VIVOTEK

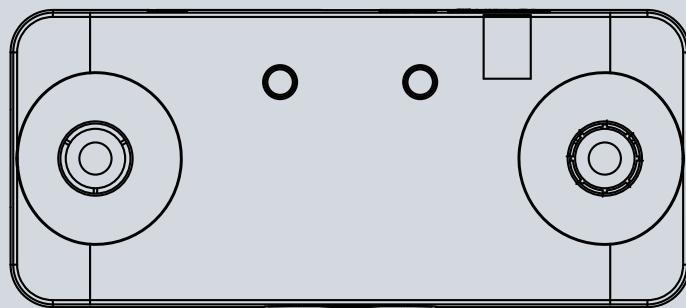# SC8131 Stereo Network Camera
User's Manual

1MP • Stereo Camera • 3D Tracking • People Counting

Rev. 1.8

Table of Contents

Overview

The VIVOTEK SC8131 is a stereo camera that provides precise tracking and people counting functionality. The dual-lens stereo camera design eliminates the defects of single-lens cameras in video analysis applications. Unlike single-lens applications that are easily affected by lighting changes or shadows, this camera enables stereo visions that accurately tracks the 3D positions of objects moving across the field of view.

The stereo camera is ideal for collecting information for retails. The people counting and trajectory detection applies in store layout improvement, queue management, and the control of service times; providing precious information for business owners.

Featuring height filtering and height perception via the triangulation computation of images acquired from two view points, moving objects can be effectively recognized. This enables people of different heights, single or in groups, to be distinguished from non-human objects such as shopping carts. Moreover, the computation of height disparity data takes place on the camera, instead of sending video streams to a dedicated computer running an analytics software. The solution saves bandwidth and reduces the chance of data loss in the event of network or power downtime.

Supported by the VCA Report utility in VAST software v1.12, the data collected by this camera is displayed in comprehensive graphs and line charts. You can monitor and compare the historical data acquired through different time periods or among different surveillance areas with the ease of use of a graphical interface.

The camera also supports ONVIF Video Analytics Service that includes object metadata, rule engine, and counting events for development of 3rd party software. It displays 3D tracking results in both live and recorded video in order to verify tracking and counting accuracy. It is possible to customize analytic rules for various applications in addition to the counting utility.

Precision and accuracy:
• Stereo Camera with 3D Depth Technology • 98 % Counting Accuracy Rate
• Not Influenced by Shadows, Reflections or Small Objects • Bi-Directional Counting on configurable detection lines
• Detection of U-turns to Avoid Double Counting

Revision History

■ Rev. 1.0: Initial release

■ Rev. 1.1: Added new features sush as event push, stereo tracking and counting results in Liveview, and cloud services.

■ Rev. 1.2: Added information for Remote Management, Maintenance, and the Analytics Event Manager. Modified some camera configuration details. Remove Event settings, because the event notifications have been incorporated as part of the counting features.

■ Rev. 1.3: Reflected changes in firmware release v. 0101g, e.g., added fixed iris mode to exposure setting, mod.sdp playback from SD card, and the removal of the default counting line.

■ Rev. 1.4:
• Added the description for video Stitching that brings up to 7 SC8131s together to provide video analytics over a large and wide floor plan.
• Added the description for Tilt, and Object type.
• Moved the Tracking and Counting configuration section further up near the beginning of the manual.
• The description for the U turn counting rules options was also included.
• The later firmware revision removed the audio functions.
• Added notifications that the height of the camera canister (4cm) must be deleted if the ceiling height is measured from floor to ceiling.

■ Rev. 1.5:
• Corrected DI/DO pin related description.

■ Rev. 1.6:
• Added the installation height FOV tables for SC8131-F2, -F4, and -F6.

■ Rev. 1.7:
• Added description for Queue Analysis and service time counting. See page 79.
• Added description for Tampering detection. See page 84.
• Added description for Passer-by counting. See page 78.
• Updated event rule parameters.
• Updated Report Push options, w/ device local time, camera status flags, counting/zone contents, Queue raw data. See page 85.
• Updated FTP report filename format to accommodate report time format in different countries. See page 88.
• Added log database IDs via Restful api and Report Push.
• Added a note for browsing SC8131s with different versions of firmware.
• The multiple-camera stitching procedure can now take place among cameras at once, instead of stitching between two cameras at one time.

■ Rev. 1.8:
• Updated LED behaviors.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

■ SC8131	■ Mounting plate
■ Screw pack	■ Software CD
■ L-type Hex key wrench	■ Quick Installation Guide
■ Alignment sticker	

⚠ **IMPORTANT:**

When browsing the counting results from multiple SC8131s running different revisions of firmware, use the **Ctrl** + **F5** keys to avoid having to clean cached data.

Symbols and Statements in this Document

INFORMATION: provides important messages or advices that might help prevent inconvenient or problem situations.

NOTE: Notices provide guidance or advices that are related to the functional integrity of the machine.

Tips: Tips are useful information that helps enhance or facilitate an installation, function, or process.

WARNING: or IMPORTANT:: These statements indicate situations that can be dangerous or hazardous to the machine or you.

Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

⚠ IMPORTANT:

Requirements for Running Stereo Tracking Video Analysis:

1. The recommended installation height ranges from **2.4** to **3.6** meters. If the camera is unavoidably installed in a position higher than **3.6m**, you can use the zoom-in mode operation. Different lens provide different FOVs. See the FOV tables at page 9 for details.

2. The embedded video tracking and counting analysis requires a monitoring session on Microsoft IE 10 or IE 11 browser.

3. Lens cleanliness is also required because dust spots or smears on dirty lens can produce miscalculation of pixels, correlation, and movements.

4. Avoid impacts to the lens modules. The relative positions of the lens have been carefully calibrated in factory. Even if the lens positions have slightly changed, optical parameters and stereo correlation will be affected, and then you should return the camera for a repair.

5. For other installation concerns, please refer to page 13, Considerations.

6. Avoid glass and reflective materials, such as aluminum foils, in the field of view. If unavoidable, you can use the Exclusive area settings to get rid of the side effects.

7. Make sure the camera is installed appropriately above the area of your interest, e.g., an entrance to building. Also use a leveling tool to make sure the camera is mounted horizontally level.

8. Due to the system load, do not open two configuration web consoles at the same time.

Refer to page 51 for the configuration details about the embedded **Stereo Tracking** and **Counting** functionality.

✎ NOTE:

· This camera is powered by a PoE switch or PoE injector. This equipment is to be connected only to PoE networks without routing the the outside plant.

Physical Description

Front Panel

LEDs

Dual lenses

Rear Panel

Mounting hole   DI/DO terminal block

RJ45 port

Retainer rivets

Top View

Reset   Release tab   MicroSD card slot

Reset

Micro SD

USB 2.0

USB for iBeacon
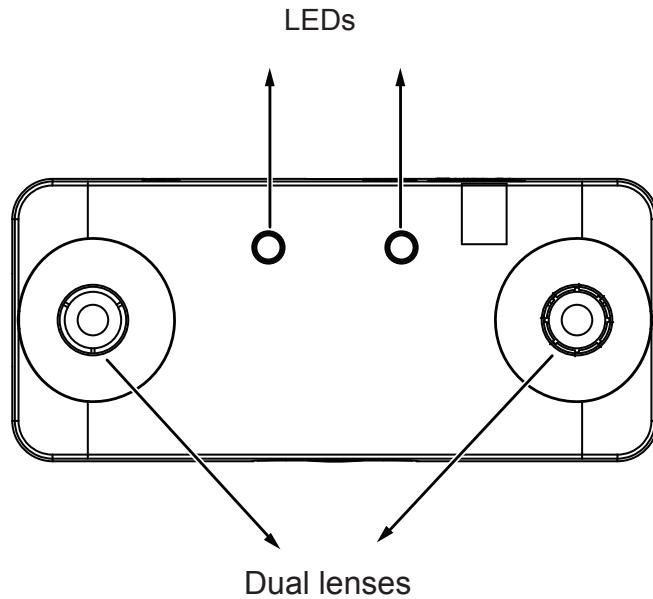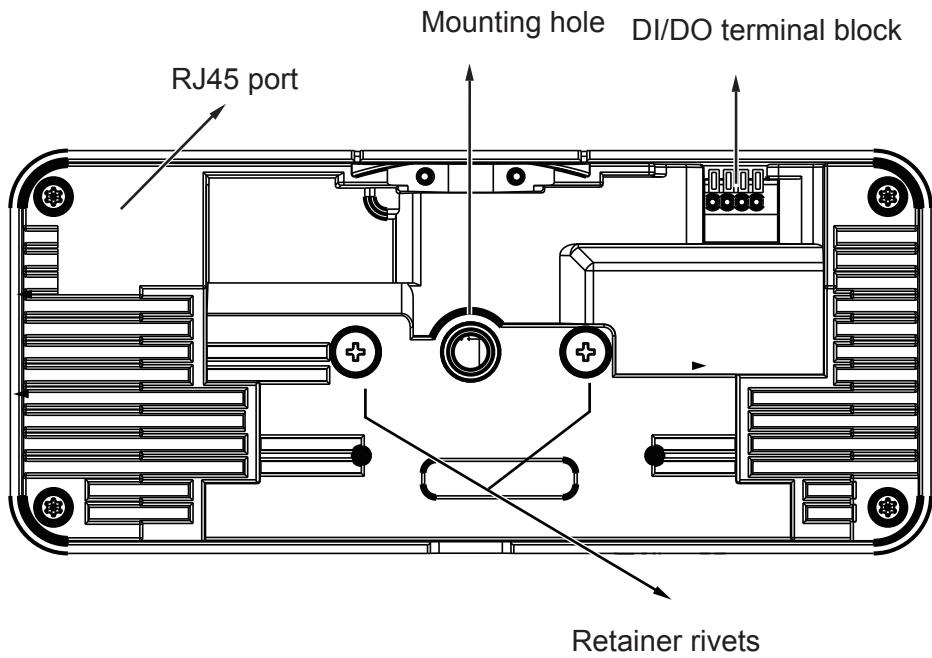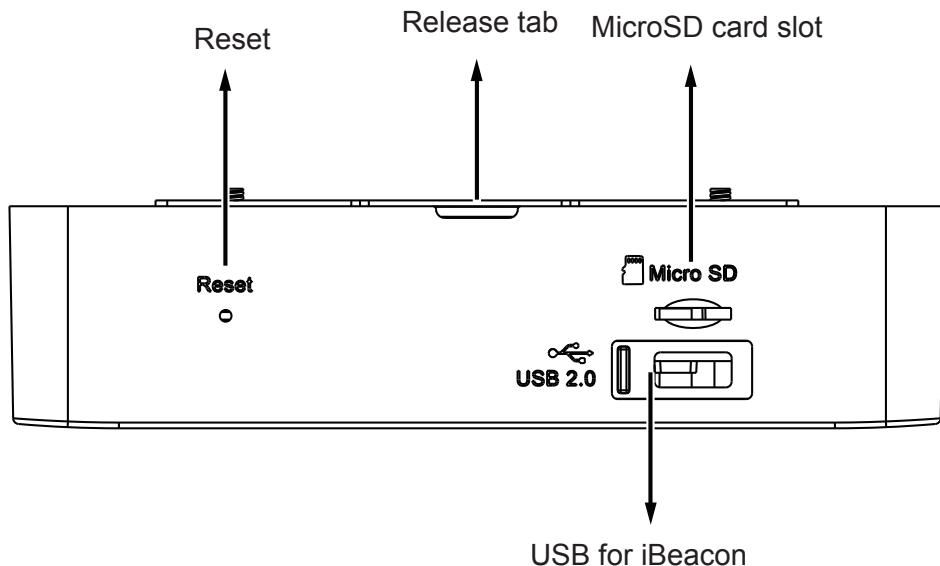
The USB port output is 5V, 2.42W

⚠ **WARNING:**

Please do not remove the protective sheet before the installation is done. Dirty lens can seriously affect the accuracy of video analysis.

Installation Heights

SC8131(F2): 240~500 cm (7.9~16.4')
SC8131(F4): 500~800 cm (16.4~26.2')
SC8131(F6): 800~1000 cm (26.2~32.8')

SC8131-F2

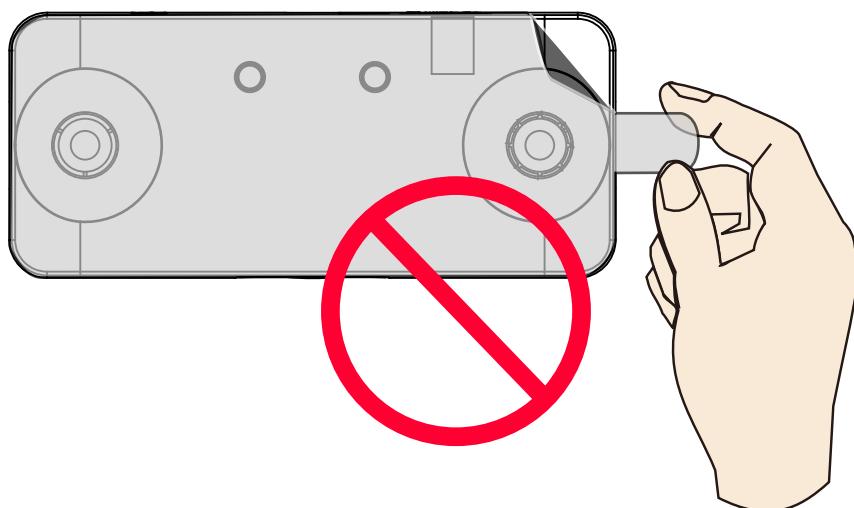| Zoom ratio		1.0	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8
FOV (Horizontal)	HFOV	HFOV	HFOV	HFOV	HFOV	HFOV	HFOV	HFOV	HFOV	HFOV
Distance with next camera (H)*	Height									
140.1	240	254.8	242.1	229.4	216.6	203.9	191.1	178.4	165.6	152.9
191.1	260	305.8	290.5	275.2	259.9	244.6	229.4	214.1	198.8	183.5
242.0	280	356.8	338.9	321.1	303.3	285.4	267.6	249.7	231.9	214.1
293.0	300	407.7	387.4	367.0	346.6	326.2	305.8	285.4	265.0	244.6
344.0	320	458.7	435.8	412.8	389.9	367.0	344.0	321.1	298.2	275.2
395.0	340	509.7	484.2	458.7	433.2	407.7	382.3	356.8	331.3	305.8
445.9	360	560.6	532.6	504.6	476.6	448.5	420.5	392.5	364.4	336.4
	380		581.0	550.5	519.9	489.3	458.7	428.1	397.6	367.0
	400				563.2	530.1	496.9	463.8	430.7	397.6
	420					570.8	535.2	499.5	463.8	428.1
	440						573.4	535.2	496.9	458.7
	460							570.8	530.1	489.3
	480								563.2	519.9
	500									550.5

* Distance between cameras when configured in a stitching configuration.

* Unit in centimeter.

** The number in front of HFOV (Horizontal FOV) stands for zoom ratio, if applied.

SC8131-F4

Zoom ratio		1.0		1.1		1.2		1.3		1.4	
FOV (Horizontal / Vertical)		HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV
Distance with next camera (H)*	Height										
225.0	360	274.9	177.8	261.2	168.9	247.4	160.0	233.7	151.1	220.0	142.2
249.9	380	299.9	193.9	284.9	184.2	269.9	174.5	254.9	164.8	239.9	155.1
274.9	400	324.9	210.1	308.7	199.6	292.4	189.1	276.2	178.6	259.9	168.1
299.9	420	349.9	226.3	332.4	214.9	314.9	203.6	297.4	192.3	279.9	181.0
324.9	440	374.9	242.4	356.2	230.3	337.4	218.2	318.7	206.1	299.9	193.9
349.9	460	399.9	258.6	379.9	245.6	359.9	232.7	339.9	219.8	319.9	206.9
374.9	480	424.9	274.7	403.7	261.0	382.4	247.3	361.2	233.5	339.9	219.8
399.9	500	449.9	290.9	427.4	276.4	404.9	261.8	382.4	247.3	359.9	232.7
424.9	520	474.9	307.1	451.2	291.7	427.4	276.4	403.7	261.0	379.9	245.6
449.9	540	499.9	323.2	474.9	307.1	449.9	290.9	424.9	274.7	399.9	258.6
474.9	560	524.9	339.4	498.6	322.4	472.4	305.4	446.2	288.5	419.9	271.5
499.9	580	549.9	355.5	522.4	337.8	494.9	320.0	467.4	302.2	439.9	284.4
	600			546.1	353.1	517.4	334.5	488.6	315.9	459.9	297.4
	620					539.9	349.1	509.9	329.7	479.9	310.3
	640							531.1	343.4	499.9	323.2
	680									539.9	349.1
	700									559.9	362.0
	720										
	740										
	760										
	780										
	800										
	820										
	840										
	860										
	880										

* Distance between cameras when configured in a stitching configuration.

	1.5		1.6		1.7		1.8	
	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV
360	206.2	133.3	192.5	124.4	178.7	115.6	165.0	106.7
380	225.0	145.4	210.0	135.8	195.0	126.1	180.0	116.4
400	243.7	157.6	227.5	147.1	211.2	136.6	195.0	126.1
420	262.4	169.7	244.9	158.4	227.5	147.1	210.0	135.8
440	281.2	181.8	262.4	169.7	243.7	157.6	225.0	145.4
460	299.9	193.9	279.9	181.0	259.9	168.1	239.9	155.1
480	318.7	206.1	297.4	192.3	276.2	178.6	254.9	164.8
500	337.4	218.2	314.9	203.6	292.4	189.1	269.9	174.5
520	356.2	230.3	332.4	214.9	308.7	199.6	284.9	184.2
540	374.9	242.4	349.9	226.3	324.9	210.1	299.9	193.9
560	393.7	254.5	367.4	237.6	341.2	220.6	314.9	203.6
580	412.4	266.7	384.9	248.9	357.4	231.1	329.9	213.3
600	431.2	278.8	402.4	260.2	373.7	241.6	344.9	223.0
620	449.9	290.9	419.9	271.5	389.9	252.1	359.9	232.7
640	468.7	303.0	437.4	282.8	406.2	262.6	374.9	242.4
680	506.1	327.3	472.4	305.4	438.7	283.6	404.9	261.8
700	524.9	339.4	489.9	316.8	454.9	294.1	419.9	271.5
720	543.6	351.5	507.4	328.1	471.2	304.6	434.9	281.2
740			524.9	339.4	487.4	315.1	449.9	290.9
760			542.4	350.7	503.6	325.6	464.9	300.6
780					519.9	336.1	479.9	310.3
800					536.1	346.7	494.9	320.0
820					552.4	357.2	509.9	329.7
840							524.9	339.4
860							539.9	349.1
880							554.9	358.8

SC8131-F6

Zoom ratio		1.0		1.1		1.2		1.3		1.4	
FOV (Horizontal / Vertical)		HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV
Distance with next camera (H)*	Height										
147.6	500	295.3	209.9	280.5	199.4	265.8	188.9	251.0	178.4	236.2	167.9
164.1	520	311.7	221.5	296.1	210.4	280.5	199.4	264.9	188.3	249.4	177.2
180.5	540	328.1	233.2	311.7	221.5	295.3	209.9	278.9	198.2	262.5	186.5
196.9	560	344.5	244.8	327.3	232.6	310.1	220.4	292.8	208.1	275.6	195.9
213.3	580	360.9	256.5	342.9	243.7	324.8	230.8	306.8	218.0	288.7	205.2
229.7	600	377.3	268.2	358.5	254.7	339.6	241.3	320.7	227.9	301.9	214.5
246.1	620	393.7	279.8	374.0	265.8	354.4	251.8	334.7	237.8	315.0	223.9
262.5	640	410.1	291.5	389.6	276.9	369.1	262.3	348.6	247.8	328.1	233.2
278.9	680	442.9	314.8	420.8	299.1	398.6	283.3	376.5	267.6	354.4	251.8
295.3	700	459.3	326.5	436.4	310.1	413.4	293.8	390.4	277.5	367.5	261.2
311.7	720	475.8	338.1	452.0	321.2	428.2	304.3	404.4	287.4	380.6	270.5
328.1	740	492.2	349.8	467.5	332.3	442.9	314.8	418.3	297.3	393.7	279.8
344.5	760	508.6	361.4	483.1	343.4	457.7	325.3	432.3	307.2	406.8	289.1
360.9	780	525.0	373.1	498.7	354.4	472.5	335.8	446.2	317.1	420.0	298.5
377.3	800	541.4	384.7	514.3	365.5	487.2	346.3	460.2	327.0	433.1	307.8
410.1	820	557.8	396.4	529.9	376.6	502.0	356.8	474.1	336.9	446.2	317.1
	840			545.5	387.7	516.8	367.3	488.1	346.9	459.3	326.5
	860			561.1	398.7	531.5	377.7	502.0	356.8	472.5	335.8
	880					546.3	388.2	515.9	366.7	485.6	345.1
	900					561.1	398.7	529.9	376.6	498.7	354.4
	920							543.8	386.5	511.8	363.8
	940							557.8	396.4	525.0	373.1
	960									538.1	382.4
	980									551.2	391.7
	1000										

* Distance between cameras when configured in a stitching configuration.

|		1.5		1.6		1.7		1.8	
		HFOV	VFOV	HFOV	VFOV	HFOV	VFOV	HFOV	VFOV
	500	221.5	157.4	206.7	146.9	191.9	136.4	177.2	125.9
	520	233.8	166.1	218.2	155.1	202.6	144.0	187.0	132.9
	540	246.1	174.9	229.7	163.2	213.3	151.6	196.9	139.9
	560	258.4	183.6	241.2	171.4	223.9	159.1	206.7	146.9
	580	270.7	192.4	252.6	179.5	234.6	166.7	216.5	153.9
	600	283.0	201.1	264.1	187.7	245.3	174.3	226.4	160.9
	620	295.3	209.9	275.6	195.9	255.9	181.9	236.2	167.9
	640	307.6	218.6	287.1	204.0	266.6	189.5	246.1	174.9
	680	332.2	236.1	310.1	220.4	287.9	204.6	265.8	188.9
	700	344.5	244.8	321.5	228.5	298.6	212.2	275.6	195.9
	720	356.8	253.6	333.0	236.7	309.2	219.8	285.5	202.9
	740	369.1	262.3	344.5	244.8	319.9	227.3	295.3	209.9
	760	381.4	271.1	356.0	253.0	330.6	234.9	305.1	216.9
	780	393.7	279.8	367.5	261.2	341.2	242.5	315.0	223.9
	800	406.0	288.6	379.0	269.3	351.9	250.1	324.8	230.8
	820	418.3	297.3	390.4	277.5	362.6	257.7	334.7	237.8
	840	430.6	306.0	401.9	285.6	373.2	265.2	344.5	244.8
	860	442.9	314.8	413.4	293.8	383.9	272.8	354.4	251.8
	880	455.2	323.5	424.9	302.0	394.5	280.4	364.2	258.8
	900	467.5	332.3	436.4	310.1	405.2	288.0	374.0	265.8
	920	479.9	341.0	447.9	318.3	415.9	295.6	383.9	272.8
	940	492.2	349.8	459.3	326.5	426.5	303.1	393.7	279.8
	960	504.5	358.5	470.8	334.6	437.2	310.7	403.6	286.8
	980	516.8	367.3	482.3	342.8	447.9	318.3	413.4	293.8
	1000	529.1	376.0	493.8	350.9	458.5	325.9	423.3	300.8

Considerations

Note the following when planning the camera installation:

