.

Default topic prefix

Enter the default topic prefix. When setting the default topic prefix, the final topic is created by combining the default topic prefix and message topic. When additionally publishing MQTT, you can set whether to use the default topic prefix. For more information, refer to **[Event]**>**[MQTT]**>**[Publication/Subscription]**>**[Publication]**>**[Adding MQTT publications]**.

Connection message

This is the message a client sends to a broker when the connection is complete. Select an item to be used as a connection message. You can add messages in the **[Event]**>**[MQTT]**>**[Publication/Subscription]**>**[Publication]** tab.

LWT message

The LWT (Last Will and Testament) message is a message in which the broker declares in advance that it will send a message designated to a certain topic when the connection between the client and the broker is abnormally disconnected. Select an item to be used as the LWT message. You can add messages in the **[Event]**>**[MQTT]**>**[Publication/Subscription]**>**[Publication]** tab.

Publication/Subscription

MQTT (Message Queueing Telemetry Transport) is based on a publication and subscription protocol. When a publisher sends a topic and message to a broker, the broker sends a topic to the subscriber and the subscriber is subscribed to the message of the topic. Any client can be a publisher or a subscriber as it is not specified.
On the **[Publication/Subscription]** page, you can add and edit publication and subscription message items so that a MQTT client can publish and subscribe to messages on certain topics using the MQTT protocol.

Publication

Sets the MQTT topic and messages to be published. The topic and message are delivered to the client that is subscribing to a topic published.

Adding MQTT publications

1. Click the **[Add]** button.
2. Follow the steps below in the **[Add MQTT publication]** dialog box.
   - **Name**: Enter the name of the message to publish.
   - **Default topic prefix**: Select the checkbox to include the default topic prefix set when sending a message. In this case, the message is sent with the default topic prefix along with the topic. For example, if "camera" is set as the default topic prefix, and "connection" is set as the topic to publish, the message will be sent with "camera/connection" as the content. You can set the default topic prefixes in **[Event]**>**[MQTT]**>**[Client setup]**>**[Default topic prefix]**.
   - **Topic**: Enter the topic to publish.
   - **QoS**: Select the desired level for the MQTT publication.
     - 0: Clients only send a topics and messages, and clients and brokers will not proceed with any additional steps to check with the items sent from each other or to respond to them. In other words, the topic and message are sent, but the result is not guaranteed.
     - 1: A client will repeatedly send the same topic and message until a broker confirms receipt.
     - 2: It is ensured that a broker receives the same topic and message only once through the handshake between the client and the broker.
   - **Retain**: Select **[Enable]** to let a broker save the published message to send to a new subscriber that is subscribed to the topic later on.
   - **Payload**: Enter the message content to be published.
3. Click **[OK]**.

- To edit the set MQTT publication information, select the desired item, and click **[Modify]**.

Deleting MQTT publication messages

1. Select an item to delete from the MQTT publication list.
2. Click the **[Delete]** button.

Subscription

Sets the MQTT topic and messages to subscribe.

Adding MQTT subscriptions

1. Click the **[Add]** button.
2. Follow the steps below in the **[Add MQTT subscription]** dialog box.
   - **Name**: Enter the name of the message to subscribe to.

- **Topic**: Enter the topic to subscribe to.
- **Type**: Select the subscription method of the topic and a message.
  The MQTT topic can be organized in a hierarchy by separating it with slashes (/), such as "event/objectdetection/person."
  Also, wild cards can be used. Use a # to subscribe to all topics of lower levels. For example, you can subscribe to all lower-level topics such as A/B/a, A/B/a/D, A/B/b, and A/B/b/D by entering A/B/#.
  Use a + to comprehensively subscribe to topics of a certain level. For example, you can comprehensively subscribe to topics such as A/B/a/D, A/B/b/D, and A/B/c/D by entering A/B/+/D.
  - **Stateless**: An event occurs whenever a message is received from a topic that is subscribed to and the event occurrence status will be released immediately. If the subscribing message is received several times, an event will occur upon each receipt.
    For example, if you set an "on" message to subscribe in the "home/light" topic in order to trigger an event that turns on the light, the light will be turned on and then soon turned off by receiving the "on" message. If the same message is received several times, the light will be turned on and off whenever the message is received.
  - **Stateful**: When a message is received from a topic that has been subscribed to, an event will occur, and the event occurrence status will be maintained afterward. The status will be disabled if a message different from the subscribing message is received. Therefore, if subscribing messages are received continually, a new event will not occur even if you receive messages several times.
    For example, if you set an "on" message to subscribe in the "home/light" topic to trigger an event that turns on the light, the light will be turned on and the turned-on status will be maintained when you receive the "on" message. If it receives messages aside from "on," the light will be turned off. Afterward, the light will be turned on again if an "on" message is received.
- **QoS**: Select the desired level for the MQTT subscription.
  - 0: When a client sends a topic, the client and broker do not proceed with further steps to confirm its receipt.
  - 1: Send the same topic several times until the client who sent a topic receives the confirmation of its receipt.
  - 2: It is ensured that a broker receives the same topic only once through the handshake between the client and the broker.
- **Payload**: Enter the message content to subscribe to.

3. Click **[OK]**.

- To edit the set MQTT subscription information, select the desired item, and click **[Modify]**.

Deleting MQTT subscriptions

1. Select an item to delete from the MQTT subscription list.
2. Click the **[Delete]** button.

Shock detection

If a shock or vibration is detected on the camera or a change in physical position is detected, a shock detection event can be generated.

Shock detection

Enable shock detection

To enable shock detection events, select **[Enable shock detection]**.

Level of detection

Set the level value that is the basis of shock detection. If a shock is detected above the set level value, a shock event is generated.
When a shock or vibration is detected, a graph showing the shock or vibration value applied to the camera is displayed, and when a shock detection event occurs, the graph color changes.

Sensitivity

The higher the sensitivity, the more sensitive the detection level graph will be.

Motion detection

A motion detection event can be created when a motion detection area and the exclude area are set and a motion is detected from inside the area set by the user.

Motion detection

Enable motion detection

To use the motion detection event, select **[Enable motion detection]**.

> **Note**
>
> - The motion detection area and the exclude area are set and used according to the size range of the motion.
> - In any of the following cases, the performance of the motion detection event may deteriorate and a malfunction may occur:
>   - If an object is similar in brightness or color to the background on the screen
>   - If a small motion occurs near the edge of the screen
>   - If an overall change on the screen occurs continuously at random due to factors such as scene changes and sudden illumination changes
>   - If a moving object comes too close to the camera
>   - When one object hides another object
>   - When the motion of an object is too fast
>   - When reflection, blurring or shading occur due to strong light such as direct sunlight, high illumination or headlights from a vehicle
>   - In cases of severe snow, rain or wind, or sunset or sunrise.

Include area

The area designated by the user is set as the motion detection area.

Setting an area

When you select 4 corners of an image with the mouse, it is set as the motion detection area and the color of the number buttons in **[Area]** changes.
Up to 8 areas can be set and the level, sensitivity, and minimum duration can be set separately for each motion detection area.

Changing an area

You can change the size of a motion detection area by moving a corner of the motion detection area. To move a motion detection area, click and drag the relevant area with the mouse.
To create a polygon (N-gon), first select and create a quadrilateral. When a [+] sign appears, click it to add another point. You can add up to 4 additional points to create a polygon of your choice.
To delete a vertex, hover over the vertex you want to delete. Then the [-] sign appears on the point. Clicking the [-] sign deletes the vertex.

Deleting an area

To delete a motion detection area, click **[x]** at the relevant area on the screen and click the **[OK]** button on the delete confirm window.

Area

When a motion detection area is added, the color of the number buttons in **[Area]** will change. When you click the number button, the relevant motion detection area will appear from the preview screen.

Level of detection

This sets the standard level of motion detection. You can set the level for each motion detection area in **[Area]**, and when a motion is larger than the set level, a motion detection event will be created.
Also, as a motion in each area is detected, a motion graph will appear, and when a motion event is created, the color of the graph will change.

Sensitivity

This sets the motion detection sensitivity for each area. Set a lower sensitivity for an environment where the background and an object are clearly distinguishable and a higher sensitivity for an environment where the background and an object are not clearly distinguishable.

Minimum duration (s)

Minimum duration (s): Sets the minimum amount of time to trigger an event after detection. When the movement lasts longer than the set period of time, the event is triggered.

Exclude area

The area designated by the user is set as the exclude area.

Setting an exclude area

When you select 4 corners of an image with the mouse, it is set as the exclude area, and the color of the number buttons in **[Area]** changes. Up to 8 exclude areas can be set.

Changing an exclude area

You can change the size of an exclude area by moving a corner of the exclude area. To move an exclude area, click and drag the relevant area with the mouse.
To create a polygon (N-gon), first select and create a quadrilateral. When a [+] sign appears, click it to add another point. You can add up to 4 additional points to create a polygon of your choice.
To delete a vertex, hover over the vertex you want to delete. Then the [-] sign appears on the point. Clicking the [-] sign deletes the vertex.

Deleting an exclude area

To delete an exclude area, click **[x]** at the relevant area on the screen and click the **[OK]** button on the delete confirm window.

Area

When an exclude area is added, the color of number buttons in **[Area]** will change. When you click the number button, the relevant exclude area will appear from the preview screen.

Common

Sets the min and max sizes of an object to detect.

Size

Click the bottom right corner and drag the mouse to change the size. Changing the size also changes the **[Minimum]** and **[Maximum]** values under **[Size]**.

> **Note**
>
> - If the ROI and Exclude areas are identical or overlap each other, the Exclude area has priority over the other.
> - Any movement smaller than the specified minimum size or larger than the specified maximum size will not be detected. please determine the best values for the minimum/maximum detection sizes that are appropriate for the installation environment in order to avoid any false detection arising out of small and/or large noises. Remember that the same movement in the same spot does not always result in the same detection size. Therefore, it is recommended to allow small/big enough rooms for your minimum/maximum size limits in consideration of the deviation in detected sizes.

Tampering detection

A tampering detection event can be created when the screen is blocked or the camera position is changed.

Tampering detection

Enable tampering detection

To use the tampering detection event, select **[Enable tampering detection]**.

Level of detection

This sets the standard level of tampering detection. A tampering detection event is created when a tampering of the set level is detected.
Also, when a tampering is detected, a graph showing the level of tampering will appear, and when a tampering detection event is created, the color of the graph will change.

Sensitivity

Higher sensitivity results in a more sensitive response of the detection level graph.

Minimum duration (s)

This sets the minimum time to detect a tampering and create an event. A tampering detection event is created only when tampering persists for the minimum duration.

Except dark images

To exclude a sudden decrease in brightness on the screen, as such in the case of a sudden extinction of lights or blocking of lights, from the tampering detection event, select **[Enable]**.

> **Note**
>
> - The detection performance may deteriorate on a uniform background, or in a night-time, low-light environment.
> - If the camera shakes too much or if there is sudden change in light, the tampering detection may not function properly.
> - It may take up to 5 seconds for a tampering detection event to be created after a tampering occurs.
> - When a camera tampering is detected, the function will restart after stabilizing for approximately 5 seconds, and any tampering will not be detected during the stabilization process.
> - When an incorrect event is repeatedly being created, errors can be minimized by gradually lowering the level.
> - If you set the level of detection too low, then it is possible to trigger an alarm out of quite small changes on the screen, but it can also lead to false detection cause by objects in motion or change in brightness.

WiseAI

Exclude area

The **[Exclude area]** feature allows you to set an area to prevent objects from being detected in the set area. If there are two or more channels, you can set an exclude area differently for each channel.

Exclude area

List

The **[List]** shows a list of exclude areas you set.

Setting exclude areas

- On the video, create a quadrilateral around the area you want to exclude from detection by clicking 4 times.
- Then the set exclude area is created on the video and added to the **[List]**.
- You can create up to 8 exclude areas.

Changing exclude areas

- To resize the exclude area, drag a vertex to your desired position.
- To create a polygon with 5 or more sides, hover over any lines of the created quadrilateral.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex.
  - You can create polygons with up to 8 sides.
  - To delete vertices, hover over a vertex you want to delete. Then the **[-]** button appears on the point. Clicking the button deletes a vertex.
- To relocate the exclude area, drag the area to your desired position.