1. The installation site must be adequately lighted for optimal accuracy with video analysis.
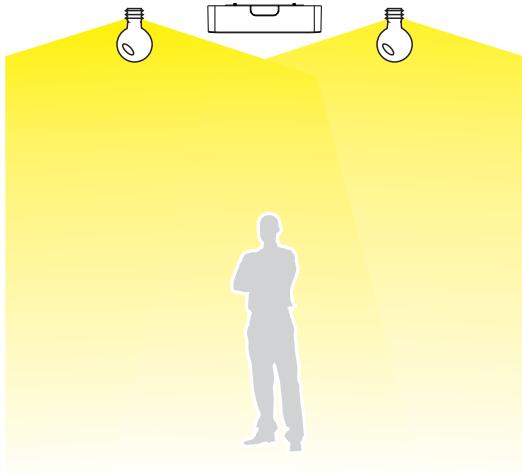
2. It is preferred that the camera is mounted directly above the objects to be counted. Use tools such as a spirit level to ensure the camera is installed level.
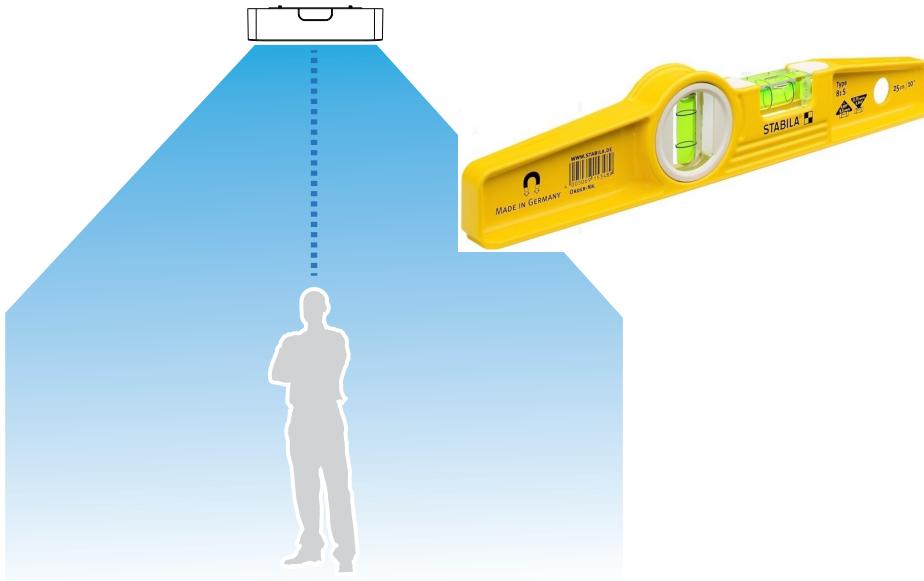
3. By building a 3D depth map from an overhanging position, the objects' height information can be acquired, and thus the drawbacks of 2D video counting can be eliminated. The silhouette of heads and shoulders and their relative depth information enable the camera to distinguish human activities from the background and other objects, such as shadows, shopping carts, and dogs.
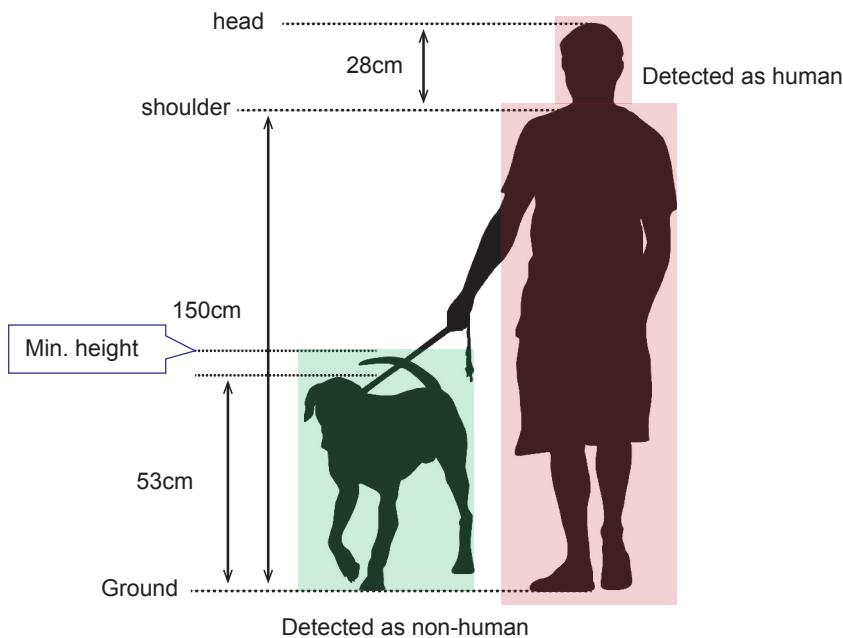
4. The receommended installtion position is **2.4m ~ 3.6m**. Higher position is also allowed. For positions higher than **3.6m**, you can also use the Zoom-in mode operation.

   4-1. Use a spirit level to ensure the camera is installed level.

   4-2. Use a laser distance meter to measure the installation height. The height information **MUST BE** correctly measured and entered in the camera's configuration page.

   4-3. Please **delete** the height of the camera canister, e.g., 250cm (ceiling height) -4cm (the height of camera canister) = 246cm. The reason for doing so is because the lenses are at the lower edge of the canister.
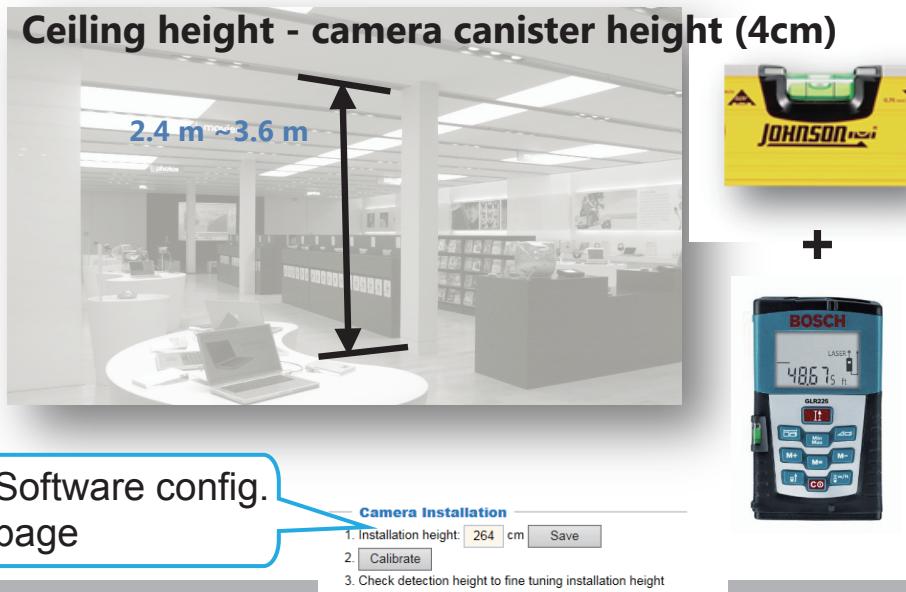
5. Below are the configuration elements for operating the SC8131 3D camera: .
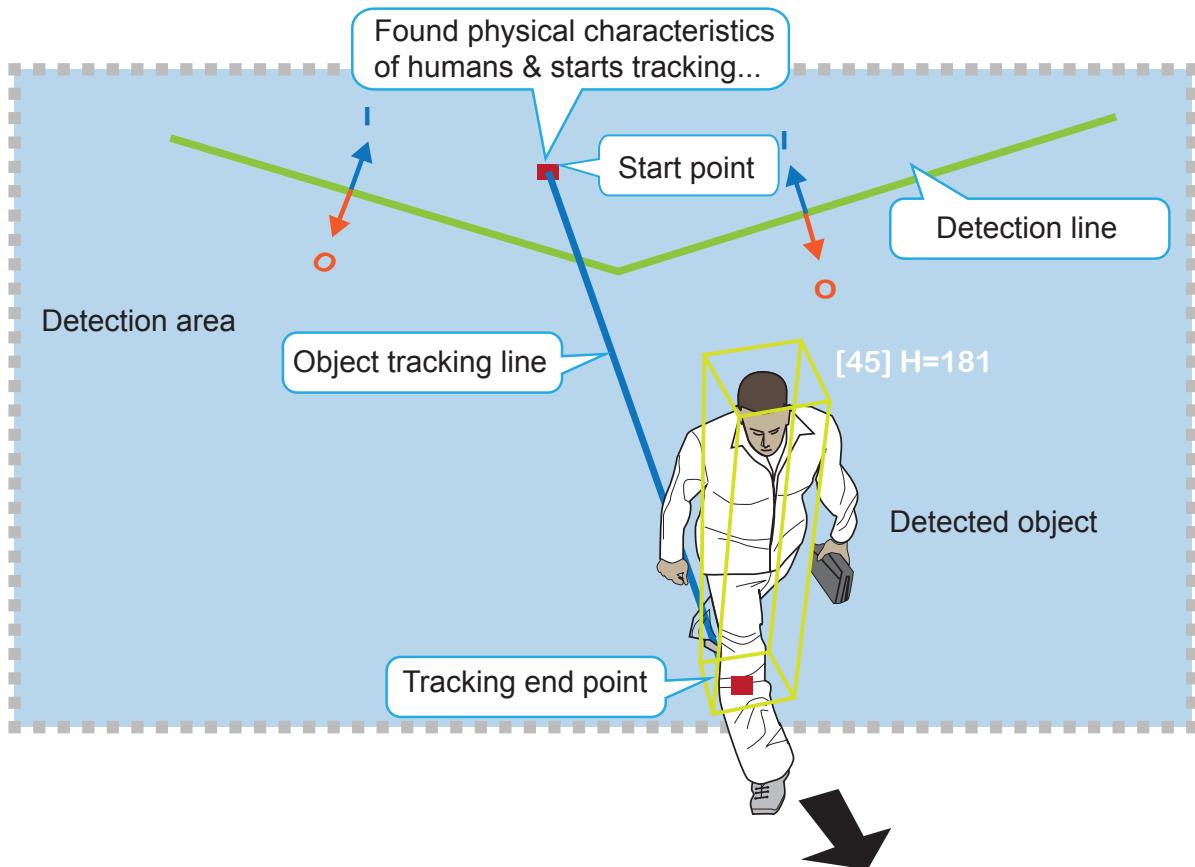
The counting takes place when a moving object appears in the detection area and moves across the detection line.

6. For counting to work properly, you should avoid having the view covering a large portion of walls as shown below.

   6-1. Keep camera away from wall or other obstacles to optimize the effectiveness of FOV.

   6-2. Select a location that can cover a longer object trajectories for better tracking results.

7. You can use the Exclusive area setting to get rid of the effects of some elements in the scene. They include: white or bright surfaces, mono-color surfaces, mirror, glass door, or reflective materials that might introduce false images. Avoid covering the floor with Exclusive areas.

Exclusive area

Mono-color surface

White table top

stainless, reflective panel

white marble
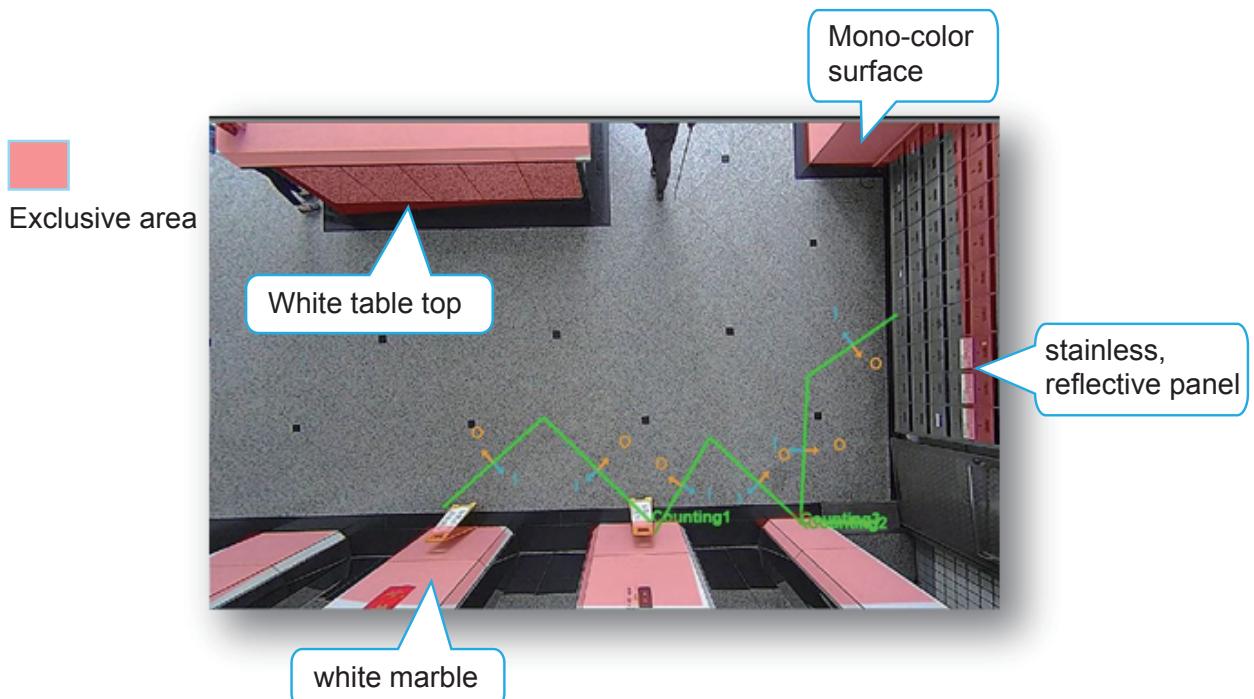
8. An effective counting requires an object to be detected, and then moves across the detection line. Avoid setting the line too close to the edge of detection area.

Not enough space to recognize objects....

Detection line

Detection area
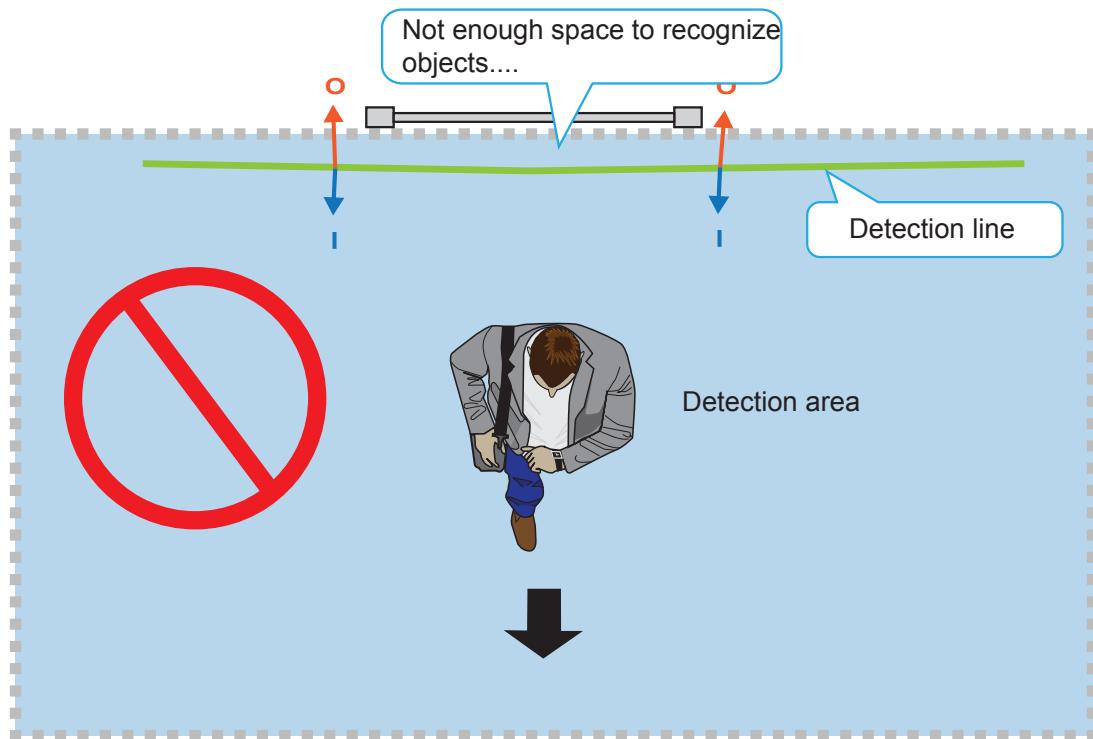
9. By drawing the line slightly away from the place where customers make their appearance allows enough space for recognition to take place. A start and an end point across the line enable the movement to be considered as a count.
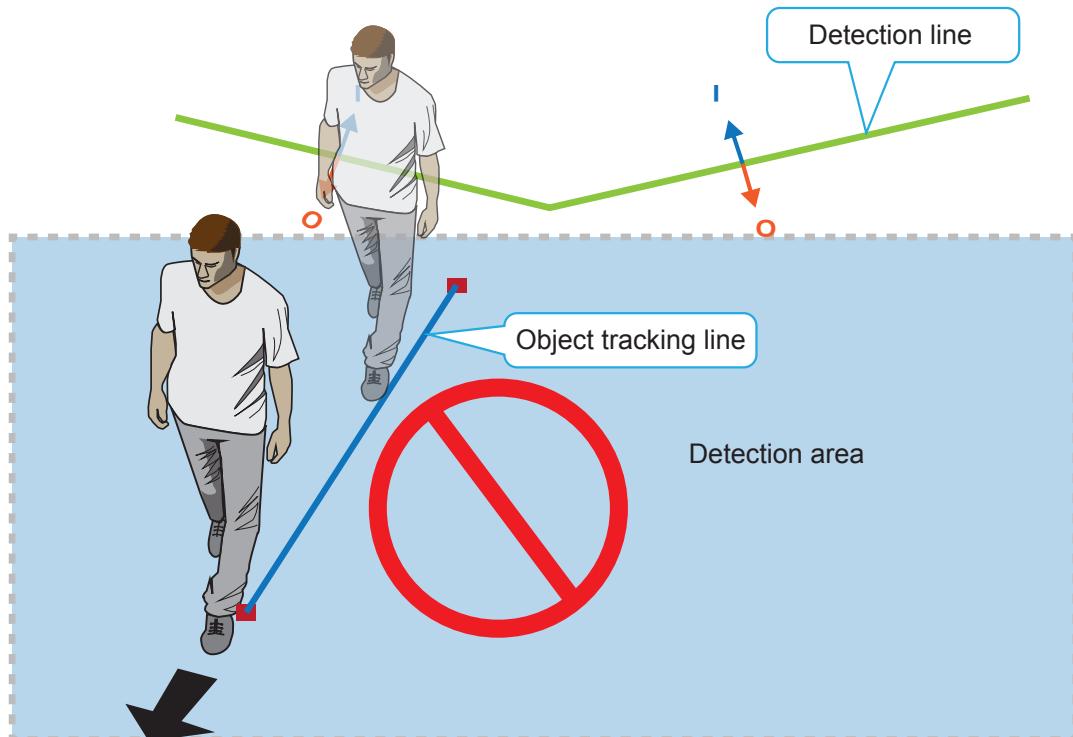
The stop point is where the object vanishes from the scene.

Detection line

The start and end points take shape across the line.
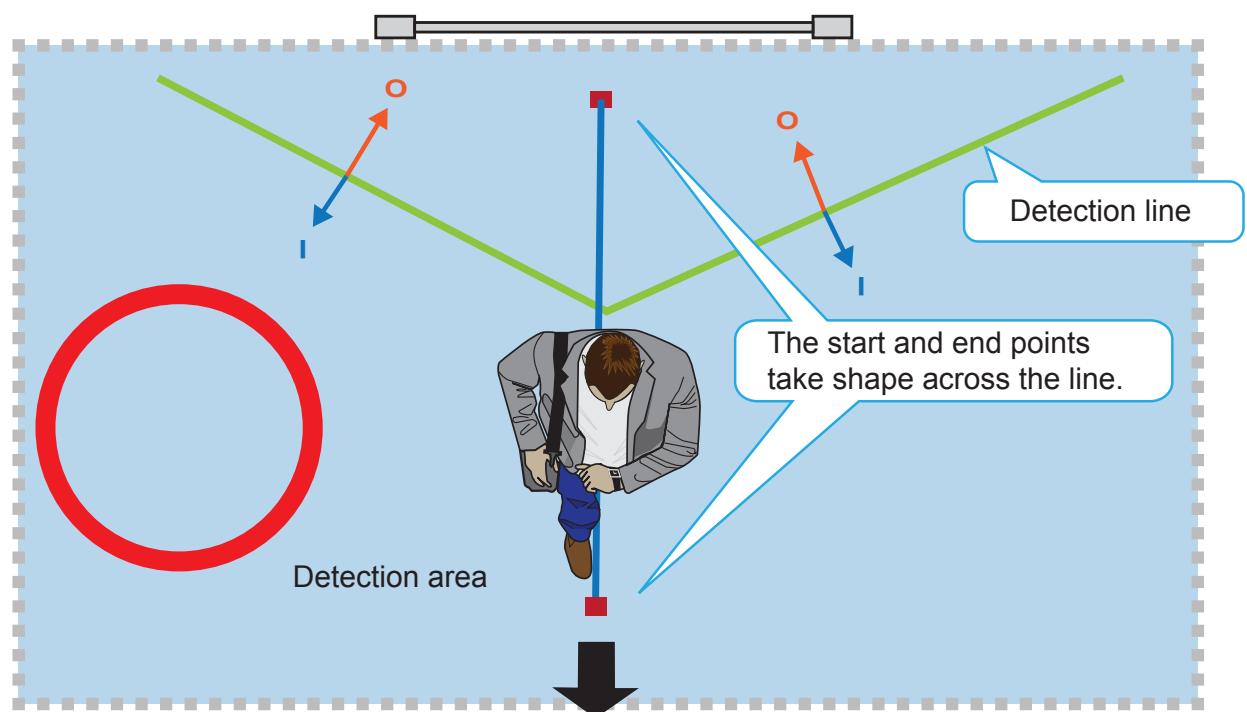
Detection area

10. Always configure the coverage of the detection area in that the complete silhouette of objects can be contained. If only part of the moving object is covered, the counting will fail. The entire object needs to appear in the detection area for the camera to acquire its height information.

Only part of the human is covered by the detection area.

Detection line

Detection area

Object tracking line
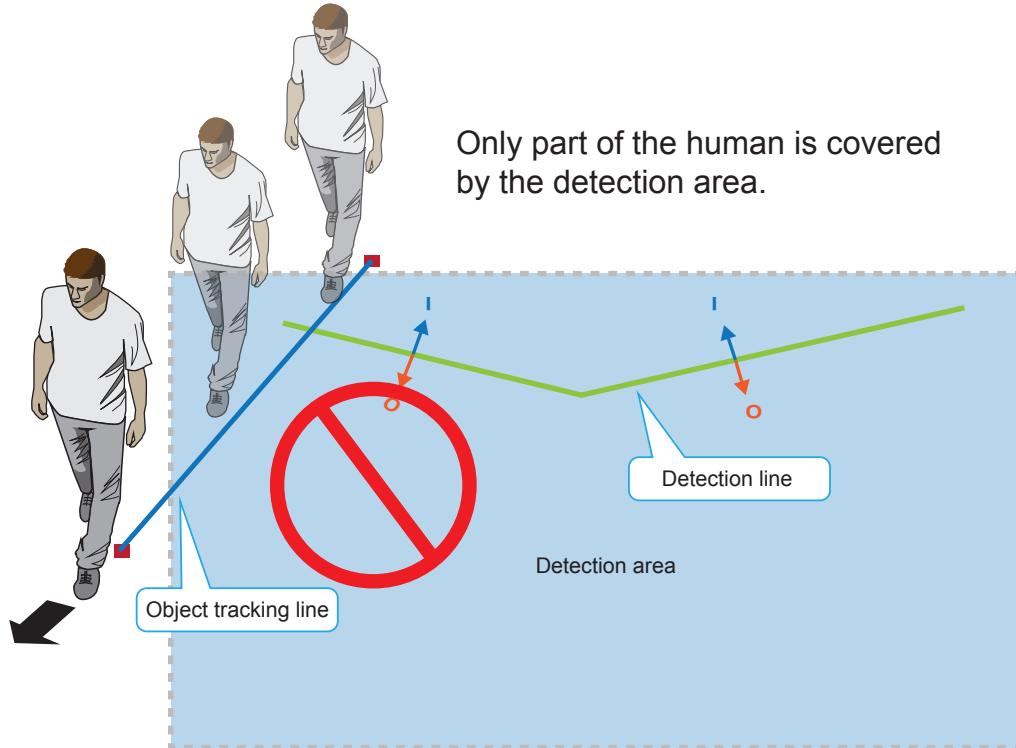
11. Always place the detection line inside the detection area.