Deleting exclude areas

1. Hover over the row of the exclude area you want to delete in the **[List]** or click the exclude area on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the area.

Changing the names of exclude areas

- Double-click the set-area name you want to change in the **[List]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Exclude area

The metadata for the objects detected in the exclude area is not transmitted. To transmit metadata about the information and detailed properties of those objects, turn on the **[Enable object data from the excluded area]** toggle.

Object detection

The **[Object detection]** feature detects objects of the types you select.
To enable the **[Object detection]** feature, turn on the toggle at the top.
If there are two or more channels, you can set an object type to be detected and minimum duration (observation time) differently for each channel.

Object detection

Object

Select the object types to detect (person, face, vehicle, license plate). For vehicles, five subtypes are available: car, bus, truck, motorcycle, and bicycle. Multiple selections are allowed for both object types and vehicle subtypes.

Detection condition

Set the **[Minimum duration]** to set conditions to trigger an event when an object is detected. An object must stay in the camera's field of view for longer than the set minimum time to trigger an object detection event and to send the relevant data.

> **Note**
>
> False detection may occur if:
> - The brightness or color of an object is similar to the background of the screen.
> - Multiple motions occur irregularly or continuously due to scene transitions, etc.
> - A stationary object is constantly moving in the same position.
> - Various objects are randomly blocking each other (50% or more).
> - Objects are moving too quickly.
> - Strong light sources, like direct light, lamps, or car headlights, generate reflections, smearing, or shadows.
> - There is heavy snow, rain, wind, etc., or there is a sunset or sunrise.
> - A moving object is in close proximity to the camera.

BestShot & Attributes

The **[BestShot & Attributes]** feature generates the most reliable thumbnail image (BestShot) for the selected object.
If you select an object type under **[BestShot]** and then select an object type under **[Attributes]** for each channel, you can view the generated BestShot along with its properties.
To enable the **[BestShot & Attributes]** feature, turn on the toggle at the top.
If there are two or more channels, you can select the object type for its BestShot to be generated and the object type for its attributes to be displayed, differently for each channel.

BestShot

Object

Under **[Object]**, select an object type per channel (multiple selections are possible).
The BestShot for the selected object is generated with the highest reliability. The BestShot then appears on the right side of the screen on the **[BestShot & Attributes]** page.

Image encoding

You can encode the BestShot in a Base64 format and send metadata using Real-Time Streaming Protocol (RTSP). If you select **[Base64]**, the BestShot will be encoded in a Base64 format and sent as metadata using RTSP.

> **Note**
>
> Even if an object is detected according to certain conditions, the BestShot may not be sent.
> The BestShot may not be generated, or the **[BestShot]** feature may deliver poor performance if:
> - Only part of the object is photographed.
> - There are many objects, causing them to overlap each other.
> - Objects are moving too quickly.
> - A poor image quality or out-of-focus image makes it difficult to see.

Attributes

Attributes

You can view more detailed, meaningful information on each object.
Under **[Attributes]**, select an object type per channel (multiple selections are possible).
You can display both the BestShot generated according to your settings and the properties you selected.
The BestShot and its properties appear on the right side of the screen on the **[BestShot & Attributes]** page.

Line crossing

The **[Line crossing]** feature detects the objects that cross the virtual line in the direction you set. You can set which object to be detected by selecting the object type.
To enable the **[Line crossing]** feature, turn on the toggle at the top.
If there are two or more channels, you can set a virtual line and the object type differently for each channel.

Line crossing

List

The **[List]** shows a list of virtual lines you set.

Setting virtual lines

- Click on the video screen, and then click on it again where you want. Then a virtual line with the start and end points appears.
- When the line to detect objects is created, the line is also added to the **[List]**.
- You can also set the direction of the arrow on the line. To change the direction of the virtual line, click the arrow in the center of the line. Objects are counted only when they cross in the direction of the arrow, in the opposite direction of the arrow, or in both directions based on the virtual line.

Changing virtual lines

- To resize the virtual line, drag the start or end point to your desired position.
- To add a vertex to the line, hover over the line.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex. Up to six vertices can be created.
  - To create virtual lines of different shapes, drag the vertices to your desired position.
  - To delete a start or end point, or a vertex, hover over the point you want to delete. Then the **[-]** button appears. Clicking the button deletes the point.
- To relocate the virtual line, drag the line to the desired position.

Deleting virtual lines

1. Hover over the row of the virtual line you want to delete in the **[List]** or click the line on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the line.

Changing the names of virtual lines

- Double-click the set-line name you want to change in the **[List]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Object

Select the types of objects to be detected.

Specifying objects

Only selected objects that cross the virtual line are detected.

1. From the **[List]** or on the video screen, select a virtual line.
2. Under the **[Object]**, select the type of the object to be detected (multiple selections are possible).

Notes

An error may occur or the function may not work if:

- The brightness or color of an object is similar to the background of the screen.
- Multiple motions are being made irregularly or continuously due to scene transitions, etc.
- A stationary object is constantly moving in the same position.
- Various objects are randomly blocking each other.
- A single object is split into many objects, or two or more objects combine into one.
- Objects are moving too quickly.
- Strong light sources, like direct sunlight, lamps, or car headlights, generate reflections, smearing, or shadows.
- There is heavy snow, rain, wind, etc., or there is a sunset or sunrise.
- A moving object is in close proximity to the camera.
- The OSD menu of the camera is adjusted.
- An object is crossing the start and end of the virtual lines.
- The brightness of the moving object is similar to that of the point where it crosses the virtual line.

IVA area

The **[IVA area]** feature detects the entry, exit, intrusion, and loitering of objects based on detection areas you virtually set. In terms of appearance and disappearance, all objects, including the selected type of object, are detected.
To enable the **[IVA area]** feature, turn on the toggle at the top.
If there are two or more channels, you can set an IVA area differently for each channel.

IVA area

List

Displays a list of IVA area rules you set.
The list under **[IVA area]** is automatically synchronized with that under **[Appear (Disappear)]**.