Detection line

Object tracking line

Detection area

Start point

Detection line

Object tracking line

Detection area

End point
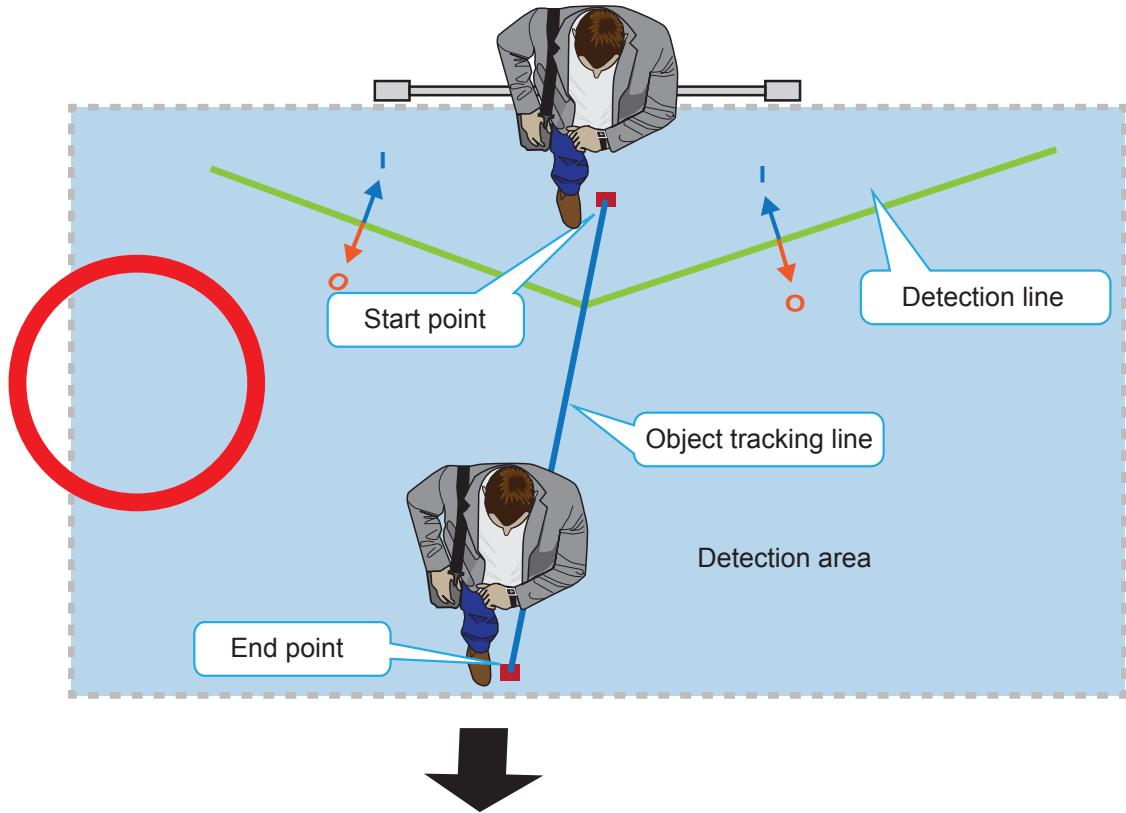
12. If the camera needs to be installed unavoidably at a position higher than 3.6 meters, you can use the Zoom-in mode configuration. See the **Stereo Tracker** > **Configuration** page. See page 51 for related parameters.

Note that if the Zoom-in mode is applied, the zoom-in factor should be set between 1 and 1.8.

Zooming factor = 1

Zooming factor = 1.8

5.7m

13. For Line Crossing and countng configuration, unnecessary objects should be avoided. A door, a floating curtain, and moving objects such as an escalator can cause mistakes with calculation.

14. If the VAST software is used for accumulating counting results, set the counting event notification option to the "real-time" mode.

15. Apply to exclude some regions if the interference should occur near the object trajectories. The camera might acquire incorrect depth estimation if its FOV covers the following materials:

Homogeneous surface -

Patterned surface -
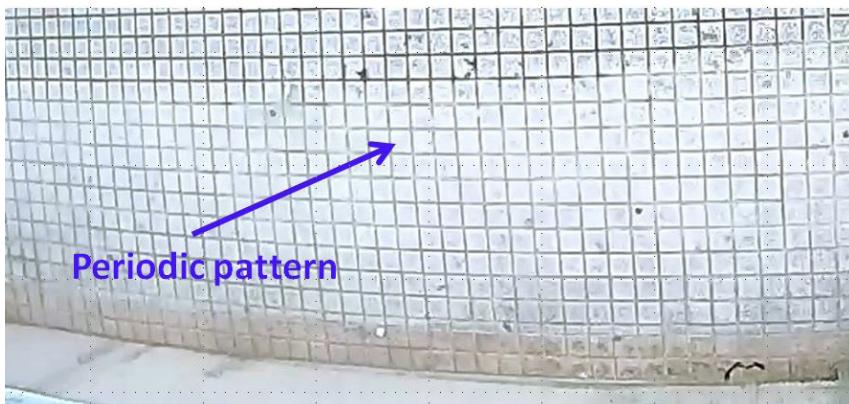
Some other possible sources of interference may include: shadows on the wall, mirrored object image on the reflective surface.

Check if the region exclusive setting should be applied when the Depth view video shows flickering white noises in some regions, or, object trajectories are likely to be trapped within these regions.

📝 **NOTE:**

For software configuration details, please refer to page 196.

Stitching Considerations

The following applies when stitching multiple SC8131 cameras:

1. The **Stitching** configuration takes place on the **Master** camera. 1 Master camera with up to 6 Slave cameras can form a stitiching configuration.

2. All Master and Slave cameras in a Stitching configuration should be running the same firmware.

3. The physical positions of cameras should be consistent with the stitching order. It is recommended you keep a note of all cameras' positions and IP addresses. Static IP addresses are prefereed.
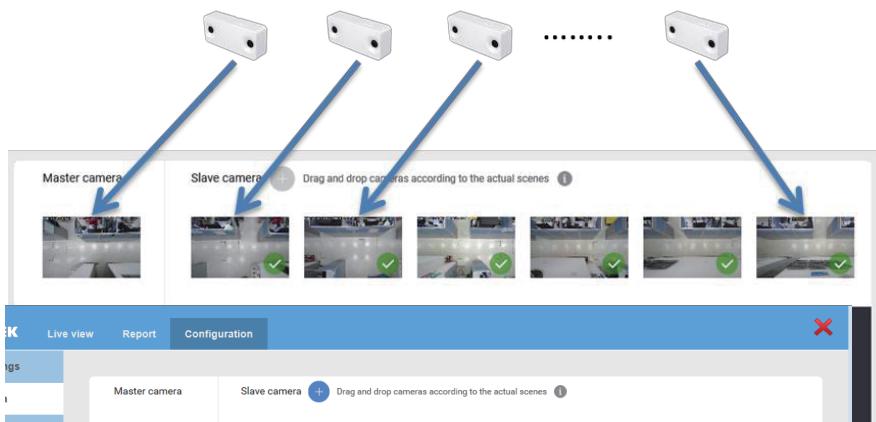
4. Select a camera on the edge of the line as the Master camera.

5. Recruit the Slave cameras via a web console to the Master camera.

6. When software configuration is done, it is best to have human traffic in and through the coverage areas of these cameras. If there are no traffic when you configure the Stitching configuration, you should have someone walking in the overlapped areas.

The peer cameras then automatically calculate the coordinations of the same moving objects that appear in the overlapped FOVs between them. The walking should persist for at least 2 minutes.
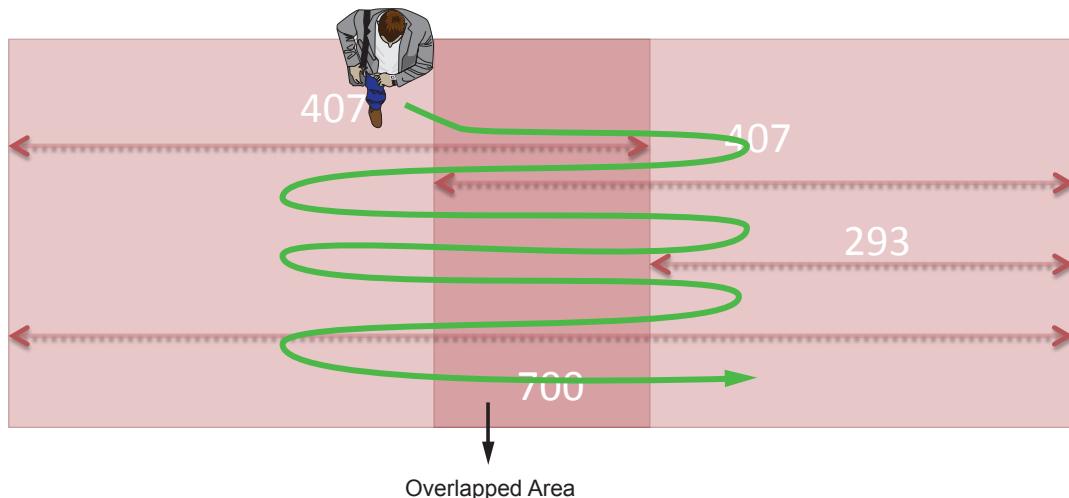
Overlapped Area

The drawing above shows the overlapped area with the cameras mounted at the 3 meters height.

7. Once the Stitching configuration is done, the positioning order of peer cameras will be fixed, and you cannot change their Stitching order unless you unstitch them.

Consider the following when stitching multiple cameras to form a large virtual floor plan:

Height (cm)*	Dist. to the next camera	Combined HFOV
240	140.2	395.0
260	191.1	522.4
280	242.1	598.9
300	293.1	700.8
320	344.0	802.7
340	395.0	904.7
360	446.0	1006.6

* Unit in centimeter.

8. The maximum distance between cameras, when mounted at a height of 300cm, is 278cm (from edge to edge). The FOVs of two cameras must overlap to a certain amount in order to cover people walking between them. An estimation of a man of 185cm tall is applied here.

278cm
293cm
300cm
Combined HFOV
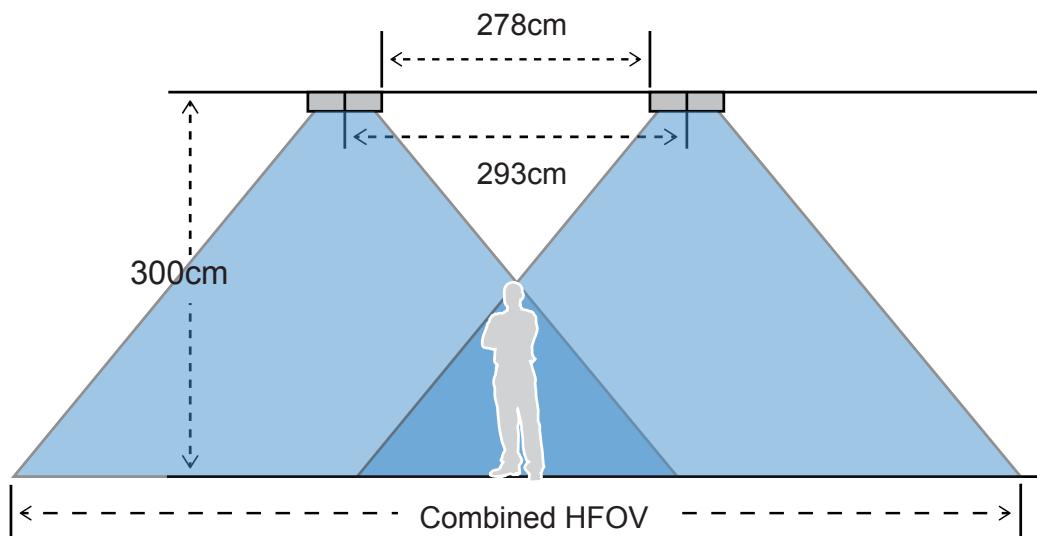
📝 **NOTE:**

• The cameras here are shown on their long side.
• The FOV is the camera's "detecting area."

9. The tracked objects will appear on the live view of a stitched configuration after a 3-seconds delay, due to the network transfer and processing time.

10. It is best that all cameras in a Stitching configuration are installed at the same height and with the same tilt angle (if applied).

Tilt Considerations

1. The camera should be mounted in a downward looking orientation. The tilt and yaw should be level so that it is looking straight down. In some cases, the camera may need to be installed to count the people passing the front of a store's entrance.
2. The camera can be mounted with an angle (20° at most) when it is not possible to install the camera with absolute downward looking.
3. However, when tilted, counting and tracking accuracy can be affected because some people's image may be blocked by other people.

20° most
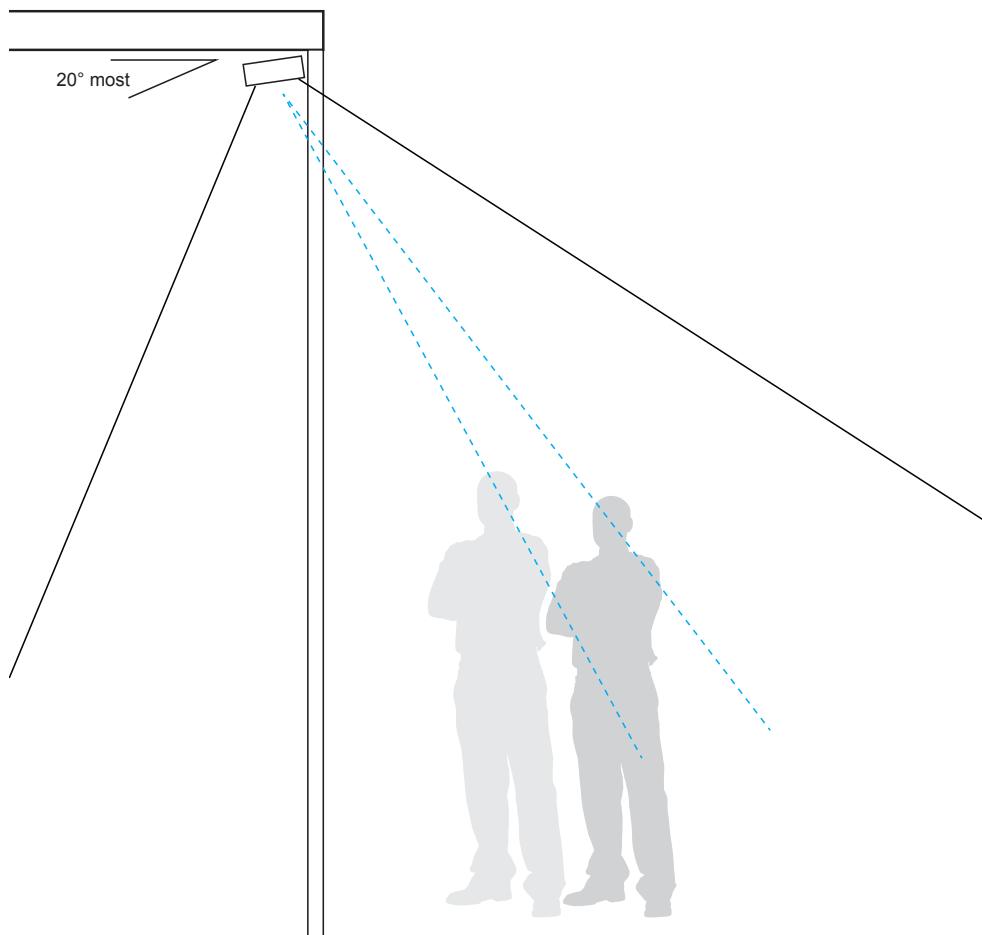
4. The applicable tilt angle and zoom in ratio are listed below:

Height (cm)	Tilt Angle range	Zoom in ratio
2.4 ~ 2.7M	-15º ~ 20º	1 ~ 1.2
2.7 ~ 3M	-15º ~ 20º	1.2
3 ~ 3.5M	-15º ~ 20º	1.4

Queue Analysis Considerations

Design Purpose: Provides a count of people waiting in line and the duration of time of their wait, or the time being serviced. The collected count data can be used by managers to improve staff management, service, and store layout.

The statistics numbers generated by Queue Analysis are listed below:

Length: The number of people stand waiting in the Queue area.

Waiting duration: Service duration is counted once a person enters a service zone. 4 count numbers are available: The Length, Maximum, Minimum, and Average duration. Note that the Max., Min., and Average counts are available only when there is 1 person standing in the Service zone, and others are waiting in the Queue area.

Service zone

Queue direction box
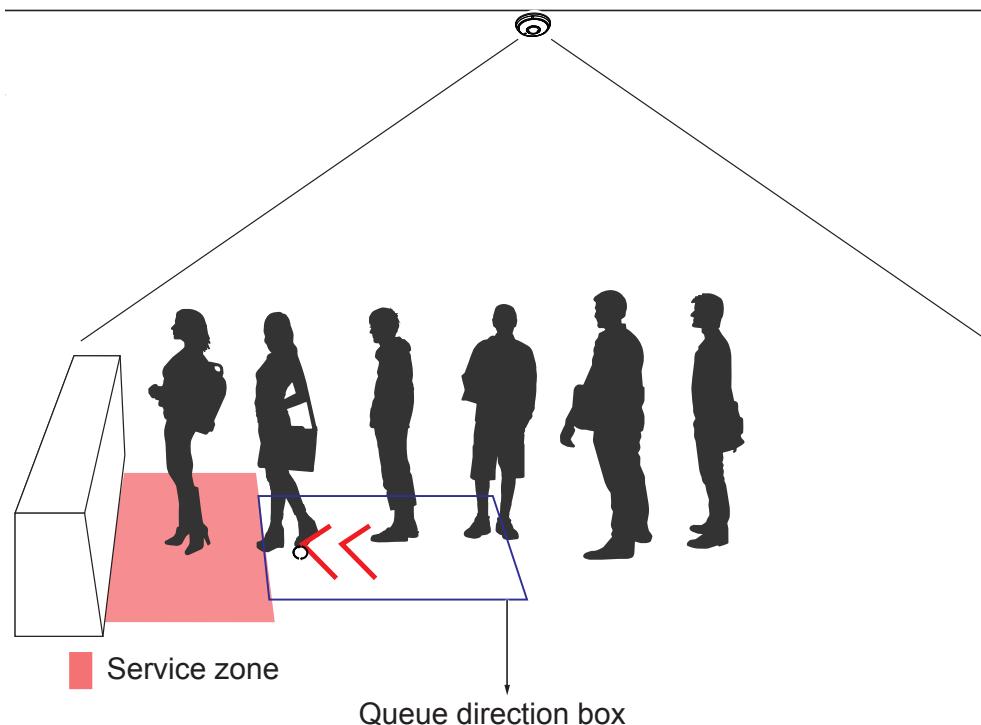
The Service zone should be placed at the position where a person receives services, e.g., in front of a cashier. The Queue direction box should be placed at where the possible waiting line takes place. The arrow marks should point to the service provider, e.g., a clerk. The Queue direction box should cover the length of 1 to 3 persons waiting in line.

The maximum length is 40.

For more information, see page 79 Queue Analysis.

There are counters that have different service positions and wait positions, such as the immigration check counters at the airports. As long as the camera's FOV can cover, you can draw different Service zones and Queue direction boxes at appropriate positions.

Service zone   Queue direction box
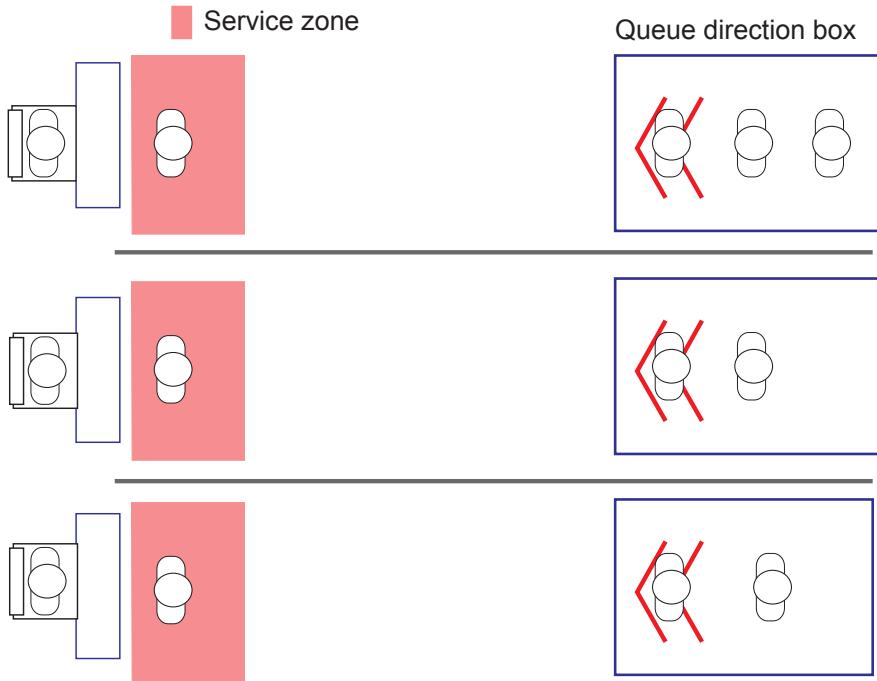
Passer-by Counting Considerations

Design Purpose: Provides a count of people who pass by near an entrance but without entering. The count can be used to evaluate how many people may have shown their interest but lack the motive to enter a store.

The working theory of the Passer-by Counting is illustrated below:

A man walked through the passer-by area and the flowpath: no passer-by count.
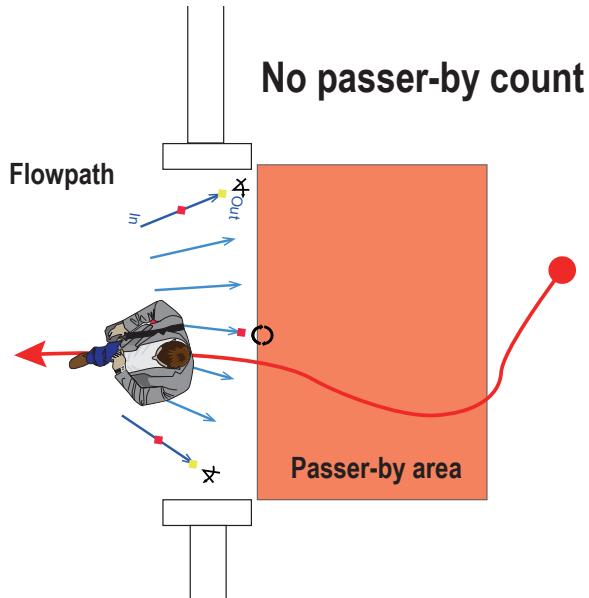
A man walked through the flowpath and the passer-by area: no passer-by count.
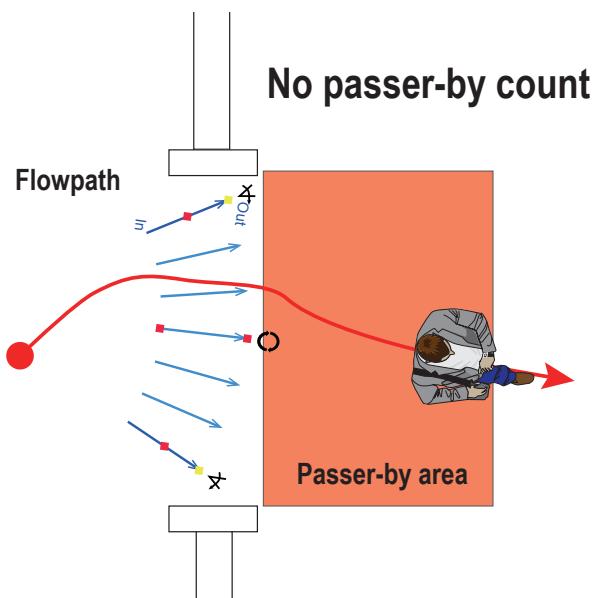
A man walked through the passer-by area but through the flowpath: 1 passer-by count.
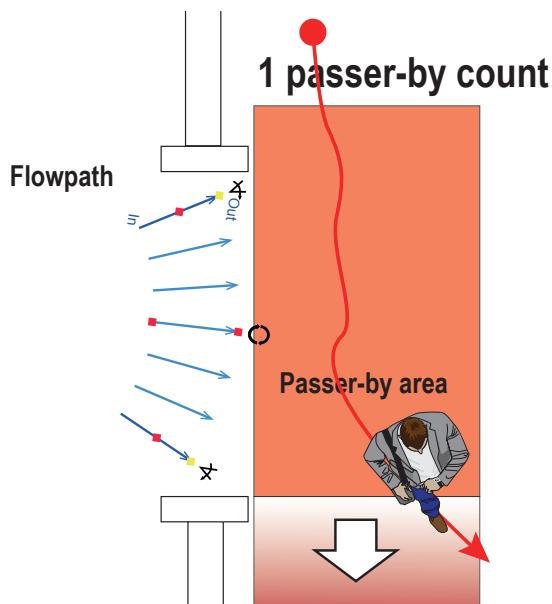
The Passer-by Counting takes effect in both single camera or stitched cameras configurations.

General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

DI- DI+ DO- DO+
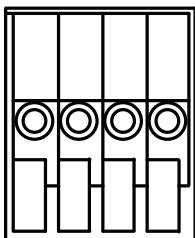
The maximum DO+ 12V output load is 0.5A.

DI/DO Diagram

1. The DO+ pin provides a 12V output voltage.
2. The max. voltage for DO- pins is 30VDC (External power).

   In order to control AC devices, the following diagram can be taken in consideration. This diagram uses a relay to control the ON/OFF condition of the AC device.

3. An external relay can be triggered by using DO+ or by an external power source, depending on the type of relay you use.
4. In case of using an individual relay (instead of using a relay module), for protection against voltage or current spikes, a transient voltage suppression diode must be connected in parallel with the inductive load.

   The 12V connection can be used to energize a relay coil with up to 50mA. If more than 50mA is required, an external power supply can be applied.
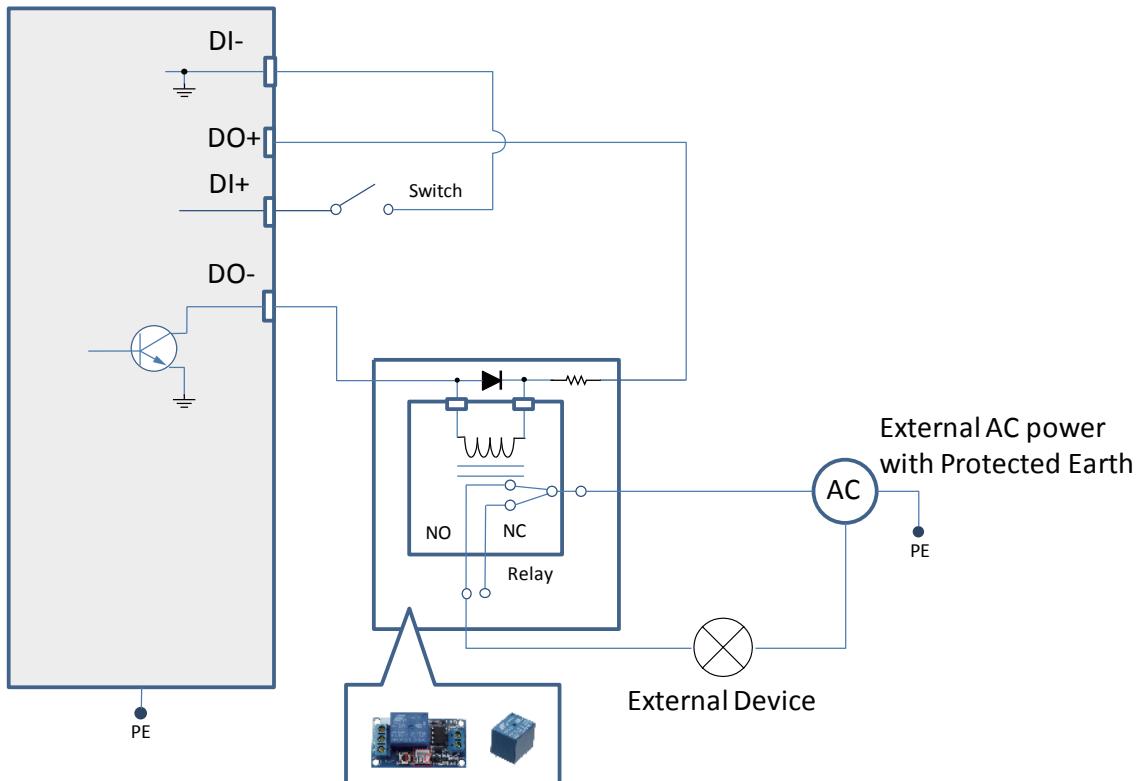
Dry contact with external DC power source to supply a relay. Dry contact is the safest connection to protect devices.
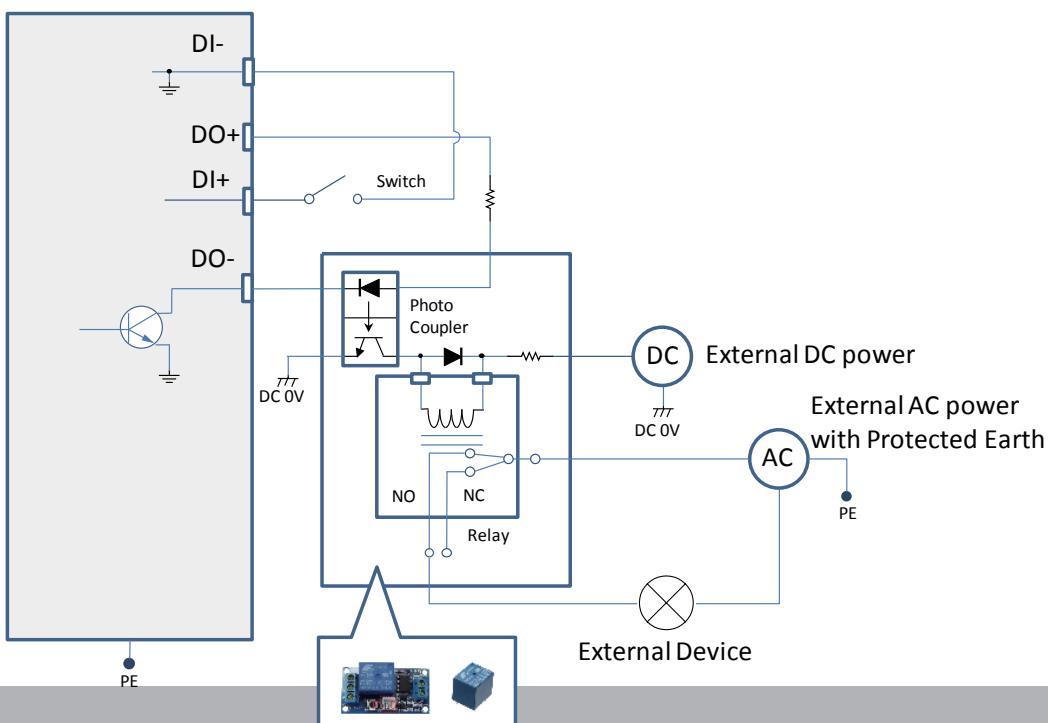
Wet contact with external DC power source to supply a relay.
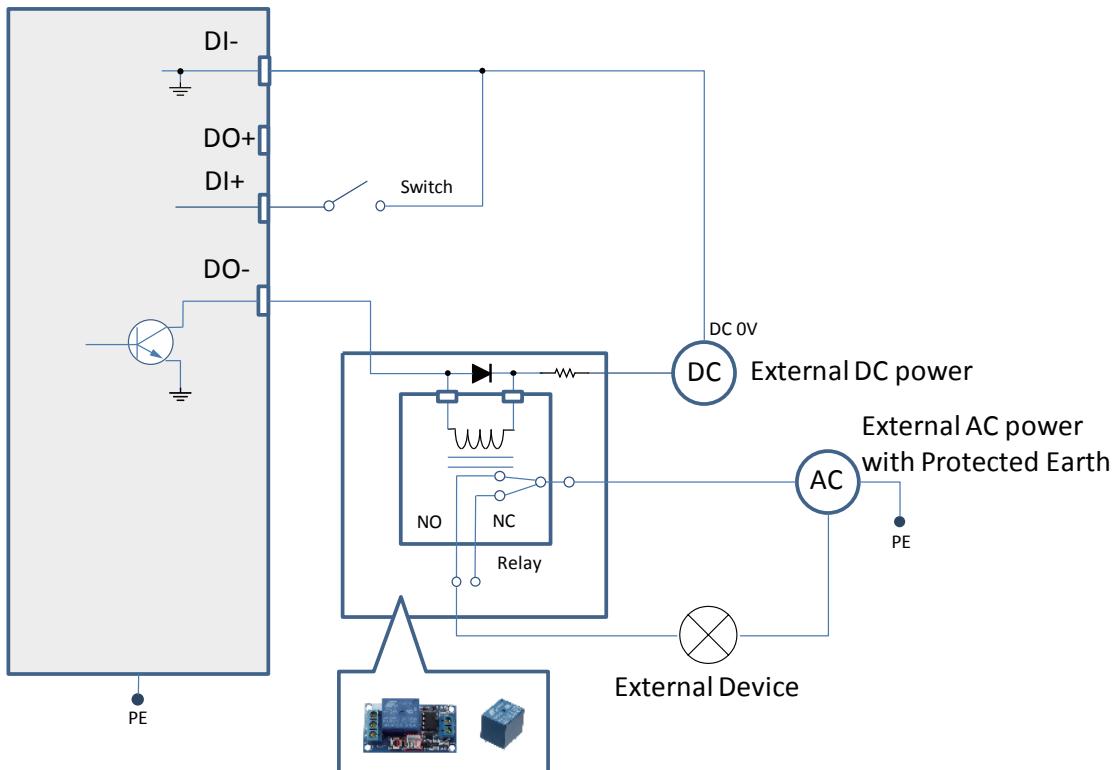
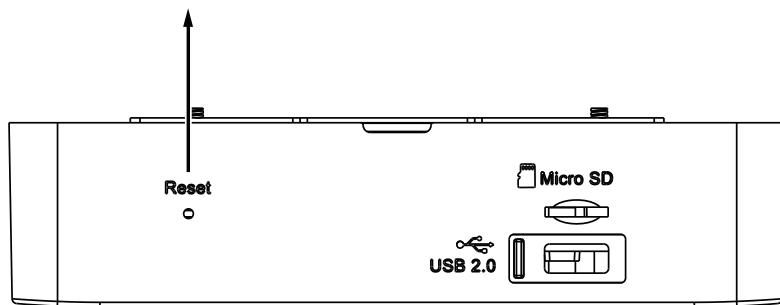Dry contact and using camera's DO+ to supply a relay.

📝 **NOTE:**

The maximum output load from DO pins is 50mA.

Hardware Reset

Recessed Reset Button

The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

Restore: Press and hold the recessed reset button until the status LED rapidly blinks. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

Micro SD/SDHC/SDXC Card Capacity

This network camera is compliant with **Micro SD/SDHC/SDXC 16GB / 8GB / 32GB / 64GB** and other preceding standard SD cards. The SD card should be of a class 6 speed or higher.

LED Definitions

	Item	System status	LED behaviors
LED Definition	1	Restoring defaults	All blinking -> all off -> all on -> all off -> Red on -> all blinking -> all off -> all on -> all off -> Red on -> Red on, Green blinking.
	2	Resetting	All off -> all on -> all off -> Red on -> Red on, Green blinking.

Install the Camera

1. Jot down the camera's MAC address for later reference.

❶

Network Camera   VIVOTEK
Model No: SC8131
MAC: 0002D10766AD
                          RoHS
CE FC C VCI
        xxxxx
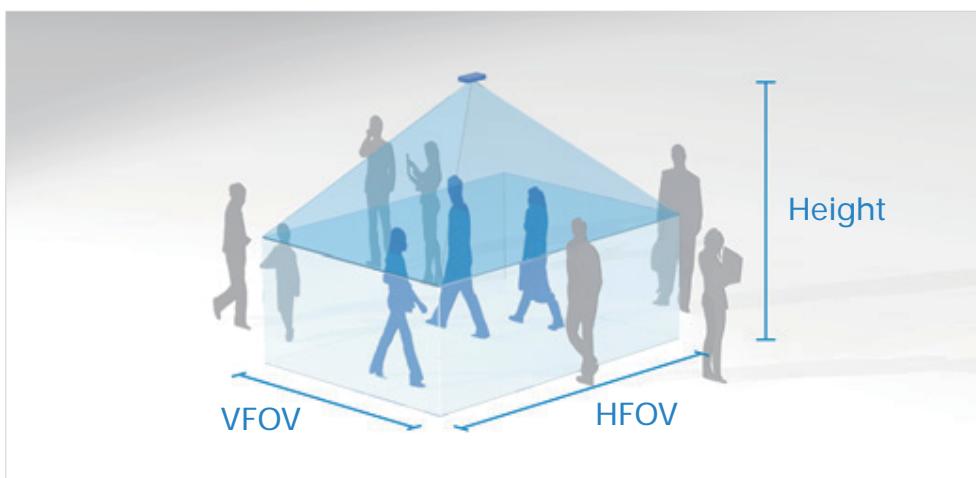Pat.6, 930, 709   Made in Taiwan

❷

2. Plan the installation features, e.g., position and installation height.

Recommended Installation Height

• Installation Height: 2.4M ~ 3.6M
• Coverage area: $1.7M^2$ ~ $5.1M^2$
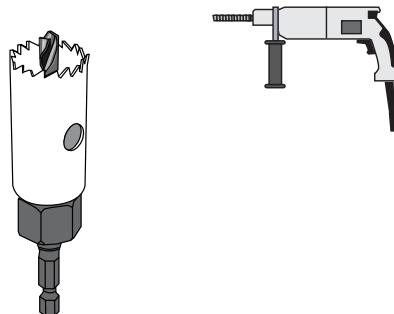

Height

VFOV   HFOV

See page 10.

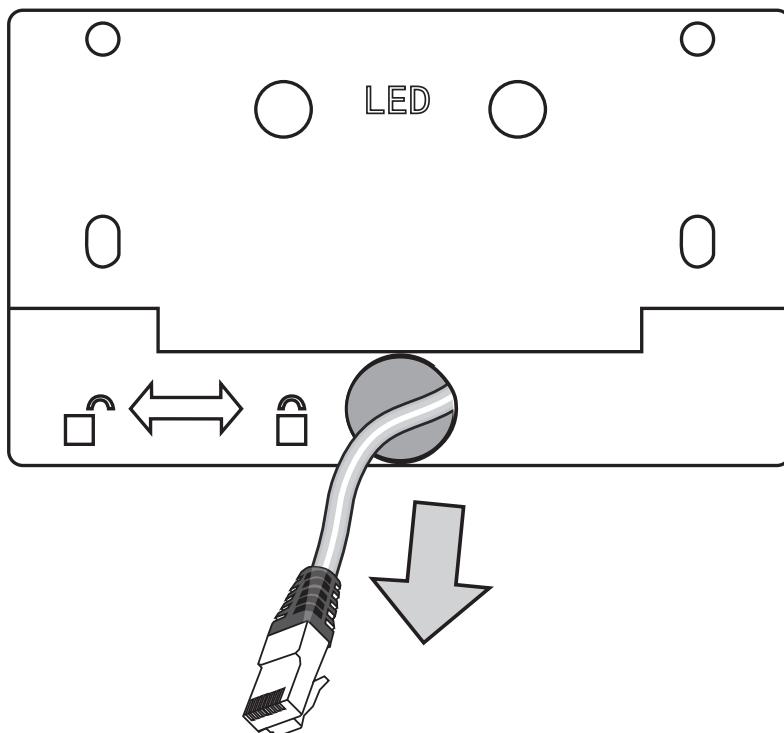## Installation Option A: Using the Mounting Plate

A1 A1. Attach the alignment sticker to a preferred position. If preferred, drill a cabling hole. See below for the diameters of it.
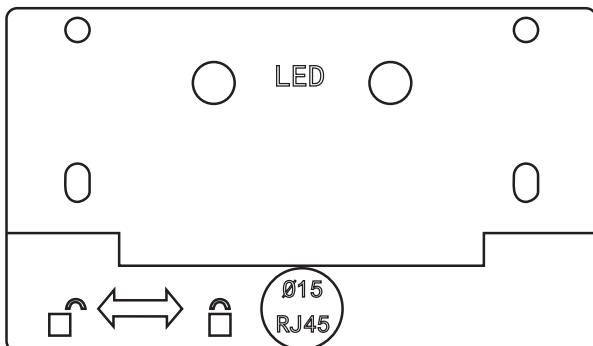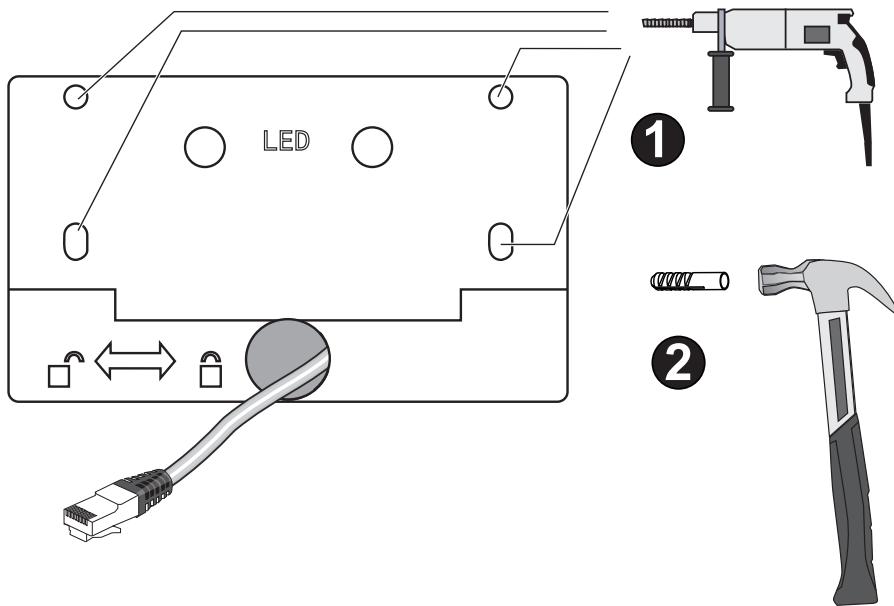

Ø15mm
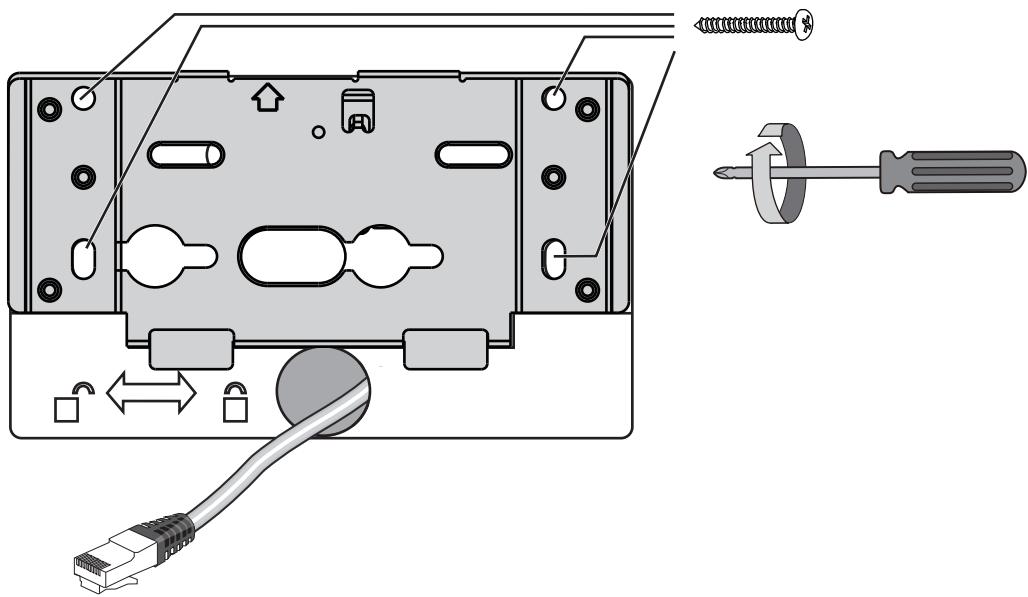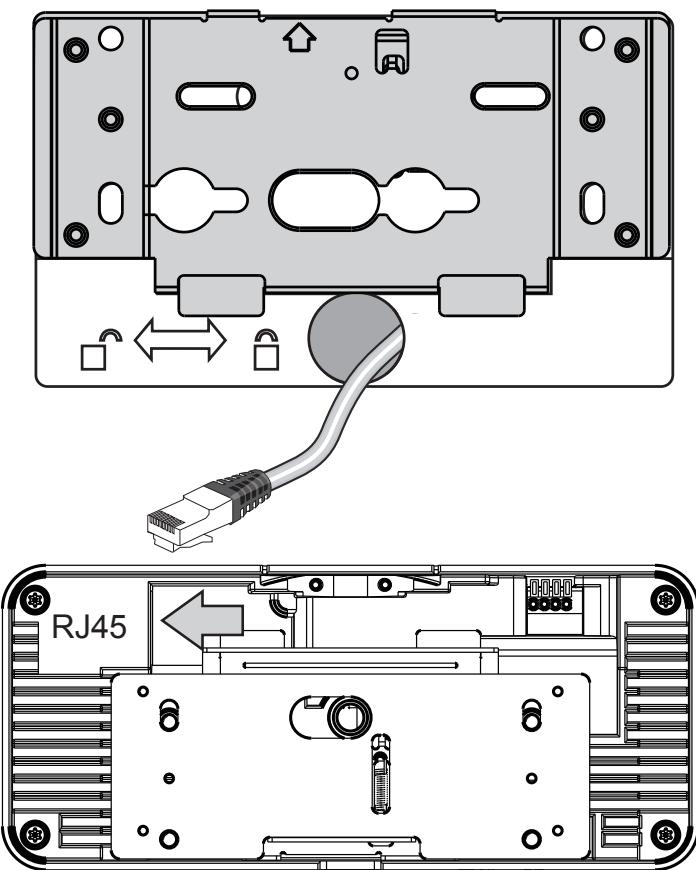
A2 A2. Route an Ethernet cable through the cabling hole.

A3 A3. Drill mounting holes and hammer the included anchors into the mounting holes.

LED

1

2

A4 A4. Secure the mounting plate to ceiling using the included screws.

A5 A5. Connect the Ethernet cable to the camera.