Setting detection areas

- On the video, create a quadrilateral around the area you want to detect the actions of objects by clicking 4 times.
- Then the set detection area is created on the video and added to the **[List]**.

Changing detection areas

- To resize the detection area, drag a vertex to your desired position.
- To create a polygon with 5 or more sides, hover over any lines of the created quadrilateral.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex.
  - You can create polygons with up to 8 sides.
  - To delete vertices, hover over a vertex you want to delete. Then the **[-]** button appears on the point. Clicking the button deletes a vertex.
- To relocate the detection area, drag the area to your desired position.

Deleting detection areas

1. Hover over the row of the detection area you want to delete in the **[List]** or click the detection area on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the area.

Changing the names of detection areas

- Double-click the set-area name you want to change in the **[List]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Object

Select the types of objects to be detected.

> **Specifying objects**
> From the **[List]** or on the video screen, select a virtual line, and then under **[Object]**, select an object to be detected. You can select multiple object types.

Detection condition

Select any of the following actions (multiple selections are possible) if you want an object to be detected: Only when the selected type of object performs the selected action is the object detected.

- **Enter**: Triggers an event when an object of the selected type enters the detection area from the outside.
- **Exit**: Triggers an event when an object of the selected type exits from the detection area.
- **Intrusion**: Triggers an event when an object of the selected type appears in the detection area and stays there for more than the time set in **[Minimum duration]** (up to 5 seconds).
- **Loitering**: Triggers an event when an object of the selected type loiters in the detection area for more than the time set in **[Minimum duration]**.

Appear (Disappear)

List

The detection areas you set under **[IVA area]** are added to the **[List]**.
The list of the **[Appear (Disappear)]** is automatically synchronized with that of the **[IVA area]**.

Detection condition

To detect the appearance (disappearance) of objects, turn on the **[Appear (Disappear)]** toggle.
An event occurs either when an object that was not in the detection area appears and remains static for more than the time set in **[Minimum duration]** (up to 1 minute) or when an object that was static in the area disappears and does not appear until the set time has elapsed.
You can set the minimum observation time for each detection area either by clicking the detection-area row in the **[List]** or by clicking the detection area on the screen.

> **Note**
> False detection may occur if:
> - The brightness or color of an object is similar to the background of the screen.
> - Multiple motions are being made irregularly or continuously due to scene transitions, etc.
> - A stationary object is constantly moving in the same position.
> - Various objects are randomly blocking each other (50% or more).
> - A single object is split into many objects, or two or more objects combine into one.
> - Objects are moving too quickly.
> - Strong light sources, like direct sunlight, lamps, or car headlights, generate reflections, smearing, or shadows.
> - There is heavy snow, rain, wind, etc., or there is a sunset or sunrise.
> - A moving object is in close proximity to the camera.
> - The OSD menu of the camera is adjusted.

Face mask detection

The **[Face mask detection]** feature detects whether an object wears a mask and triggers a face-mask detection event.
To enable the **[Face mask detection]** feature, turn on the toggle at the top.
If there are two ore more channels, you can set whether to detect face masks and detailed conditions differently for each channel.

Face mask detection

Face mask & No face mask

Select **[Face mask]** to detect an object wearing a face mask; select **[No face mask]** to detect an object not wearing a face mask.
Set the minimum duration that will be used as a condition for detecting whether an object wears a face mask to trigger an event.
For example, if you select **[Face mask]** and enter [2] for **[Minimum duration]**, a face-mask detection event will occur at least 2 seconds after an object wearing a mask is detected.

> **Note**
>
> False detection may occur if:
> - A face is obscured by an object or person.
> - A face is not facing forward, such as in profile or heading down.
> - The fast movement of objects caused severe motion blur.
> - The brightness caused by low lights, night, etc., makes it difficult to identify the shape of an object.
> - Strong light sources, like direct sunlight, lamps, or car headlights, generate reflections, smearing, or shadows.
> - There is heavy snow, rain, wind, etc., or there is a sunset or sunrise.
> - A moving object in close proximity to the camera.
> - The OSD menu of the camera is adjusted.
> - Detection areas overlap.
> - A poor image quality or out-of-focus image makes it difficult to see.
>
> Detection may not occur, or poor performance may occur if:
> - The size of faces to be detected is below 80x80.
> - The distance for detection is not within 5-6 meters at most.
> - More than half of the face to be detected is obscured.
> - The number of faces on the screen is 12 or more.

Motion detection

The **[Motion detection]** feature detects all the motions being made within the area you set.
To enable the **[Motion detection]** feature, turn on the toggle at the top.
If there are two or more channels, you can set a motion detection area differently for each channel.

Motion detection

Chart

The **[Chart]** shows a list of detection areas you set.

Setting detection areas

- On the video, create a quadrilateral around the area you want to detect the motions of objects by clicking 4 times.
- Then the set detection area is created on the video and added to the **[Chart]**.
- You can create up to 8 detection areas.

Changing detection areas

- To resize the detection area, drag the vertex to your desired position.
- To create a polygon with 5 or more sides, hover over any lines of the created quadrilateral.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex.
  - You can create polygons with up to 8 sides.
  - To delete a vertex, hover over the vertex you want to delete. Then the **[-]** button appears on the point. Clicking the button deletes the vertex.
- To relocate the detection area, drag the area to your desired position.

Deleting detection areas

1. Hover over the row of the detection area you want to delete in the **[Chart]** or click the detection area on the video screen.
2. Then the Delete button appears in the **[Chart]**. Clicking the button deletes the area.

Changing the names of detection areas

- Double-click the set-area name you want to change in the **[Chart]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Object

Specifying objects

Select a detection area on the video screen or in the **[Chart]** and then select an object type to be detected in the **[Chart]** (multiple selections are possible).

If you don't choose any object from Object, the motion of any types of objects will be detected.

Level of detection

Set the level that will be used as a condition for detecting motions. You can set the level for each set detection area either by typing a value in the entry box or by dragging the slide control of the slider. When the current motion level is greater than the set level value, the motion detection event occurs.
When motions are detected per area, a curve appears in the graph. Then the curve changes its color when the motion detection event occurs.