RJ45

A6 A6. Align the camera with the bracket, and slide the camera to the right. The camera will then be securely mounted to the bracket. Note that the side with two LEDs is the top side, and should be aligned with the arrow mark on the mounting plate.
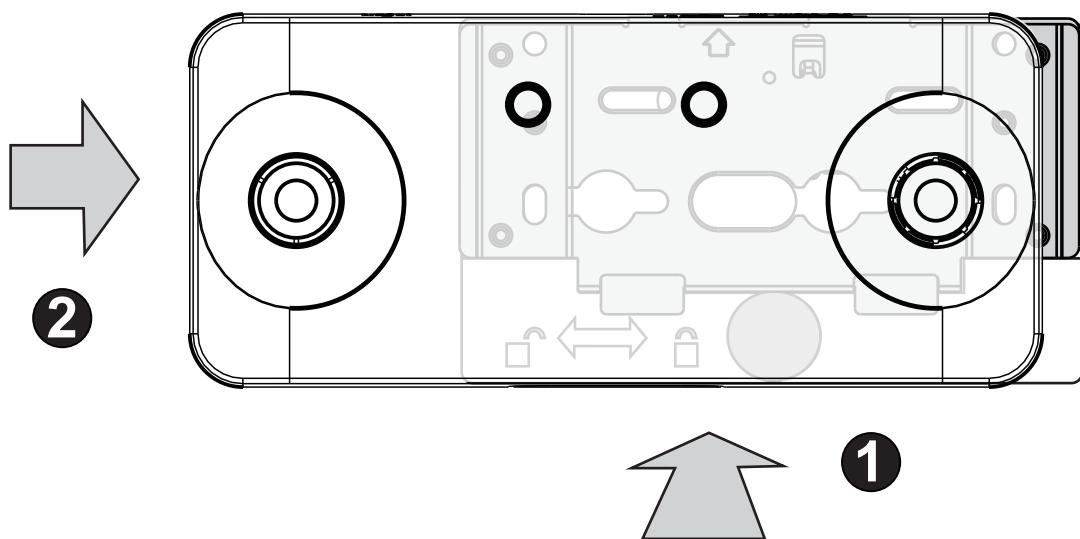
To remove a camera, use a flat blade screwdriver. Press it down against the release tab from the top side and slide the camera to the left.
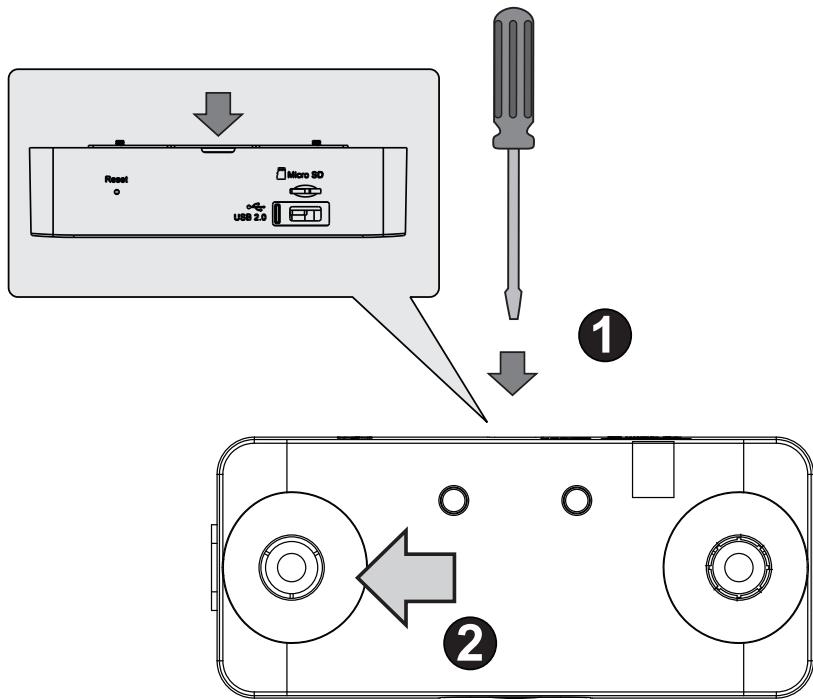
Installation Option B: Using the Camera Stand

B The camera can also be mounted to standard camera stands, such as VIVOTEK's AM-131.
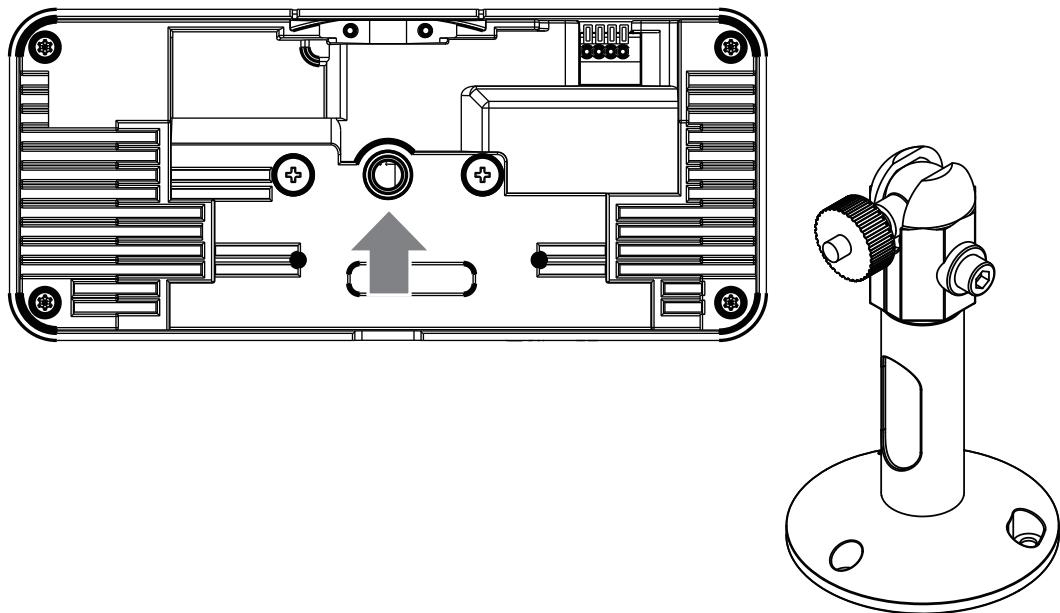
Installation Option C: Mounting to the Single Gang Box

C1 C1. You can also install the mounting bracket to a 4"x2" single gang box.
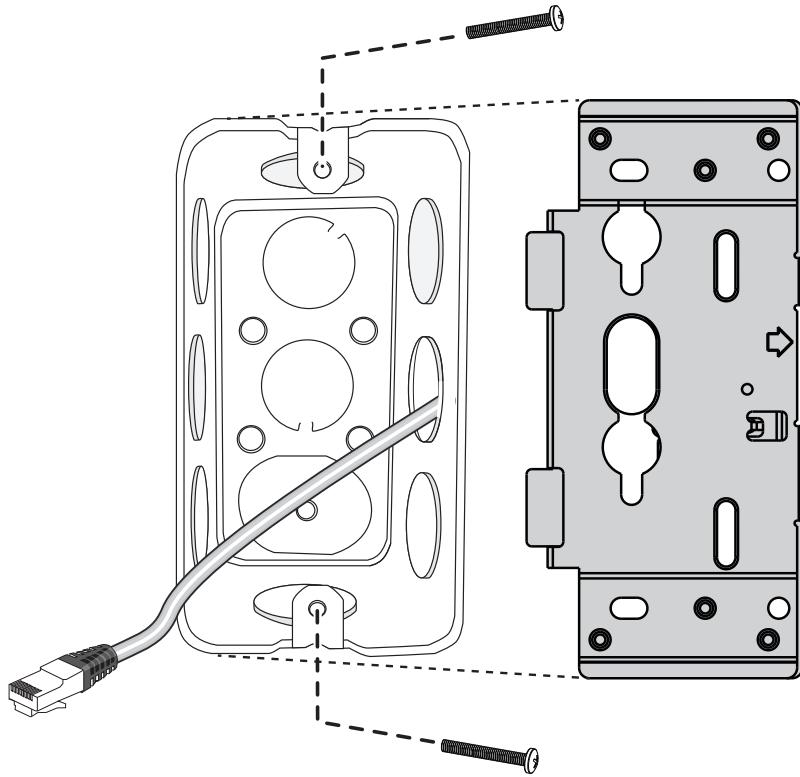
C2 C2. When installing the bracket, press the bracket toward the center of the box so that the bracket can rest firmly on the surface of the box.

See Step **A5** for the rest of the installation procedure.
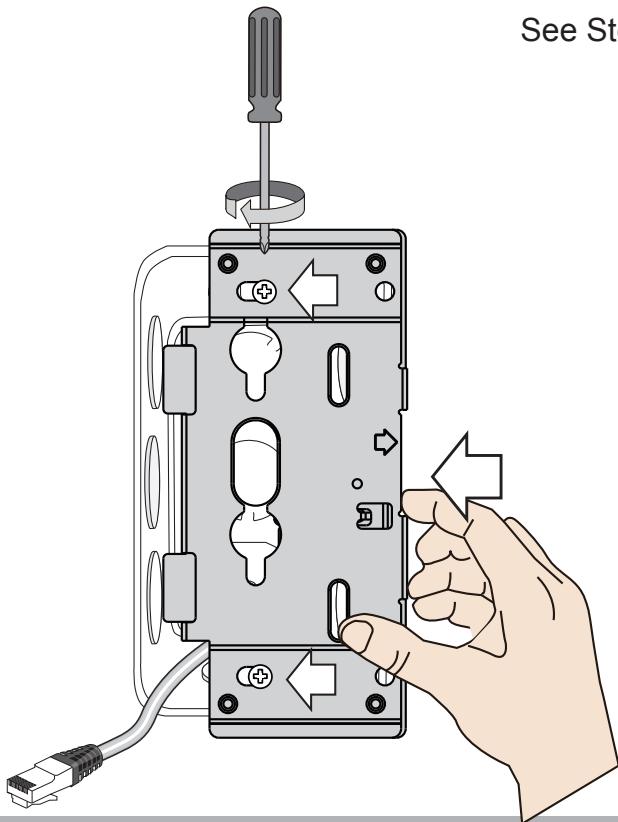
3 When the installation is done, remove the protective sheet.
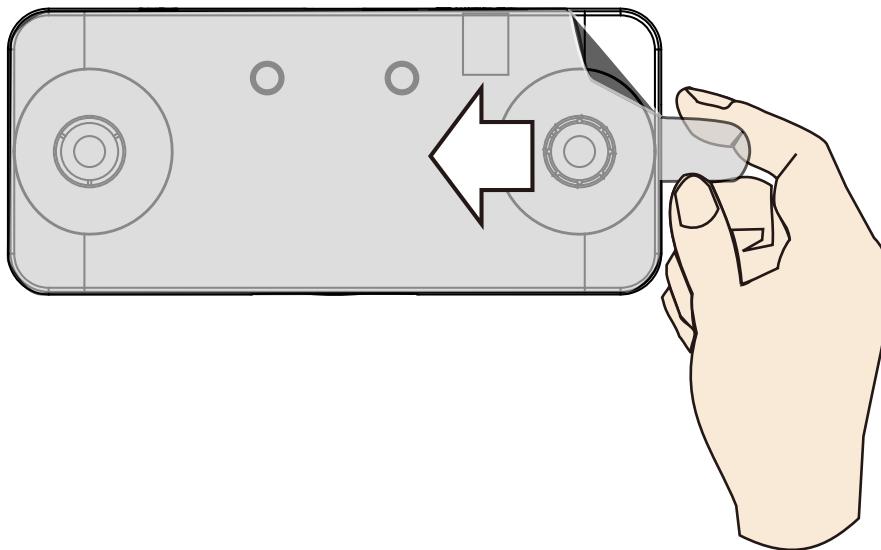
4 Use the Shepherd utility to find and access the camera. Open a web console with the camera.

The default user name and password is **root** / **root**.

5 You can use the shortcut on the home page or open the **Configuration** > **Application** > **Package** management page to access the tracking and counting configuration utility. Please refer to page 51 for the configuration details about the embedded **Stereo Tracking** and **Counting** functionality.

NOTE:

- The camera is only to be connected to PoE networks without routing to outside plants.
- For PoE connections, use only UL listed I.T.E. with PoE output.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 43 for details.
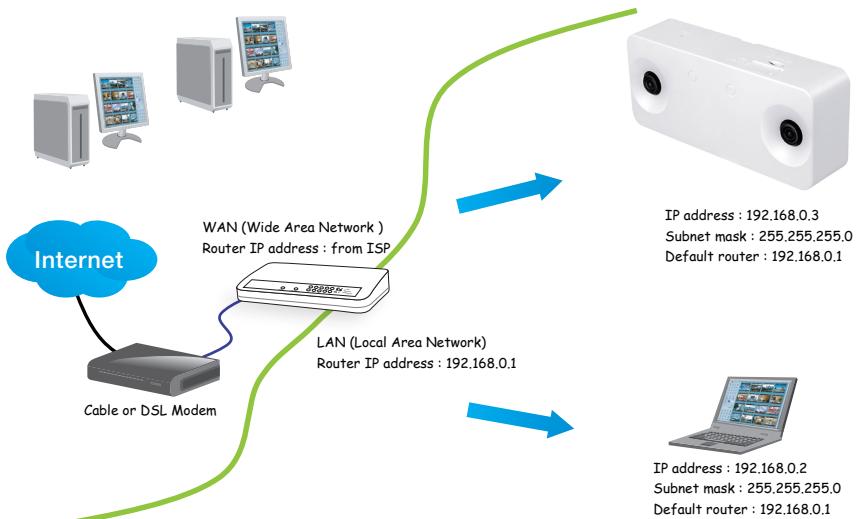
2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

   ■ HTTP port: default is 80
   ■ RTSP port: default is 554
   ■ RTP port for video: default is 5556
   ■ RTCP port for video: default is 5557

   ■ Websocket port: default is 888

   If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 161 for details.

For example, your router and IP settings may look like this:

Device	IP Address: internal port	IP Address: External Port (Mapped port on the router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 1 Websocket port	192.168.2.11:777	122.146.57.120:777
Camera 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

Configure the router, virtual server, or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

When properly configured, you can access a camera behind the router using the HTTP request as follows: http://122.146.57.120:8000

If you change the port numbers on the Network configuration page, please open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. Please consult your network administrator for router configuration if you have troubles with the configuration.

For more information with network configuration options (such as that of streaming ports), please refer to Configuration > Network Settings. VIVOTEK also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.
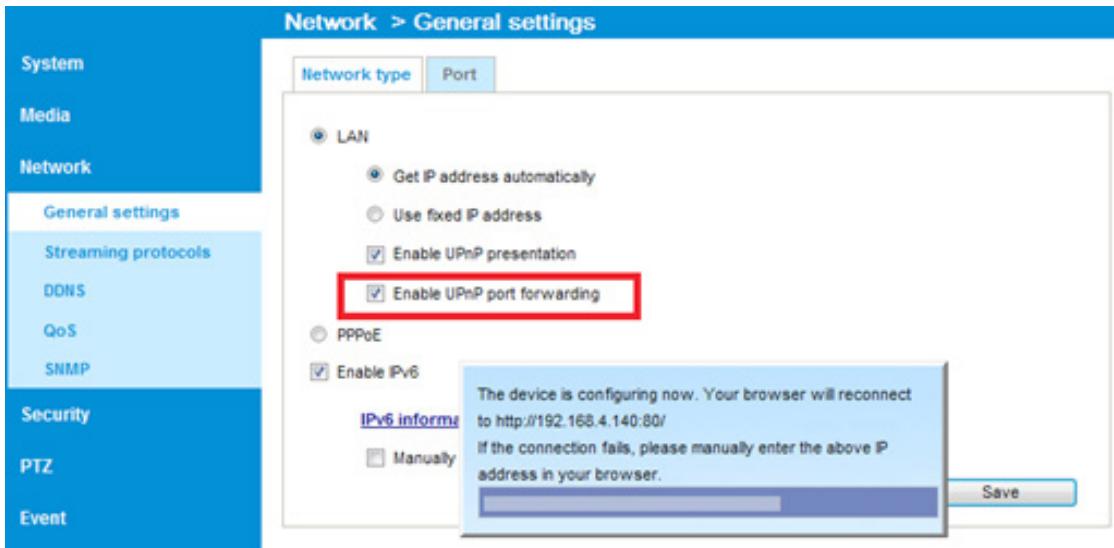
Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN setting on page 161 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 162 for details.

Software Installation

1. Install the **Shepherd** utility, which helps you locate and configure your Network Camera in the local network. If your camera comes without the CD, go to VIVOTEK's website, and locate the utility in the Downloads > Software page.

2. Run the Shepherd utility.

3. The program will conduct an analysis of your network environment.
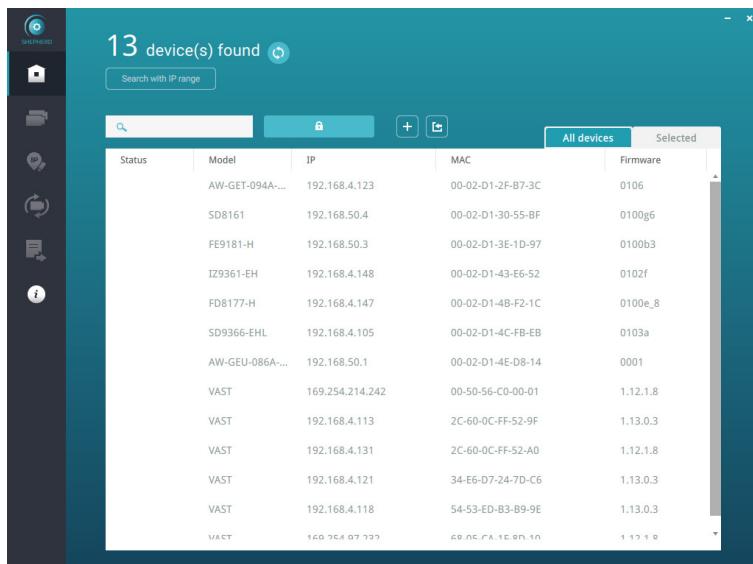
Ready to Use

1. A browser session with the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access the Network Cameras on LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:
1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will prompt as shown below. Follow the instructions to install the required plug-in on your computer.
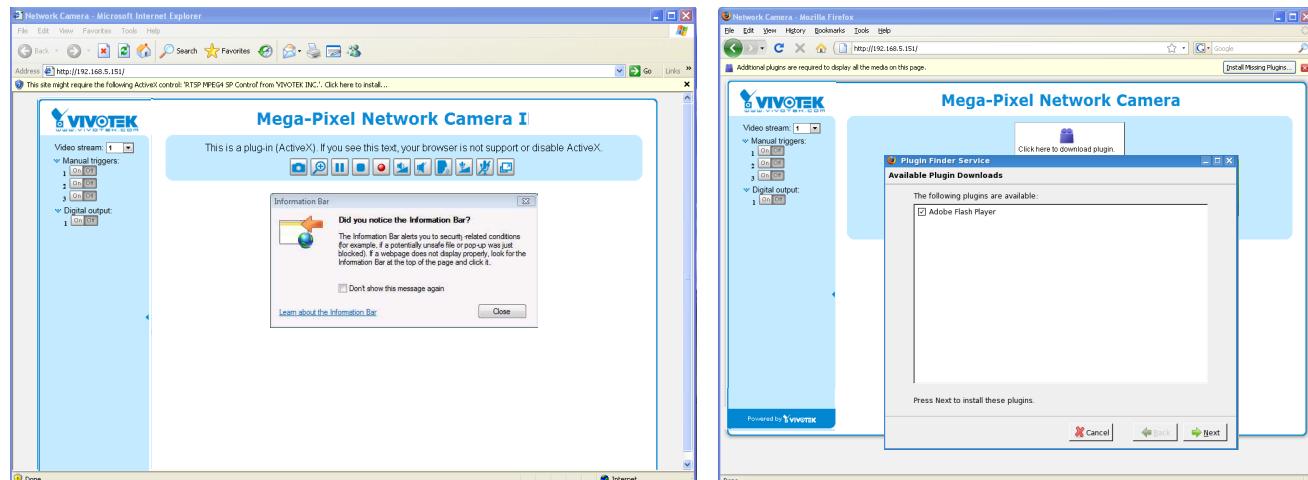
> ✎ **NOTE:**

► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.*
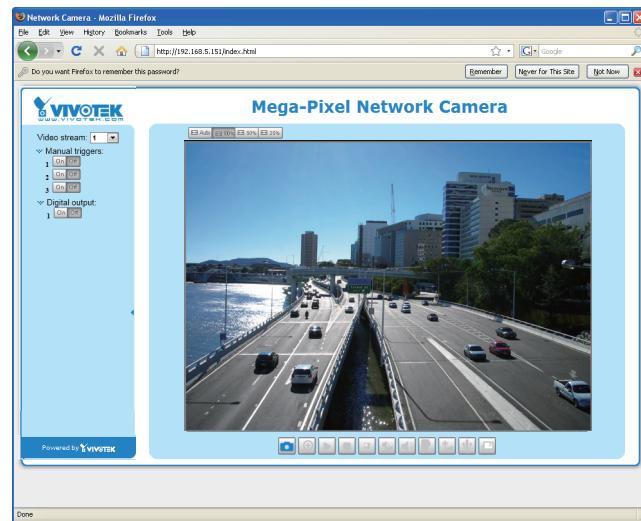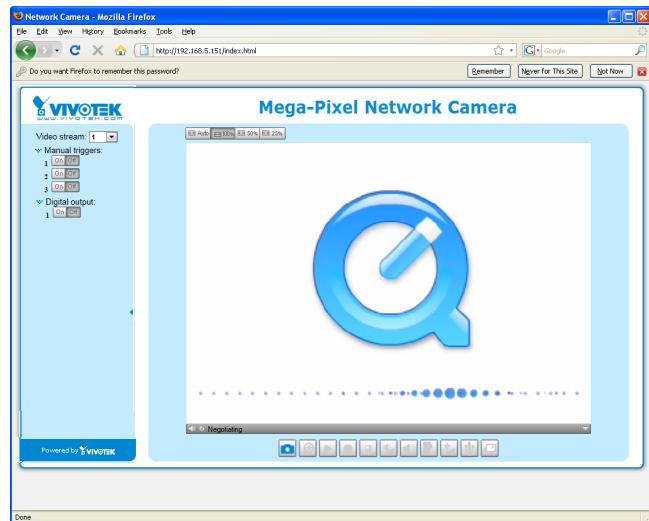
► By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.
For more information about how to enable password protection, please refer to Security on page 178.

► If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.

1. Choose Tools > Internet Options > Security > Custom Level.
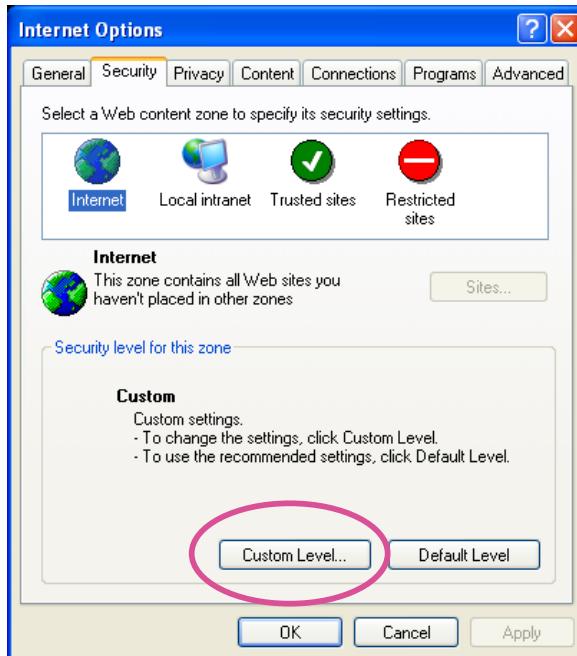
2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.
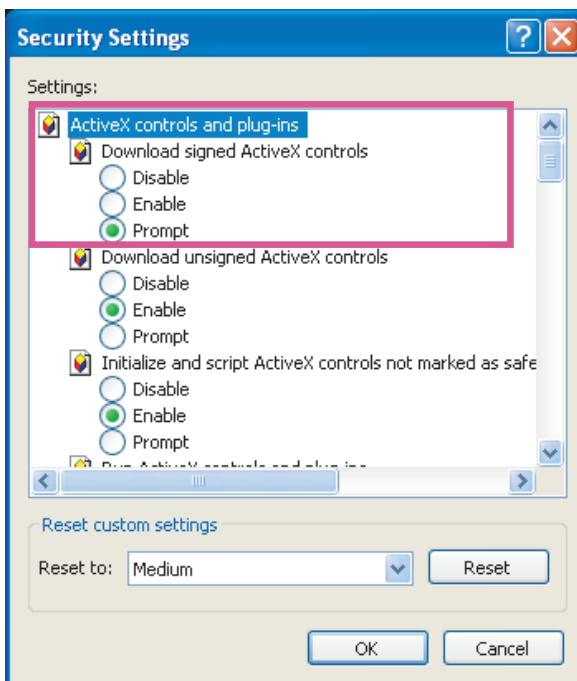
3. Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.