Minimum duration

Set the minimum duration that will be used as a condition for triggering a motion detection event. The event occurs only when the motion lasts for at least the set minimum duration. In short, if you set it to [0], the motion detection event will occur as soon as a motion is detected.

Sensitivity

Set the sensitivity of motion detection per area. Set the sensitivity level to low for environments where objects are clearly distinguishable from the background; set the sensitivity level to high for dark environments where objects are not clearly distinguishable from the background.

> **Note**
>
> False detection may occur if:
> - The brightness or color of an object is similar to the background of the screen.
> - Multiple motions are being made irregularly or continuously due to scene transitions, sudden lighting changes, etc.
> - A stationary object is constantly moving in the same position.
> - Various objects are randomly blocking each other.
> - Objects are moving too quickly.
> - Strong light sources, like direct sunlight, lamps, or car headlights, generate reflections, smearing, or shadows.
> - There is heavy snow, rain, wind, etc., or there is a sunset or sunrise.
> - A moving object is in close proximity to the camera.
> - Small motions are being made around the borders of the screen.

Dynamic privacy masking

The **[Dynamic privacy masking]** feature allows you to hide selected objects by applying a mosaic mask on video. With this feature, you can protect privacy and personal information.
To enable the **[Dynamic privacy masking]** feature, turn on the toggle at the top.
If there are two or more channels, you can select objects to be masked differently for each channel.

Dynamic privacy masking

Object

Select the types of objects (person, face, vehicle, license plate) to mask (multiple selections are possible). When you install the WiseAI application, the [Dynamic privacy masking] feature is disabled by default, and no video is displayed on the video preview screen.

Type

Selecting **[Mosaic]** displays the masked area in mosaic; selecting **[Color]** displays the masked area in color.

Transparency

When you select **[Color]** in **[Type]**, you can set how transparent the color is when you choose to display the masked area in color.

Detection condition

Set the sensitivity level of detection. Higher sensitivity values detect objects with lower confidence, resulting in higher detection rates and error rates. Conversely, lower sensitivity values may result in fewer false alarms for events, but they are more likely to fail to detect objects.

People counting

The **[People counting]** feature counts the number of people crossing the virtual line in the direction you set. A person is counted crossing the set line only when the center of the person is the body length away from the line before and after the person crosses the line. Also, for a person to be counted, the person's head must cross the virtual line together.
To enable the **[People counting]** feature, turn on the toggle on the top.
If there are two or more channels, you can set whether to count people and configure the detailed settings differently for each channel.

Counting

You can view analytics data about the people crossing the virtual line from 00:00:00 on the day to the current time. You can also check the number and total of people who have crossed the virtual line by direction.
The counting data is refreshed every 3 seconds.

List

The **[List]** shows a list of virtual lines you set.

Setting virtual lines

- Click on the video screen, and then click on it again where you want. Then a virtual line with the start and end points appears.
- When the line to count the number of people is created, the line is also added to the **[List]**.
- You can create up to 2 virtual lines.
- You can also set the direction of the arrow on the line. To change the direction of the virtual line, click the arrow in the center of the line. People are counted only when they cross in the direction of the arrow or in the opposite direction of the arrow.

Changing virtual lines

- To resize the virtual line, drag the start or end point to your desired position.
- To relocate the virtual line, drag the line to the desired position.

Deleting virtual lines

1. Hover over the row of the virtual line you want to delete in the **[List]** or click the line on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the line.

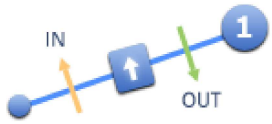
Changing the names of virtual lines

- Double-click the set-line name you want to change in the **[List]**.
- You can type the name up to 45 characters long, including English letters or numbers only (you cannot have a name that only contains numbers).

Setting counting methods

When you hover over the row of the virtual line to set the counting method in the **[List]** or click the line on the video screen, then the virtual line becomes thicker. To change the direction, click the arrow. There are two ways to count the number of people: IN counting and OUT counting.

- IN: Counts how many people moved in the direction of the arrow.
- OUT: Counts how many people moved in the opposite direction of the arrow.



Exclude area

You can set the area you want to exclude from people counting.

List

The **[List]** shows a list of exclude areas you set.

Setting exclude areas

- On the video, create a quadrilateral around the area you want to exclude from detection by clicking 4 times.
- Then the set exclude area is created on the video and added to the **[List]**.
- You can create up to 4 exclude areas.

Changing exclude areas

- To resize an exclude area, drag a vertex to your desired position.
- To create a polygon with 5 or more sides, hover over any lines of the created quadrilateral.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex.
  - You can create polygons with up to 8 sides.
  - To delete vertices, hover over a vertex you want to delete. Then the **[-]** button appears on the point. Clicking the button deletes a vertex.
- To relocate the exclude area, drag the area to your desired position.

Deleting exclude areas

1. Hover over the row of the exclude area you want to delete in the **[List]** or click the exclude area on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the area.

Changing the names of exclude areas

- Double-click the set-area name you want to change in the **[List]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Report

Report

You can receive reports of people-counting statistics.
To receive people-counting data through e-mail or FTP, turn on the **[Report]** toggle.

Schedule

Select **[Daily]** and time to receive people-counting data at the same time every day.
Select **[Weekly]** and time and days to receive people-counting data on the same day and time every week.

File name

Type a name and select the format of the file to send it via FTP and e-mail. The file name can contain up to 45 characters, including English alphabet letters, numbers, and hyphens (-). You can choose the file format between .xlsx and .txt.

Export

Click **[FTP/E-mail]** to type the details for FTP and e-mail.

Delete all data

Click **[Delete all data]** to reset all the people-counting data.
Data is not deleted after a factory reset but deleted only when you click **[Delete all data]**.

Note

An error may occur or the function may not work if:

- A person is loitering near the virtual line.
- A person is repeatedly entering or exiting the line from the edge of the line.
- A person in motion is obscured by the background or other objects near the line.
- People or the heads are not detected according to the settings for minimum size, maximum size, or sensitivity that you configure in **[Setup]**>**[Common setup]**.
- There are five or more people around the line at the same time.
- Two or more people passing closer together, such as arm-in-arm or shoulder-to-shoulder.
- A huge crowd is gathering.
- A person is moving at a speed greater than 1.5 m/s.

Vehicle counting

The **[Vehicle counting]** feature counts the number of vehicles crossing the virtual line in the direction you set. A vehicle is counted crossing the set line only when the center of the vehicle is the body length away from the line before and after the vehicle crosses the line.
To enable the **[Vehicle counting]** feature, turn on the toggle on the top.
If there are two or more channels, you can set whether to count vehicles and configure the detailed settings differently for each channel.

Counting

You can view analytics data about the vehicles crossing the virtual line from 00:00:00 on the day to the current time. You can also check the number and total of vehicles that have crossed the virtual line by direction.
The counting data is refreshed every 3 seconds.

List

The **[List]** shows a list of virtual lines you set.

Setting virtual lines

- Click on the video screen, and then click on it again where you want. Then a virtual line with the start and end points appears.
- When the line to count the number of vehicles is created, the line is also added to the **[List]**.
- You can create up to 2 virtual lines.
- You can also set the direction of the arrow on the line. To change the direction of the virtual line, click the arrow in the center of the line. Vehicles are counted only when they cross in the direction of the arrow or in the opposite direction of the arrow.

Changing virtual lines

- To resize a virtual line, drag the start or end point to your desired position.
- To relocate the virtual line, drag the line to the desired position.

Deleting virtual lines

1. Hover over the row of the virtual line you want to delete in the **[List]** or click the line on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the line.

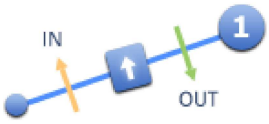
Changing the names of virtual lines

- Double-click the set-line name you want to change in the **[List]**.
- You can type the name up to 45 characters long, including English letters or numbers only (you cannot have a name that only contains numbers).

Setting counting methods

When you hover over the row of the virtual line to set the counting method in the **[List]** or click the line on the video screen, then the virtual line becomes thicker. To change the direction, click the arrow. There are two ways to count the number of vehicles: IN counting and OUT counting.

- IN: Counts how many vehicles moved in the direction of the arrow.
- OUT: Counts how many vehicles moved in the opposite direction of the arrow.



Exclude area

You can set the area you want to exclude from vehicle counting.

List

The **[List]** shows a list of exclude areas you set.

Setting exclude areas

- On the video, create a quadrilateral around the area you want to exclude from detection by clicking 4 times.
- Then the set exclude area is created on the video and added to the **[List]**.
- You can create up to 4 exclude areas.

Changing exclude areas

- To resize an exclude area, drag a vertex to your desired position.
- To create a polygon with 5 or more sides, hover over any lines of the created quadrilateral.
  - The **[+]** button then appears on the line. Clicking the button adds a vertex.
  - You can create polygons with up to 8 sides.
  - To delete vertices, hover over a vertex you want to delete. Then the **[-]** button appears on the point. Clicking the button deletes a vertex.
- To relocate the exclude area, drag the area to your desired position.

Deleting exclude areas

1. Hover over the row of the exclude area you want to delete in the **[List]** or click the exclude area on the video screen.
2. Then the Delete button appears in the **[List]**. Clicking the button deletes the area.

Changing the names of exclude areas

- Double-click the set-area name you want to change in the **[List]**.
- You can type the name up to 63 characters long, including English letters or numbers only.

Report

Report

You can receive reports of vehicle-counting statistics.
To receive vehicle-counting data through e-mail or FTP, turn on the **[Report]** toggle.

Schedule

Select **[Daily]** and time to receive vehicle-counting data at the same time every day.
Select **[Weekly]** and time and days to receive vehicle-counting data on the same day and time every week.

File name

Type a name and select the format of the file to send it via FTP and e-mail. The file name can contain up to 45 characters, including English alphabet letters, numbers, and hyphens (-). You can choose the file format between .xlsx and .txt.

Export

Click **[FTP/E-mail]** to type the details for FTP and e-mail.

Delete all data

Click **[Delete all data]** to reset all the vehicle-counting data.
Data is not deleted after a factory reset but deleted only when you click **[Delete all data]**.

> **Note**
>
> An error may occur, or the function may not work if:
> - The camera lens is mounted without lens facing the ground.
> - A vehicle is parked near the virtual line or moving back and forth.
> - A vehicle is repeatedly entering or exiting the line from the edge of the line.
> - Lighting changes occur gradually or abruptly (such as sunrise or sunset, vehicle lights beaming from the outside, and changes in color or brightness of surrounding lighting fixtures).
> - There are five or more vehicles around the virtual line at the same time.
> - A moving vehicle is obscured by the background or other objects near the line.
> - Two or more vehicles are passing in close proximity.
> - The density is very high (e.g., more than 70% in the video is moving objects).
> - Traffic is congested.
> - The IR is turned off even at night, making it difficult to recognize vehicles.
> - Environmental variables, such as snow, rain, fog, and so on make it difficult to detect vehicles.
> - The camera is trembling.

Backup & restore

You can save the current settings of the system as a file on your PC and restore the system from the backup file.

Backup & restore

Backup & restore

You can back up the settings of the WiseAI application or restore the application from the backup file.
Click **[Backup]** to create a backup file of the current settings of the WiseAI application.
Click **[Restore]** and select a backup file to restore the application from the backup file.

Factory default

Click **[Reset]** to return the application to its factory settings.

Version information

The version information shows you the information on WiseAI application and AI information. Depending on the camera model, the AI learning models may or may not be displayed.

Open source license

We provide open source licenses used by this product. Click **[View]** to see the information of the open source licenses used by this product and full license texts.

EULA

We provide the End User License Agreement (EULA) for this software product. Click **[View]** to check the agreement details.

Common setup

You can set conditions of object detection that are applied globally. You can set the sensitivity as well as the minimum and maximum size of an object to be detected.

Common setup

The object-detection settings configured in **[Common setup]** are applied to all features under **[Analytics]** and **[Statistics]**. (The statistics feature may not be supported in some versions.)

Minimum

Set the minimum size of an object to be detected. Objects smaller than the set minimum size are not detected.