⚠ **IMPORTANT:**

1. While observing and acquiring counting results from the camera, please avoid connecting the camera from more than one client computer! Multiple web sessions can stress the camera.

2. If you are operating the latest VIVOTEK Rossini series cameras, the Java plug-ins that came with them may cause compatibility issues on the browser. Try remove the plug-ins.

📝 **NOTE:**

· For a megapixel camera, it is recommended to use monitors of the 24" size or larger, of the 1600x1200 or better resolutions.

🔅 **Tips:**

1. The onscreen Java control can malfunction under the following situations:

   A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.

2. In the event of plug-in compatibility issues, you may try to uninstall the plug-in that was previously installed.

3. If you forget the root (administrator) password for the camera, you can restore the camera defaults by pressing the reset button for longer than 5 seconds.

4. If DHCP is enabled in your network, and the camera cannot be accessed, run the IW2 utility to search the network. If the camera has been configured with a fixed IP that does not comply with your local network, you may see its default IP 169.254.x.x. If you still cannot find the camera, you can restore the camera to its factory defaults.

5. If you changed your network parameters after IW2 was started, such as adding a connection to a LAN card, re-start the IW2 utility.

Using RTSP Players

To view the video streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

VLC media player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 169.
For example:
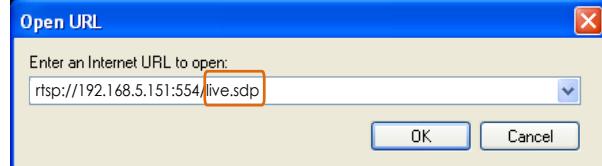
4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 169 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 36.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 169.

2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video streaming parameters as listed below.
   For more information, please refer to Stream settings on page 159.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 169.

4. Launch the player on the 3GPP-compatible mobile devices (e.g., QuickTime).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream # with small frame size and frame rate>.
   For example:
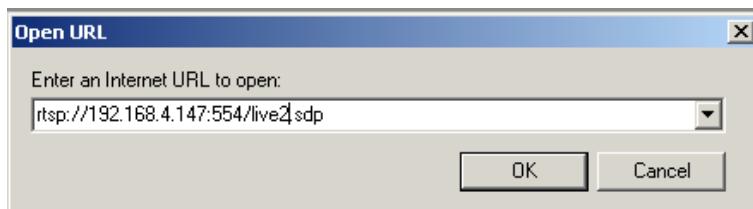
You can configure Stream #2 into the suggested stream settings as listed above for live viewing on a mobile device.

Using VIVOTEK Recording Software

The product software CD also contains a VAST recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

Stereo Tracker

> ✏️ **NOTE:**
>
> • For the design and configuration rules, please refer to page 13.
>
> • For a management session across a firewall or router (over the Internet), it is necessary to open a **Websocket port 888** (or secure port 889) on your router using the NAT traversal method for transferring metadata for counting. The default Websocket port can be changed in the Network port setting page.

Click on **Stereo Tracker** to start the embedded module in the **Application** > **Package management** page. The shortcut is also available on the main page.

1. Live View.

You will be defaulted to the **Liveview.** See below for the information on the Liveview.
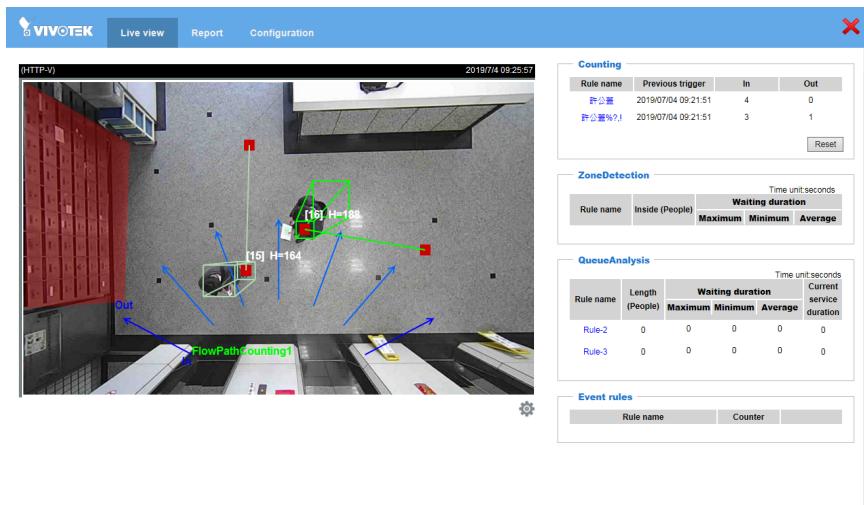
By default, the Single eye view displays. With people passing the scene, the color cubic rectangle will display to highlight a moving object. The start and end points will be linked to indicate the direction of the movement. An index number as well as the approximate height of the object will also display.
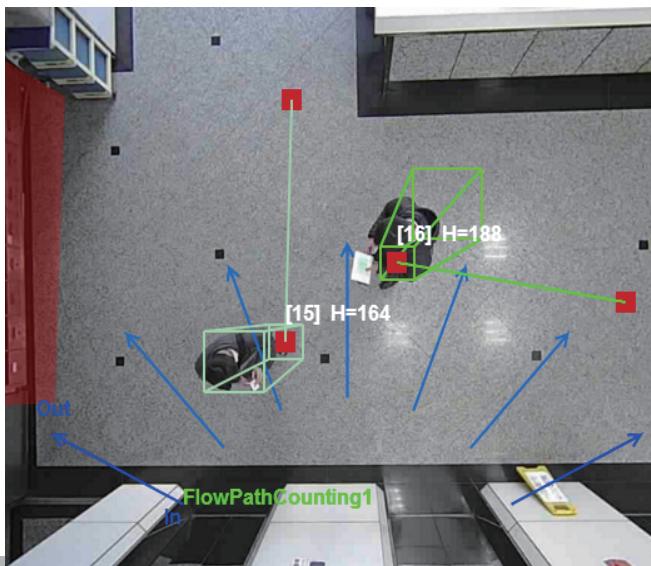
- **Display elements**: Click on the display button ⚙ at the lower right to select the count indicators.
    1. Show exclusive area: displays the exclusive areas, if configured.
    2. Show start stop map: displays the start and stop points of moving objects captured by the camera.
    3. Show object ID: displays the sequential number assigned to moving objects.
    4. Show object height: displays the height of moving objects.
    5. Show objection duration of stay: displays the duration of stay of a moving object in the detection area. The number is useful for evaluating queueing and service time.

☑ Show exclusive area
☑ Show start stop map
☑ Show object ID
☑ Show object height (H=Height)
☑ Show object duration of stay (T=Time)

⚙
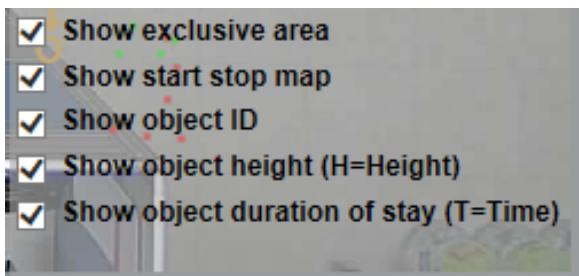
✏ **NOTE:**

The start and end points of a moving object will only appear when the object eventually disappears from the scene. If the object only lingers in the area, the start and end points may not appear.

The counting only takes effect when a moving object is detected, then moves across the detection line, and finally disappears from the area. The start stop map allows you to see where tracking starts and ends so that you might adjust the detection zone.

Tips

If you encounter the display problems with the Stereo Tracking window, try the following:

1. Try clear the browsing history. Sometimes, plug-ins from the previous browser sessions may still affect the current session.
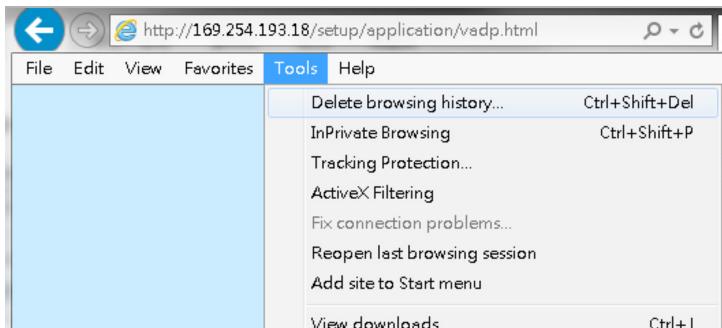
2. Press the F12 key when you open the IE10/IE11 console window. Make sure you are not running the browser in the Compatibility mode.

2. Report

The Report page displays an instant graph showing the activivities in a day's span. You can also export the collected data using the **Export data** pane below. Select the time span, UTC time (Coordinated Universal Time), file format, and interval. Note that polling the data from camera may take several minutes.

Select a configured rule to review the collected metrics accumulated by the camera.

1. Rule name: Selects a configured rule.

2. Search from: Specifies the span of days. Click to open a calendar. When done, click on the **Search** button.

The span of days will be listed on screen. You can click on any of them to view the count data. The count results will be listed in the Table or Chart view.

Note that you can click on the **In**/**Out** buttons to disable either the In or Out counts on chart. The disabled count will be indicated by a cross-out.

When in a single day and in the Chart view, you can use the Interval menu to select a different time interval. The interval serves as a scaled time axis. When choosing rougher granularities, the data collected during that span of time will be combined.
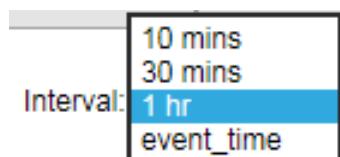
The report page also supports the display of the Queue Analysis results. Select a pre-configured Queue Analysis rule. Select a day or spans of days. The accummulated results can be displayed in a chart.
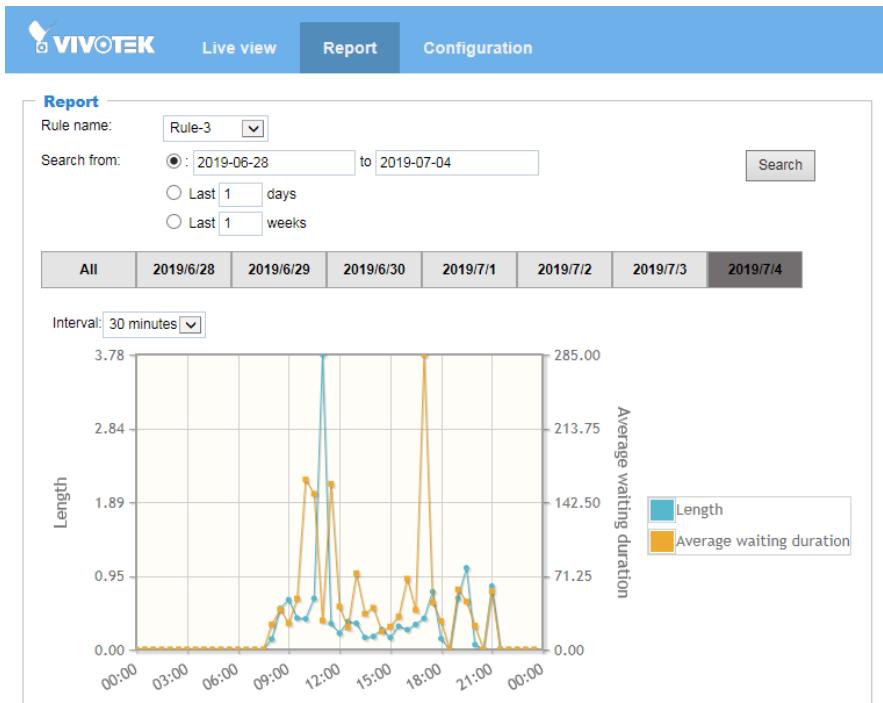
You can single-click to disable a display element. For example, you can choose to display the Average waiting duration. Click again to restore the original view.
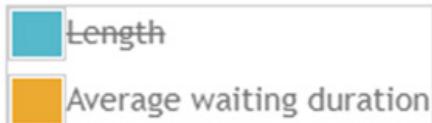
Export Data

The Export data window allows you to manually export all analytics results. Up to 2,000 entries will be stored on the camera. Users can export the report using the XML, CSV, or JSON format with the granularity of 1, 5, 15, 30 minutes, or 1, 12, 24 hours.

Select the date and time carefully using the calendar tool. Click on any number of the From time or to time entry field to bring up the calendar tool.

Event triggers: If event triggers have been configured, e.g., too many people have been detected in a detection zone, the events will be included in the exported data. See Configuration > Event rules.

CGI: You can click the CGI button to produce a line of CGI command. Copy and save the command for later use or to be implemented elsewhere. This command can specify and retrieve video counting results.

3. Configurations

To start configuring the tracking and counting rules, click on **Configurations.** The **Camera settings** window will appear.
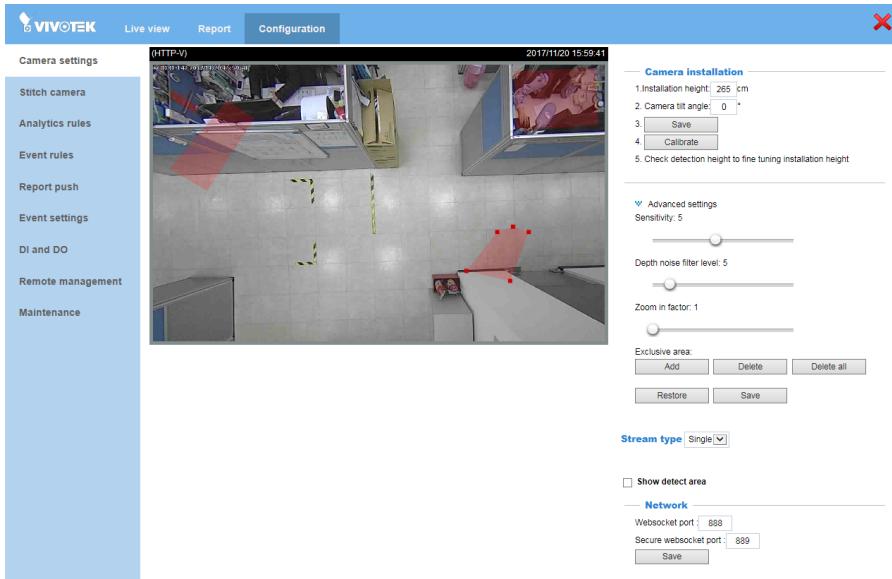
3-1. Configuration - Camera settings

The Camera settings page contains key parameters related to the physical characteristcs at your installation site. You need to carefully tune the parameters to acquire the best detection results.
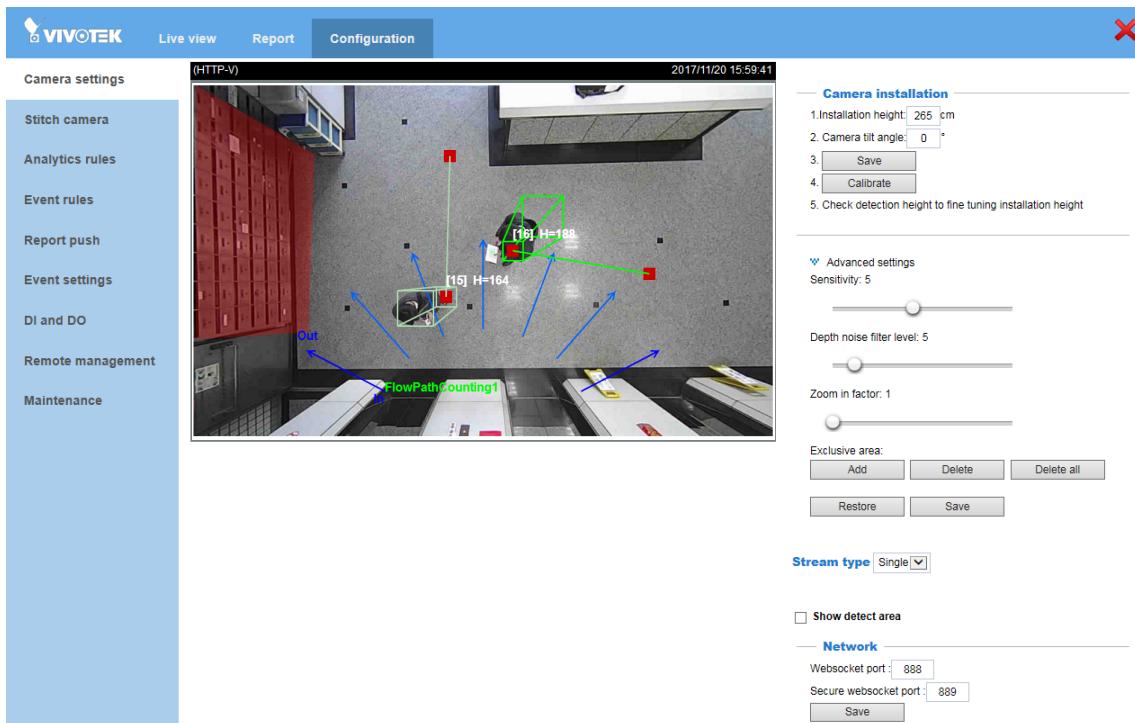
- **Installation height**: It is recommended you measure the installation height of the stereo camera and enter the number. Use a laser distance meter for an accurate number.

  If you were measuring the ceiling height (from floor to ceiling), please delete the height of the camera canister (4cm). You may also measure the height from floor to camera canister.

- **Calibrate**: Users can calibrate the installation height especially when installing the camera for the first time. The calibration function helps verify the correctness of the dual-lens depth map in the stereo vision. The correctness of such vision can be affected by incorrect intallation. Please note that errors can occur if you install the camera in a faulty condition, e.g., at a place that is too low.

  Also note that you should avoid using the function with heavy traffic in the scene while the calibration is taking place. When calibration is done, the management screen will be refreshed.

  The following message will prompt if errors occur during the calibration.

Calibrate failed! Please try again.

Please check informations below:

1. Camera mount on a suitable height

2. Objects are masking visions

3. People fast motion during the calibration
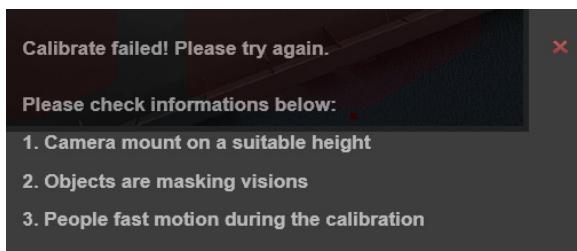
  Check detection height: Check the height number detected by camera and compare with the the actual height you measured. Adjust the installation if necessary.

Advanced settings   (click to expand the configuration menu)

- **Sensitivity**: This refers to the effectiveness level of human head shape and depth differential algorithms for human activity detection. You may try to tune up or tune down the sensitivity level and oberve the result in the Liveview window. However, if your installation site contains a lot of misleading objects, e.g., complex scenes with numerous non-target moving objects, setting the sensitivity level too high may result in false inputs.

- **Depth noise filter level**: An analytics mechanism filters out unreliable depth correlation data in cases where homogeneous surface or periodic pattern scene exist. Chances are it may be impossible to ignore these regions because objects may still pass through these regions.

  - **When to consider increasing the Depth noise filter level?**

    Sometimes, the floor itself may consist of homogeneous surface or patterned materials. In such cases, it is not possible to draw exclusive regions to get rid of these regions because the moving object will inevitably pass these regions.

    The Depth noise filter level is useful when you need to suppress the interference from homogeneous or patterned surfaces on the floor. Increase the level to suppress possible interference. However, if the level is too high, the depth information of moving objects may also be suppressed, resulting in the chance of losing objects' movement tracks.

    If the interference is very significant and the Depth noise filter level must be set to a higher value, try increase the Sensitivity level to reduce the possibility of losing object tracks. You can check if the Depth noise filter level should be increased. For example, the Depth view video shows significant flickering white noises in the floor area.
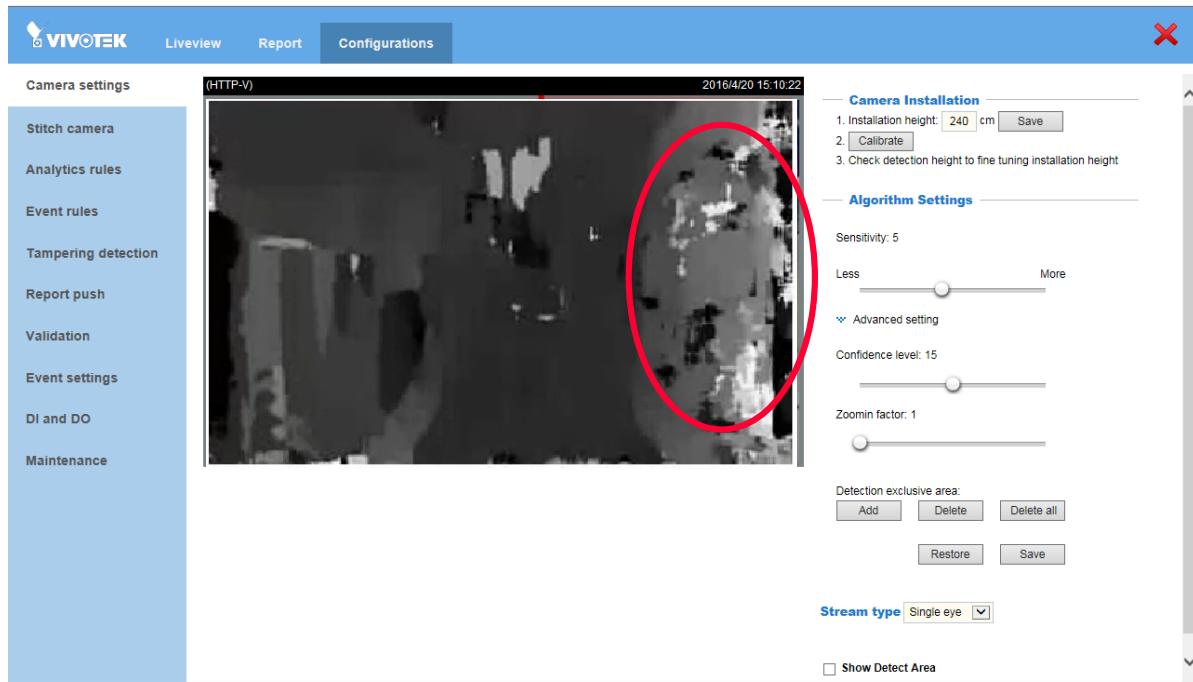
Object trajectories are likely to be trapped in these regions