Maximum

Set the maximum size of an object to be detected. Objects larger than the set maximum size are not detected.

Sensitivity

Set the detection sensitivity. When you set the sensitivity value higher, even objects with low reliability are detected.

> **Note**
> Detecting objects with low reliability in detection may result in a high false-detection rate.

Log

The important event logs are recorded while the camera is in operation. You can view the accumulated log history.

System log

You can view the dates, times, and details about changes to system settings and to the operation of the features of the system.

Log type

You can view the dates, times, and details of system changes. Select **[All]** to view the date, time, and details of all the events that occurred on the selected system.

Backup

You can back up the selected log and export the backup log to a text file. To back up the system logs, click **[Backup]**.

Event log

You can view the dates, times, and details about events that occurred on the camera.

Log type

You can view the date and time of the event's occurrence and the details. Select **[All]** to view the dates, times, and details of all the events that occurred on the selected camera (channel).

Backup

You can back up the selected log and export the backup log to a text file. Click **[Backup]** to back up the event logs.

> **Note**
>
> All the log messages are provided in English, regardless of the language you set in the WebViewer.
> Up to five minutes of event log history may be lost when the camera is powered off.
> A maximum of 1,000 logs are stored per log. After the 1,001st log, the oldest log is deleted.

Audio detection

An audio detection event can be created when audio above a set level is detected while the camera is capturing an image.

Audio detection

Enable audio detection

To apply the audio detection event, select **[Enable audio detection]**.

Level of detection

This sets the level standard for audio detection. An audio detection event is created when audio above the set level is detected.
When audio is detected, a graph will appear, and when an audio detection event is created, the graph color will change.

> **Note**
>
> - The lower the level of detection is, the smaller change in sound it can detect.
> - The audio level of detection value is designed to detect a sound at the threshold level or higher by normalizing the input data to a value between 1 and 100, and it is irrelevant to the decibel (dB) values.
> - Go to **[Video & Audio]**>**[Audio setup]**>**[Source]** to select Microphone and set the sufficient level of sound so that the audio detection function can operate properly.
> - Audio gain can be set from **[Video & Audio]**>**[Audio setup]**>**[Gain]**.

Product information

Check the model name and serial number of the product and set the device name, location, description and language.

Product information

Model

The model name of the product you are currently using is displayed. Changes cannot be made to the model name.

Serial number

The serial number of the product you are currently using is displayed. Changes cannot be made to the serial number.

Device name

Enter the device name of the product you are currently using. If you have installed a number of cameras, a different device name for each camera is recommended.
Enter up to 8 characters long, including uppercase (A-Z), lowercase (a-z), numbers, or special characters (excluding #'"&+:<>=₩%*).

Location

Enter the installation location of the product you are currently using. If you have installed a number of cameras, a different location name is recommended to distinguish between them.
Enter up to 32 characters long, including uppercase (A-Z), lowercase (a-z), numbers, special characters (only ~`!@$^()_-|{}[];,./?).

GPS coordinates

Select to enter the camera's **[GPS coordinates]**.

Longitude

You can enter or view the longitude value. Up to 6-digit decimal numbers can be typed within the range of -180 to 180.

Latitude

You can enter or view the latitude value. Up to 6-digit decimal numbers can be typed within the range of -90 to 90.

Description

Enter the description of the product you are currently using. You can enter other necessary information, including the installation date and location where the screen is showing.
Enter up to 32 characters long, including uppercase (A-Z), lowercase (a-z), numbers, special characters (only ~`!@$^()_-|{}[];,./?).

Memo

Enter the description of the product you are currently using. Enter other necessary information that were not entered on the description section.
Enter up to 32 characters long, including uppercase (A-Z), lowercase (a-z), numbers, special characters (only ~`!@$^()_-|{}[];,./?).

Language

Select the language of the product you are currently using. When you select a language and click Apply, all UI will be changed to the relevant language.

Open source license

We provide open source licenses used by this product. Click the **[View]** button to see the information of the open source licenses used by this product and full license texts.

WisePower

You can monitor the power consumption of the camera and set Eco mode.

> **Note**
>
> If sufficient power consumption data has not been collected, the monitoring value may be displayed as 0 W.
> If you set [Period] to [1 day] or [1 week], the minimum required collection time is 15 minutes, and if it is set to [1 month], the minimum required collection time is 60 minutes.
> The results of monitoring a camera's power consumption may differ from the actual usage depending on the usage conditions.

Power monitoring

You can select the period for monitoring power. You can choose from [1 day], [1 week], or [1 month].
Only the [Max. power] and [Avg. power] values change according to the selected period, while other values display the current value. For example, if you select [1 day], the maximum value of the power consumption that occurred during the day is displayed in [Max. power], and the average value of the power consumption that occurred during the day is displayed in [Avg. power].
The sampling interval for power consumption is 15 minutes if the period is set to [1 day] or [1 week], and 60 minutes if the period is [1 month].

- **PoE class(PSE)**: Displays the PoE class, which categorizes the power supplied by the switch (PSE, Power Sourcing Equipment). This class is based on the power requested by the connected device: Class 3 for 13W, Class 4 for 25.5W, and Class 5 for 40W. This helps the switch provide the correct power to the device.
- **Power requested**: Displays the LLDP value requested by the camera to the switch.
- **Current power**: Displays the current power consumption.
- **Max. power**: Displays the maximum power consumption during the set period by reflecting the power as "0" during the time the camera is off.
- **Avg. power**: Displays the average power consumption during the set period by reflecting the power as "0" during the time the camera is off.

Upgrade / Restart

You can upgrade the software of the product you are currently using, perform a factory default, back up or restore the configuration, or restart.

Upgrade/Downgrade

Software can be upgraded as new firmware versions are released. You can also downgrade to a previous version.

Software

The software version of the product you are using is displayed. Changes cannot be made to the software version.
You can view the software details, including the ISP version applied to the software and SUNAPI version, by clicking the **[Info]** button.

Software upgrade/downgrade

You can upgrade or downgrade the software of the product in use. To upgrade or downgrade the software, click the **[...]** button. Select the file and click the **[Open]** button. Upgrade/downgrade will start when you click the **[Start]** button. When the upgrade or downgrade is complete, the camera boots and you are automatically disconnected. You need to connect to the web viewer.

Note

- The latest security patches might not be applied if you downgrade the firmware.
- Upgrade can take up to 10 minutes. Do not terminate the program while upgrading is in progress. Doing so may result in the program failing to upgrade properly.
- For the web viewer to work properly, you need to delete all the browser caches before connecting again after the software upgrade.
- You can download the latest software version from Hanwha Vision's website: http://www.hanwhavision.com

---

Factory default

Resets the system configuration to what it was at the time of product purchase. When you click the **[Reset]** button and then click the **[OK]** button in the confirm window, the factory default reset will be carried out. (Logs won't be reset though.)

If you wish to reset the system configuration (except for the network configuration and installed open platform configuration) to factory default, select **[Except network parameter & open platform]**. When a factory default is carried out, the connection with the camera will be terminated. When you reconnect to the web viewer for the first time, you will need to enter the password again.

Configuration backup & restore

You can backup and save the current camera setup or restore a desired configuration. You can create a number of backup files for desired configurations, or restore and use a desired configuration according to the purpose or environment when using the product.

Backup

When you click the **[Backup]** button, a backup file of 'model name Config.bin' will be created.

Restore

When you click the **[Restore]** button, a window where you can select a backup file to restore will appear. When you select a backup file and press the **[Open]** button, the configuration will be restored based on the relevant backup file.

> **Note**
>
> - When you restore the configuration, the connection with the camera will be terminated automatically and you will need to reconnect to the web viewer.
> - If you use an imported backup file for a different model than the product you are currently using, the product may malfunction. Do not use a backup file for a different model or change the configuration manually.

Restart

Restart the camera system. Click the **[Restart]** button, and when the confirm window appears, click the **[OK]** button. The camera will restart and the web viewer window will close. You will need to reconnect to the web viewer.

Log

You can check camera-related logs. You can check information including camera access, system changes and events which have occurred, and backup log information for each log type.

> **Note**
>
> Logs can be checked in order of most recent log first.
> Up to 1,000 logs can be saved. By selecting **[View 10 lines]**, **[View 15 lines]**, or **[View 20 lines]**, you can set how many logs will be displayed on one page.
> When the number of logs that are saved exceeds 1,000, a new log is saved after deleting the oldest log.

Access log

You can check login and logout information for each access account.

Log type

You can check accounts which have accessed the camera, login and logout date, and time information. When you select All, you can check login and logout, date & time, and detailed information for all access IDs.

Export

You can back up the selected log type as a text file. To back up the access log, click **[Export]**. The log file information is displayed as camera model name_log type_backup date, and time.

System log

You can check date & time and detailed information for system changes.

Log type

This allows you to check camera system setup change information, along with the date and time. When you select All, you can check date & time and detailed information for all system changes.

Export

You can backup the selected log type as a text file. To backup the system log, click **[Export]**. The log file information is displayed as camera model name_log type_backup date, and time.

Event log

You can check the date & time and detailed information for an event which has occurred in the system.

Log type

You can check occurrence date & time and detailed information for a selected event. When you select All, you can check the date & time and detailed information for all events occurring in the system.

Export

You can backup the selected log type as a text file. To backup the event log, click **[Export]**. The log file information is displayed as camera model name_log type_backup date, and time.

Remote log transmission

You can send logs remotely. Select **[Enable]** to send camera logs remotely.

IP type

Select the IP address type between IPv4 and IPv6.

Server address

Enter the server address of the remote system to send logs to.

Port

Enter the port information to connect to the remote system.

Type

Select the protocol that the camera uses to communicate with the server.

Format

Select the logging format of the log messages between **[RFC3164]** and **[RFC5424]**.

Open platform

When you install an additional application on the camera, you can use the functions of the installed application in addition to existing functions.

> **Note**
>
> You can check all the applications installed on the camera by clicking **[Apps]** at the right top of the web viewer. To customize application settings, click **[Go App]** in the Apps dialog box.

Open platform

You can check the information of applications installed on the camera.

Data usage

Displays the memory usage and CPU usage for each application. When you hover over the graph, detailed information appears.

Metadata generation amount

Displays the generation amount per metadata in a circular graph.
The real-time metadata generation amount per app is displayed in a bar chart.
When you hover over the graph, detailed information appears.

App list

You can check the list of applications currently installed. Up to 10 applications can be installed.

- **No.**: Applications are numbered in the order they are installed.
- **Application name**: Displays the name of the application. The name can be up to 59 characters long.
- **Model**: Displays the model name when you use paid apps; displays "-" in case of the free app WiseAI.
- **Version**: Displays the version of the application.
- **Priority**: Displays the priority of the application.
  The priority can be set in **[Settings]** of **[Go App]**.
- **Status**: Displays the statuses of the application: "Running" when the application is running; "Stopped" when the application is not running.
  CPU usage and metadata generation are shown as graphs. However, the metadata generation amount is only shown for BestShot and metadata.
- **Go App**: Navigates to the screen provided by each application. Click the arrow next to **[Go App]** to check or set the following details.
  - **Info**: Displays the installation date and total running time of the application.
  - **Settings**: Select **[Enable]** in **[Auto start]** to automatically run the application when the camera is turned on and the main task is executed. If the total resource usage of the camera (including the camera's main task and applications) increases, the running applications are forcibly terminated in the order of "Low" priority set in **[Priority]**. If the priorities are the same, the application with higher usage is forcibly terminated.

- **License**: Displays the license information required for app installation when you use paid apps; displays "-" in case of the free app WiseAI.

Installing applications

1. Click the **[Install]** button.
2. In the **[Open]** dialog box, select the application file in cap format and click the **[Open]** button.
3. When the confirmation message appears, click **[Yes]**. The installed application will be added to the **[App list]**.

Deleting applications

1. Select the application to delete from the **[App list]** and click **[Uninstall]**.
2. When the confirmation message appears, choose whether or not to keep the existing settings. The uninstalled application will be forcibly terminated.

Note

- For questions regarding the installation and usage of applications, contact the developers' website of Hanwha Vision (http://step.hanwha-security.com).


Hanwha
Vision