This is the view of the installation site. The white wall is unavoidable.
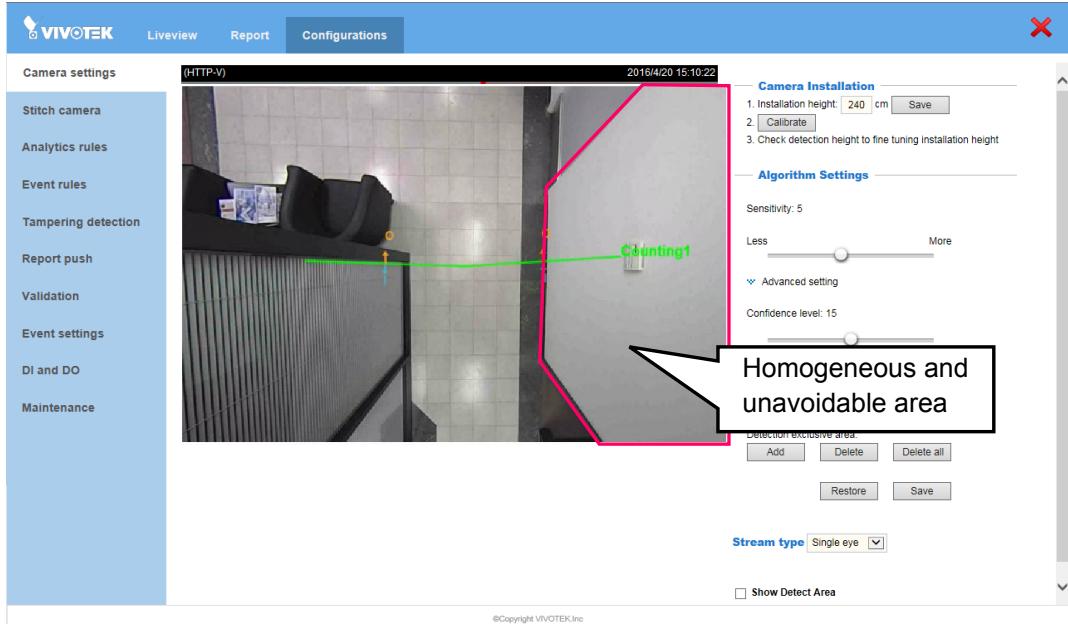
Shown below is the result when the Depth noise filter level is tuned up. White noises have disappeared.
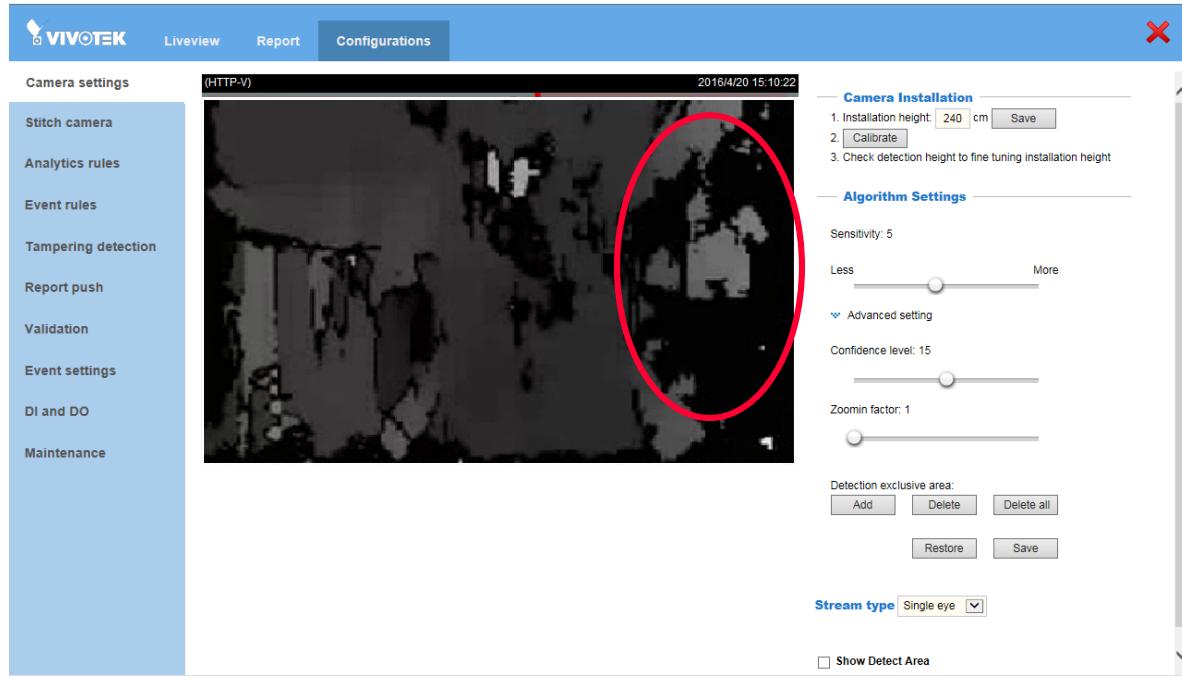
- **When to consider decreasing Depth noise filter level?**

  If camera installation height is higher, the effective area of a person moving in the depth map will be smaller.
  If camera installation is higher than 3.3 meters, it is recommended to revise the following settings to minimize the possibility of losing objects' tracks.

  In this case, you can decrease the Depth noise filter level in order to preserve more depth information.

  You can increase the sensitivity level to keep good track of objects with their depth information.

- **Zoom-in factor**: The digital zoom-in applies when the camera installation height is higher than 3.6 meters. The tradeoff is that you may lose some of the field of view.

- **Exclusive area settings**: This allows you to exclude certain areas in your field of view from tracking detection: such as a table, a mono-color wall, a surface of a different height, mirror, objects that are reflective, glass door, and shadows. The Exclusive area should not cover the floor.

  Up to 8 polygon "exclusive" windows can be created using multiple mouse clicks on the screen (create peripheral points). Click on the peripherals of the target area (polygon). At least 3 clicks are required, and up to 20 clicks can be applied to define an exclusive area. Conclude the exclusive area by clicking on the initial point the second time. You can create multiple exclusive areas. Double-click on the last corner point to complete an exclusive window.

  Click **Add** if you need more exclusive windows. Click **Save** to preserve your configuration every time you created an exclusive window.

  If necessary, repeat the process to create more exclusive windows.
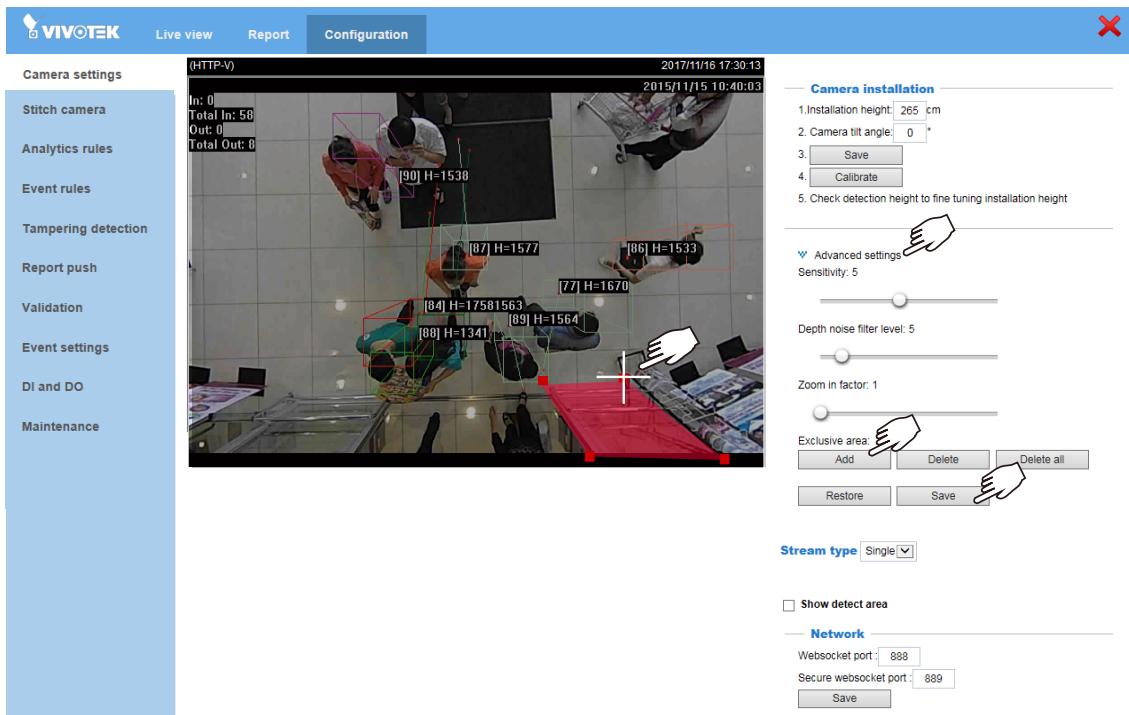
- **Stream type**:

The following display options are available:
* Single Eye Rectified HD video (up to 1280x960)
* Depth view video (320x208)

See the Configuration > Camera Settings page.

- **Show Detect Area**: Select to display the effective detection area currently enabled by your analytics rules. Note that this area may not display if you have no effective rules.

  Due to the visual perspective of the camera mounted on top, a person enters the scene from the edge of the FOV with his feet appearing first, and then his/her head. Only until he/she comes to a place directly underneath the camera, the head and fee positions can be aligned. A person's feet are detected first, and if a detection line is configured too close to the border, a person may not be appropriately recognized when his/her head has not entered the FOV.

  The conceptual drawing below shows a camera view at a low installation height.
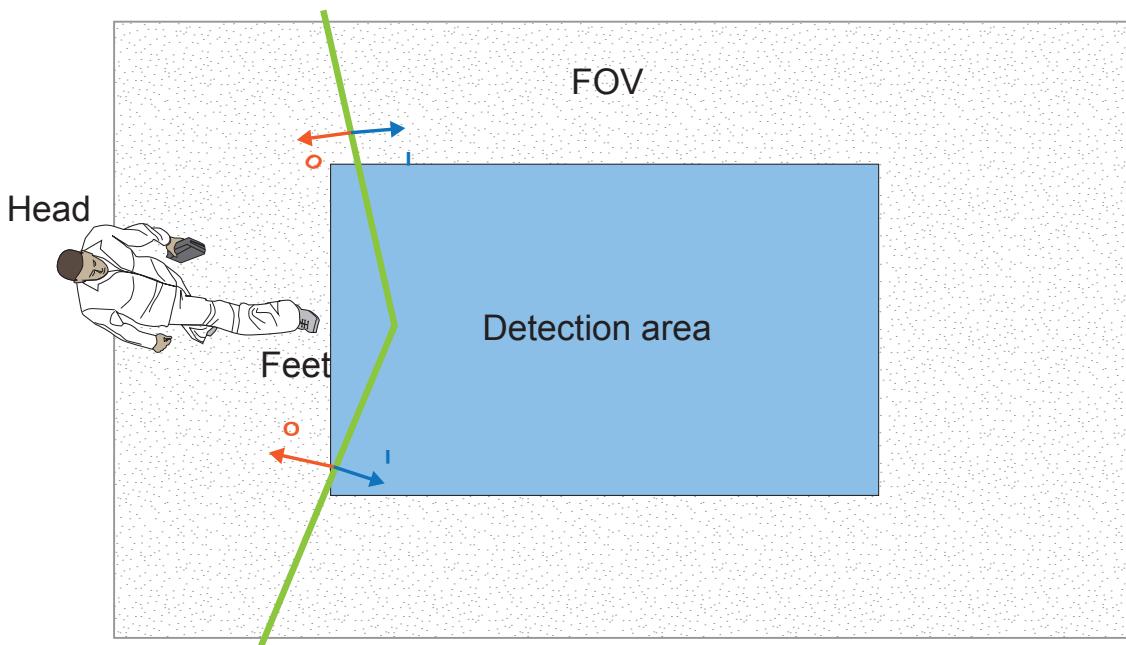
- **Network**:
  Websocket port: The Websocket enables two-way communications between browser-based applications with servers that does not rely on opening multiple HTTP connections, in order to avoid long polling. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The protocol provides an alternative to HTTP polling from a web page to a remote server.

  For a management session across a firewall or router (over the Internet), it is necessary to open a **Websocket port 888** or a secure port **889** on your router using the NAT traversal method for transferring metadata for counting. The default Websocket port is also user configurable.

3-2. Configuration - Stitch camera

Video Stitching can be used to bring up to 7 SC8131s together to provide video analytics over a large and wide floor plan. Count lines can then be be applied individually or across the FOVs of multiple cameras to cover a wide area.

⚠ **IMPORTANT:**

It is very important that all cameras in a stitched view configuration have an identical **time**, **time zone**, and **DST** configuration. Without an identical time and time zone settings, problems will occur with the statistics report.

It is highly recommended that all cameras be configured to be listening to an NTP (Network Time Protocol) server.

To stitch up cameras in a Stitching configuration,

   1. Click on the ⊕ Add button.
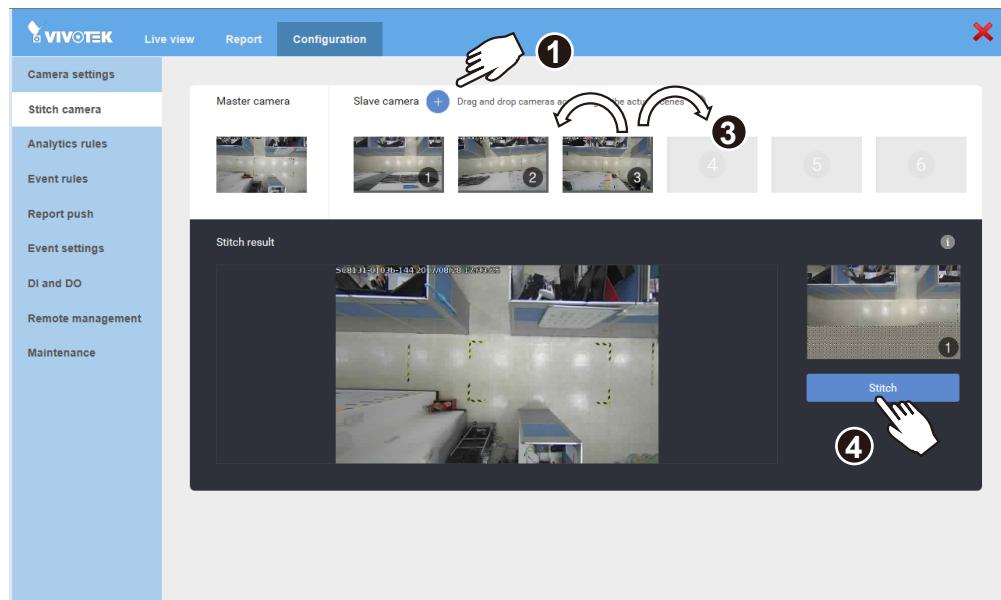
2. Enter the IP addresses of the cameras that will serve as the Slave cameras. Enter the credentials if they all use the same credentials.

It is recommended that you configure a static IP for all Master and Slave cameras.
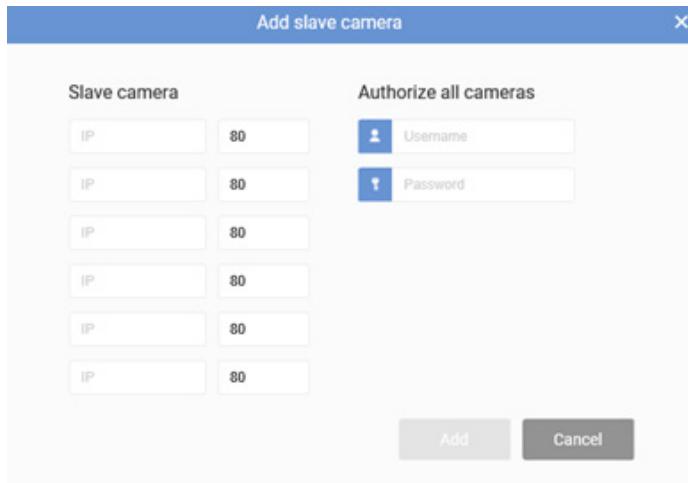
3. The stitching order on screen must coincide the physical locations of Slave cameras. Observe the screenshots, and click and drag the cameras into the correct positions.
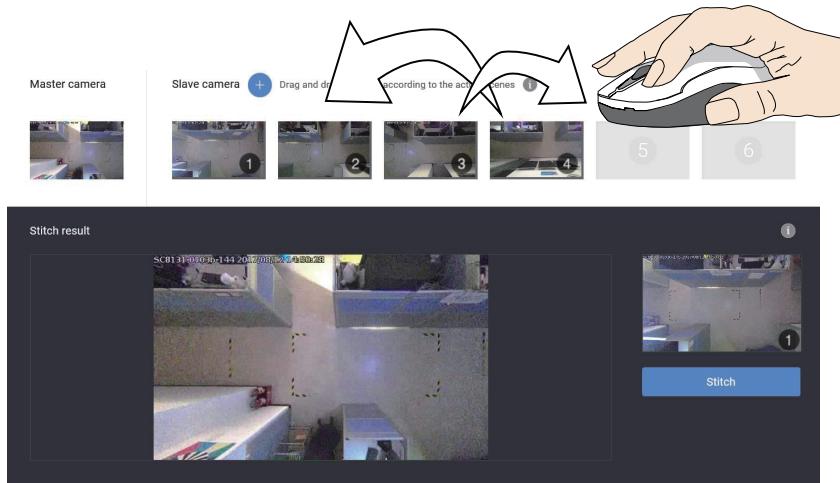
4. Before you click the Stitch button, make sure you have a co-worker to walk across the overlapped FOV between the cameras that will be stitched together.

Note that he/she should walk across the overlapped FOVs by entering, leaving, and repeating the process for about 2 minutes. By doing so, he/she should be able to provide an enough number of the motion vectors for the stitched cameras to recognize the same objects in the overlapped FOV. You can have a man walking across the overlapped FOVs of multiple cameras during the stitching process.

Click the Stitch button and tell your co-worker to start walking across the overlapped FOVs.

Overlapped Area
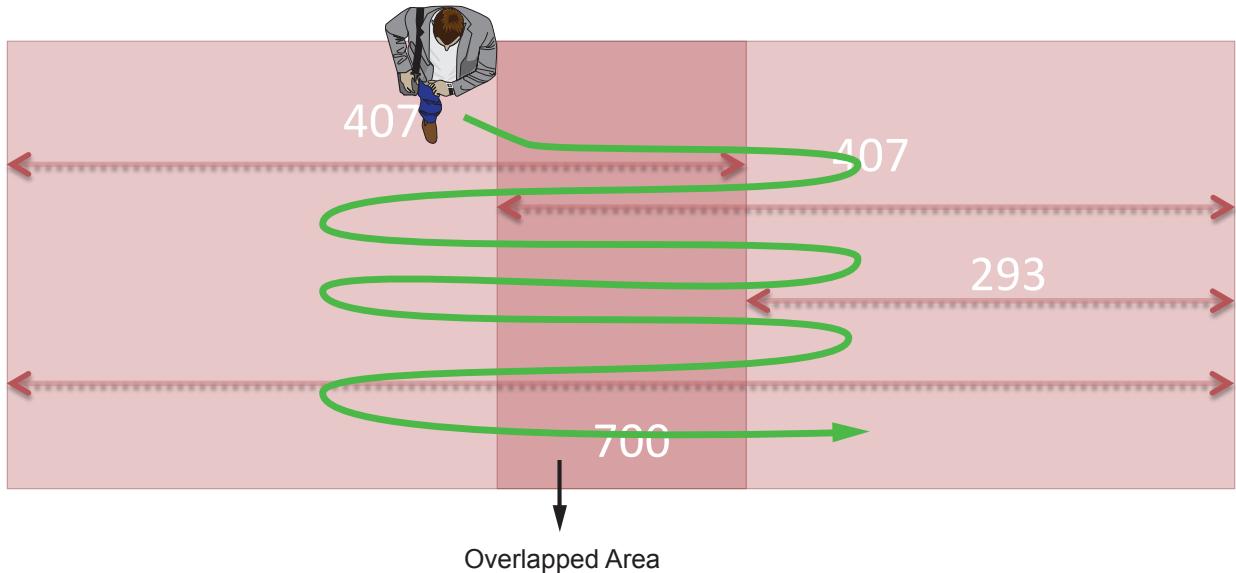
Stitching proceeds as a consecutive process. It can proceed wtih one Master and multiple slave cameras, and proceeds until all Slave camera are stitched.

There is no time limits on the Stitching process. Starting from the first Slave camera, once the Stitching is completed, a Success ✅ icon appears on its representative image, and you should inform your co-worker to move on to the overlapped FOV with the next camera.

The screen capture below shows that:

1. The Stitching between Slave #2 and Slave #3 has completed,

2. The Stitching process between Slave #3 and Slave #4 is taking place.
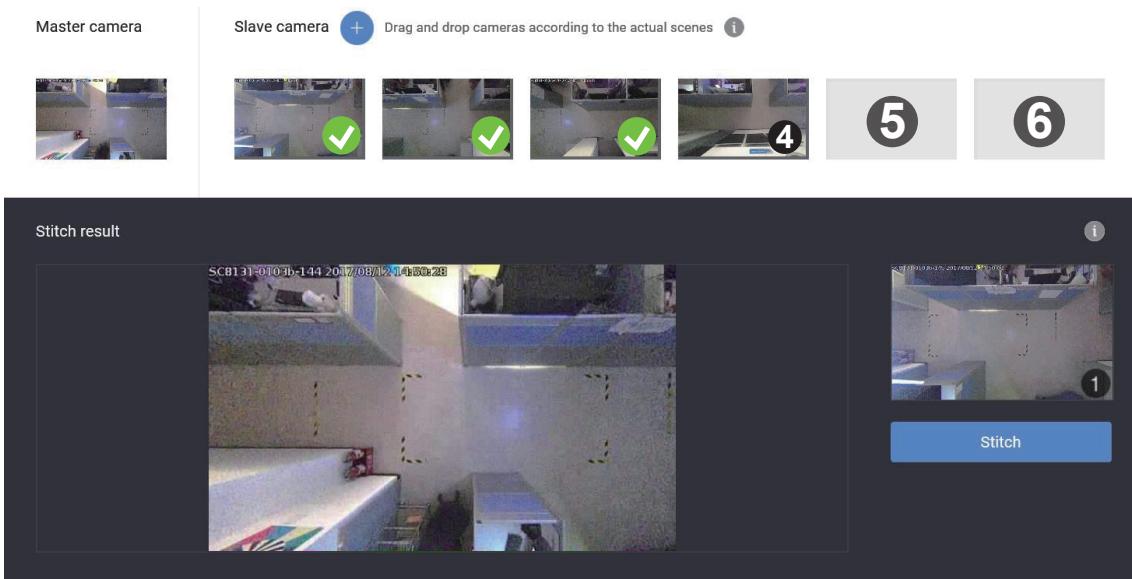
If not satisfied with the stitching results, you can select the adjacent cameras and use the Retrain button to redo the stitching process. Red squares will appear to indicate the selected cameras.

The process can be stopped and reversed at any stage if any errors should occur.

When Stitching is completed, the stitched, elongated image will be available on the live view. Proceed with configuring the analytics rules and other configurations.

3-3. Configuration - Analytics rules

Click on **Configurations** > **Analytics rules** to open the Analytics configuration window.

Click on the **Add** button to create a new rule.

3-3-1. Analytics rules - Counting (1st type)

A Configuration window will prompt. Click on the ⊕ **Add new rule** button to start the configuration. A detection line or flow path will appear on screen. Depending on the field of view at your installation site, click and drag the middle and end points on the line to change their positions. Place your detection line to a preferred position on the screen, e.g., at an entrance of a building.

Note that the **In** and **Out** directions are changed by turning the detection line 180 degrees. Make sure you leave enough room for an object to be detected before it moves aross the line. Draw the line as if it lays on the floor.

The maximum number of lines for an analytics rule is 3.
A maximum of 5 rules can be created. You should return to the previous page to create a new rule.
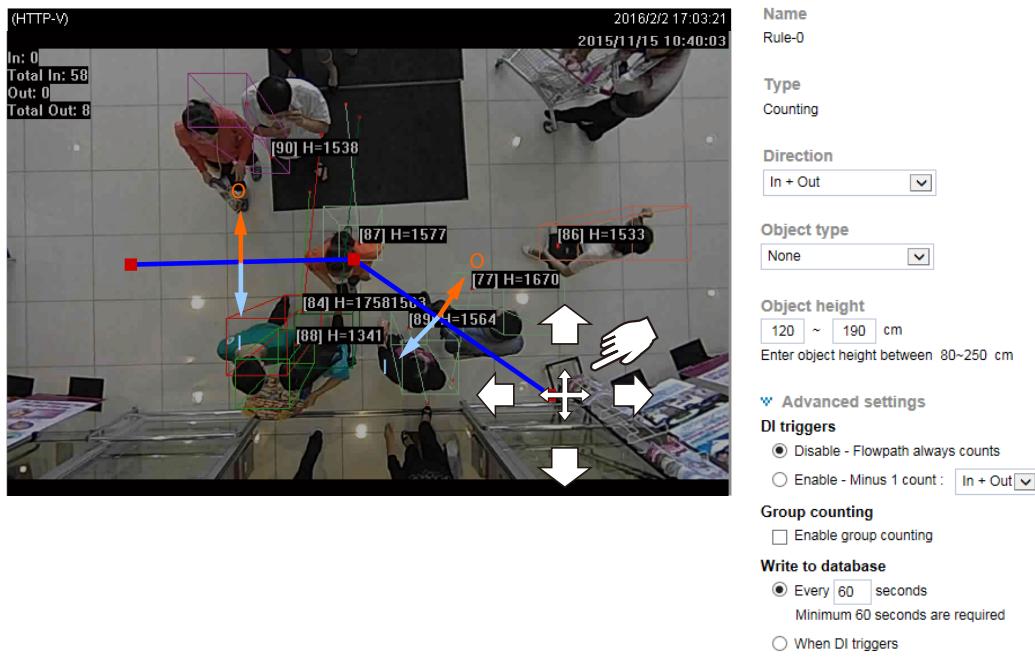
Note that there are 4 Analytics types: 1. Counting, 2. Zone detection, 3. Flowpath, 4. Queue Analysis.
The configurable parameters are different for these 4 types.

- **Direction**: Select Counting paramters as In, Out, or In & Out. If not selected, e.g., selecting the In count only, only the In counts will be recorded and reported.

- **Object type**: None or Human. Selecting Human will enhance the count accuracy for filtering situations such as when human passing by holding a cardboard box or carrying a large, tall backpack.

- **Object height**: Use this to specify the range of object height to be detected. Note that people tend to be shorter stretching their legs when walking.

- **Advanced settings**:

  - **DI triggers**: This applies when the camera DI is connected to an access control unit. The operaters of the camera may not want to count the employees of the company runnning the business facility (where the camera is installed). When an employee gains his/her access to the scene, the camera automatically decreases one count.

    Another option is "Disabled - Flowpath always counts."
  - **Group counting**: People walking or staying together for a period of time can be considered as a group. This group can be considered as a family or a group of friends, and that sometimes only one member pay the bill. The group count can be used as a statistics reference.

  - **Write to database**: Users can select to write the count records to camera either by a span of time or when a DI signal is triggered (Usually DI can be conneted to the vehicle door open signal). For example, managers can thus learn how many people get in or leave a train at which train station.

Analytics rules - Zone detection (2nd type)

Zone counting:
Records the time and quantity as people enter, leave, and waiting in the zone.

Applications:
To analyze how many people enter a certain area of a store.
To communicate how many people frequent a retail counter.

- **Detection area**: Use mouse clicks on screen to draw a polygon as your detection zone. Up to 64 clicks can be used to draw a plygon, where you expect moving objects to pass through.

- **Delay for _ seconds**:
  Enter delay: People must be present in the zone for xx seconds before the counting takes effect. When staying for a time too short, people may not have the intention for staying or entering.
  Leave delay: Taking as an effective count after people left the zone for xx seconds. If a man leaves a zone temporarily for 1 or 2 seconds, he may not intend to leave.

  Note that if you configure the Enter delay as 3 seconds, the count takes effects on the 4th second.

- **Object type**: None or Human. Selecting Human will enhance the count accuracy for filtering situations such as when human passing by holding a cardboard box or carrying a large, tall backpack.

- **Object height**: Use this to specify the range of object height to be detected. Note that people tend to be shorter stretching their legs when walking.

The Zone detection results can be configured in the **Event rules** settings to alert manager if specific events occur, e.g., more than one people are detected in front of an ATM machine.

The statistics in zone detection reports are described as follows:

Report tag name	Description
Inward count	Number of objects which went inward in aggregation time.
Sum Outward duration	Sum of dwell time for objects that left the zone before the end of aggregation time.
Total count	Total counts of dwelling objects in aggregation time.
Average duration	Average duration of dwelling objects in the aggregation time.
Average count	Average counts of dwelling objects in the aggregation time.

The system default for the aggregation time is 60 seconds, which has effects on the count of people and their dwell time in the zone, during a specific period of time. For objects that still stay in the zone by the end of aggregation time, it is difficult to learn their total dwell time. People's dwell time is calculated by adding the following sums:

    1. The dwell time since objects entered till the end of aggregation time.

    2. The dwell time of objects that left the zone during the aggregation time.

Aggregation time 1 minute
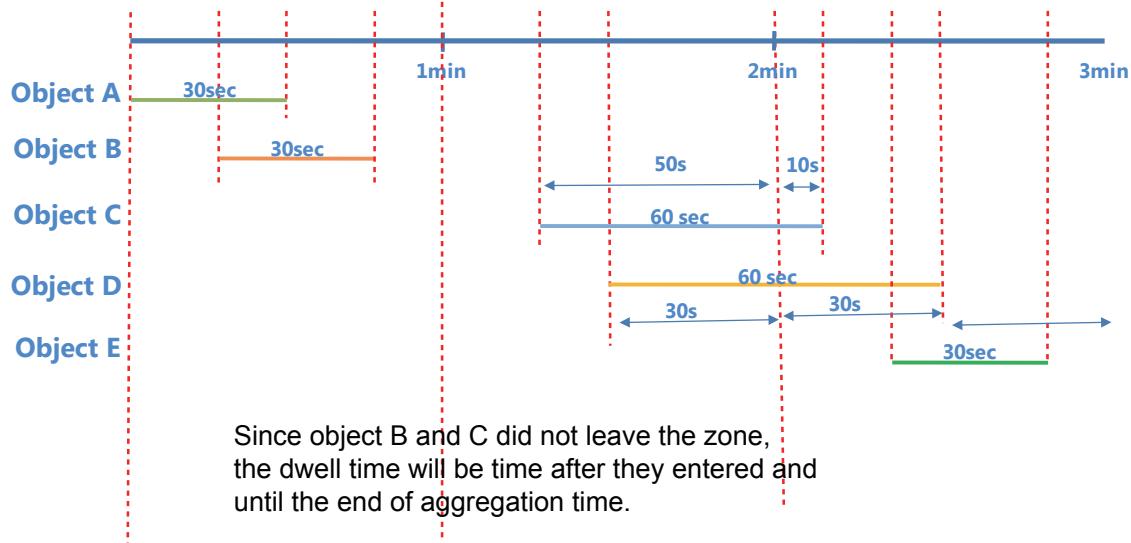
In this way, setting the aggregation time higher or lower can affect the accuracy of dwell time. Please contact our Technical Support for tuning this parameter.

Analytics rules - Flow Path Counting (3rd type)

- **Counting rules**:

The Counting rule configuration enhances count accuracy with configurable preferences if people linger or make U turns in the FOV.

One presumption is that a moving object must stay within the FOV during its movement for the Counting modes to take effect. If an object moves out of the FOV, the counting re-starts and the counting modes will not apply.
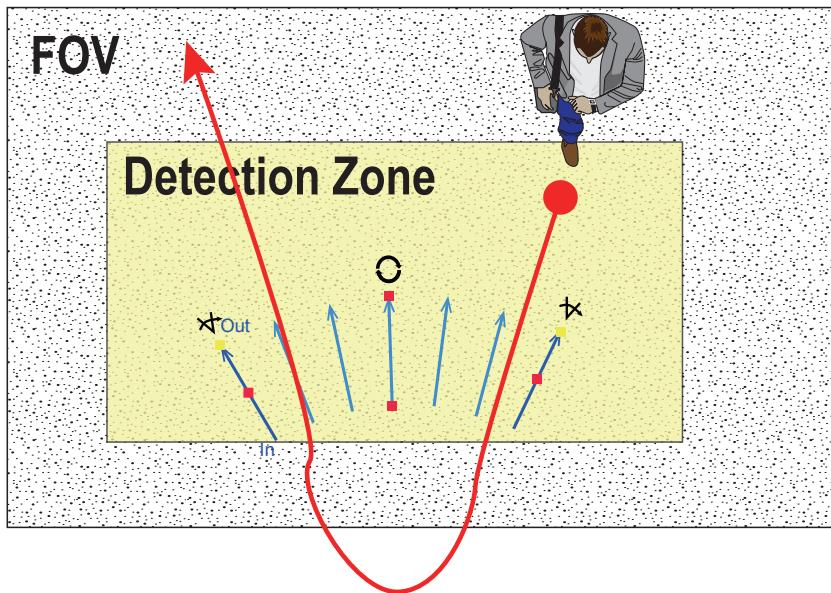
Two options are available

1. **Exclude U turn**:
This mode is the system default. The counting events will be counted only after the object exit the detected area of streaming. For example, an object crosses the counting line back and forth for several times, and during the period, the object didn't exit the FOV. The object will not be counted until it exit the detected area. The counting rule will count the object only once at the moment when the object exits the detection area.

2. **Include U turn from the outside**:
The difference of the Include U turn mode from the Exclude U turn mode lies in the side where an object enters the scene.

Several possible behaviors are illustrated as follows:

1. Objects Entering from the "In" side:

In

Out
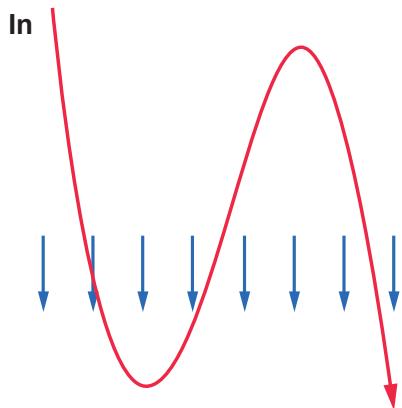
Count	Include U turn from outside (First pass)	Exclude U turn (After exit)
In	0	0
Out	1	1

In

Out
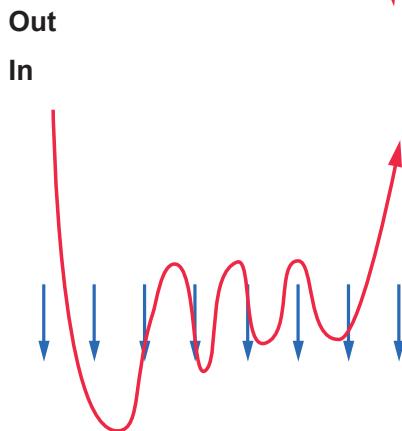
Count	Include U turn from outside (First pass)	Exclude U turn (After exit)
In	0	0
Out	0	0

2. Objects Entering from the "Out" side:

In

Out
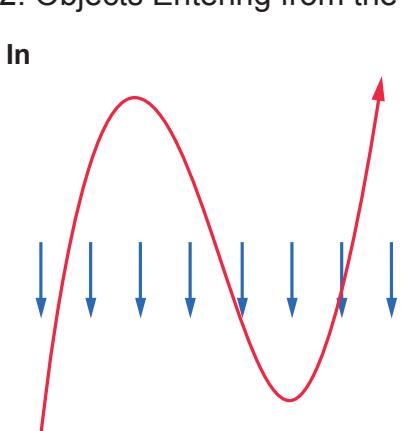
Count	Include U turn from outside (First pass)	Exclude U turn (After exit)
In	1	1
Out	0	0

In

Out
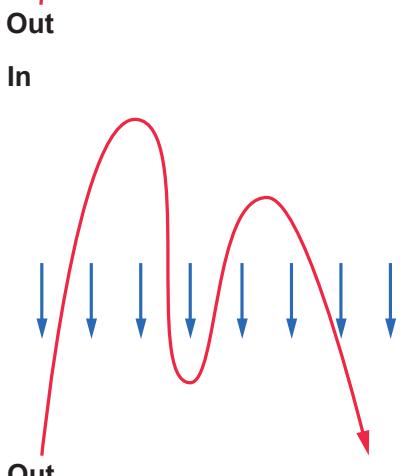
Count	Include U turn from outside (First pass)	Exclude U turn (After exit)
In	1	0
Out	1	0

The "Include U turn from the the out side" mode applies when in a crowded, confined area, such as the area near the a bus door. People may gather near the door without leaving the FOV, while it is still necessary to count the number of people moving In or Out of the vehicle.

Another applicable scenario is to detect how many people have approached a stand or a booth in a department store or museum. The management staff will then know the human traffic near specific hot spots.

• **Advanced settings**

DI triggers:

The Flow path count takes effect when a DI is triggered. This applies to the applications in public transportation. A Digital input signal is connected to a door open/close detector on a vehicle. When the door opens, the Flow path count starts; when the door closes, the count stops.
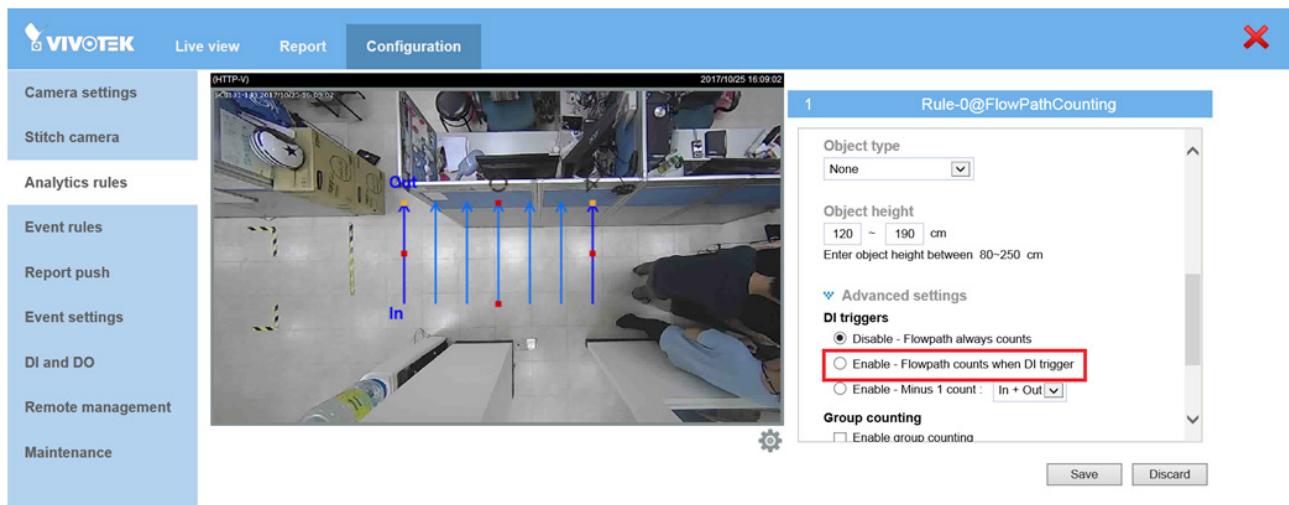
During the transition stage (from open to close), every objects whose current or original positions appear in a specific area will be counted as "In." Unless an object has passed through flowpath and already been counted as an "In" count, all objects in the area will be considered as the effective counts.
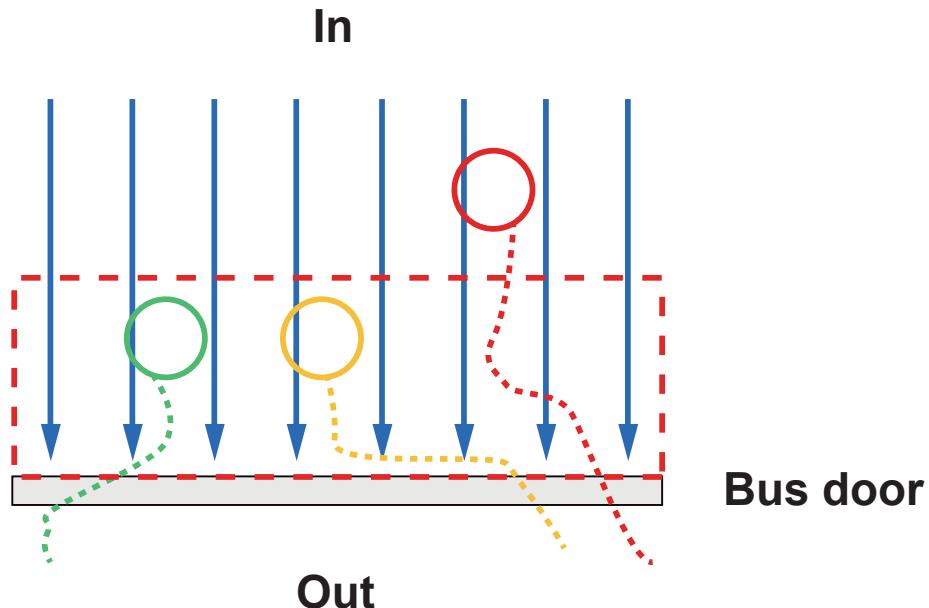
During the transition stage (from close to open), objects in a specific area will be considered as already been counted as the "In" count. When they leave the area, they will be counted as "Out." Sensitivity of the area near the vehicle door will be raised, since the traveling distance for people who have been there may be short.

In

Bus door

Out
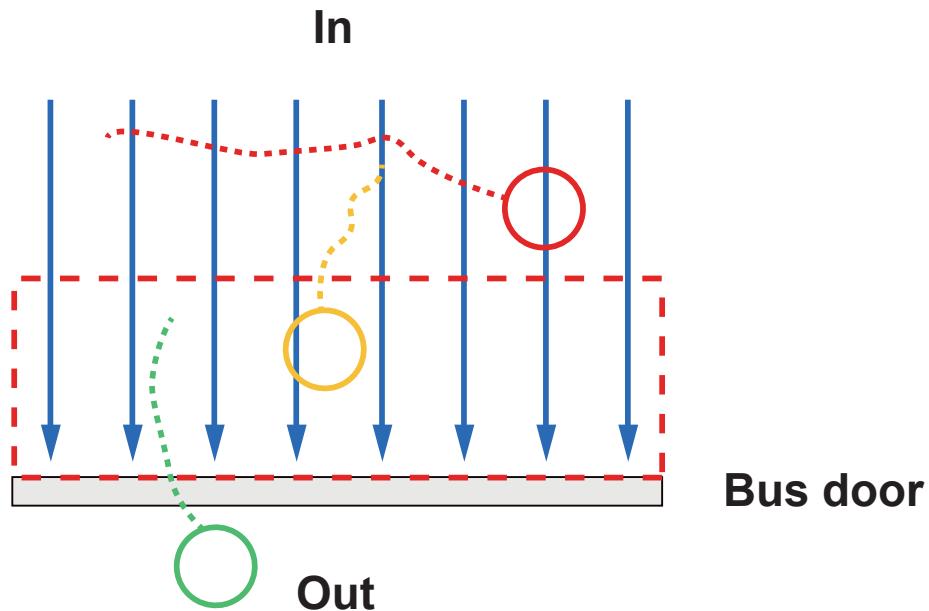
- **Minus 1 count**: This applies when the camera DI is connected to an access control unit. The operaters of the camera may not want to count the employees of the company runnning the business facility (where the camera is installed). When an employee gains his/her access to the scene, the camera automatically decreases one count.

  Another option is "Disabled - Flowpath always counts."

- **Group counting**: People walking or staying together for a period of time can be considered as a group. This group can be considered as a family or a group of friends, and that sometimes only one member pay the bill. The group count can be used as a statistics reference.

- **Write to database**: Users can select to write the count records to camera either by a span of time or when a DI signal is triggered (Usually DI can be conneted to the vehicle door open or close signal). For example, managers can thus learn how many people enter or leave a train at which train station.

3-3-2. Analytics Rules - How to Draw a Flowpath
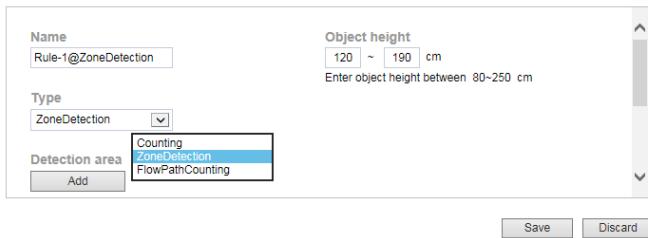
Flow path is another detection rule type. When passengers pass along the flow path, the camera will record the event and immediately update the counting report on the Liveview page.

To configure a flow path,

1 ■	Click, hold down, and drag to change the arc angle.
2 ■	Click, hold down, and drag to change the length.
3 ↻	Click, hold down, and drag to change the flow path direction. You can turn the direction 360° around.
4 ■	Click, hold down, and drag to change width.
	The Shift key can also be used with configuration. Click and drag on any part of the flow path scheme to move it across the screen.
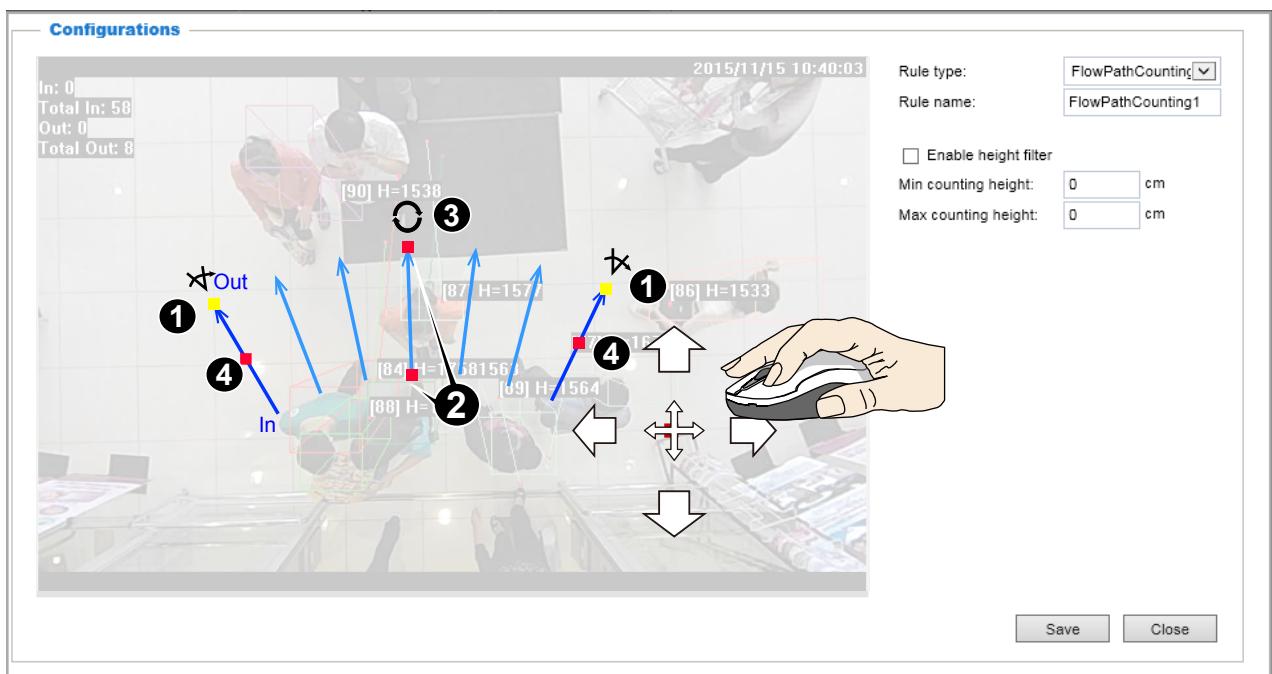
The max. and min. counting heights are also supported with the flow path. Click to select the Enable height filter checkbox. For each analytics rule, you can manually enter a set of maximum and minimum height numbers.

The counting report displays at the live view page. The counting results display instantly and the results are accumulated on the browser console.

If necessary, use the Reset report button to reset the count numbers.

Because the counting rule of Flow path is based on the entering point and the leaving point of one tracked object and the shape of the flow path scheme, it is important to configure the flow path rule carefully depending on the monitored scene. The following are the recommended usage for two common scenarios:

A section of one passageway

In this common scenario, you may want to count the number of passengers passing this section of a passageway (aisle). It is recommended to adjust the parallel flow path direction and make sure that the flow path arrows are covering the popular walking routes. If the passageway is close to the corner, for example, you could slightly expand the centre angle of the flow path to cover the route of random turns.

An exit/entrance/door/elevator
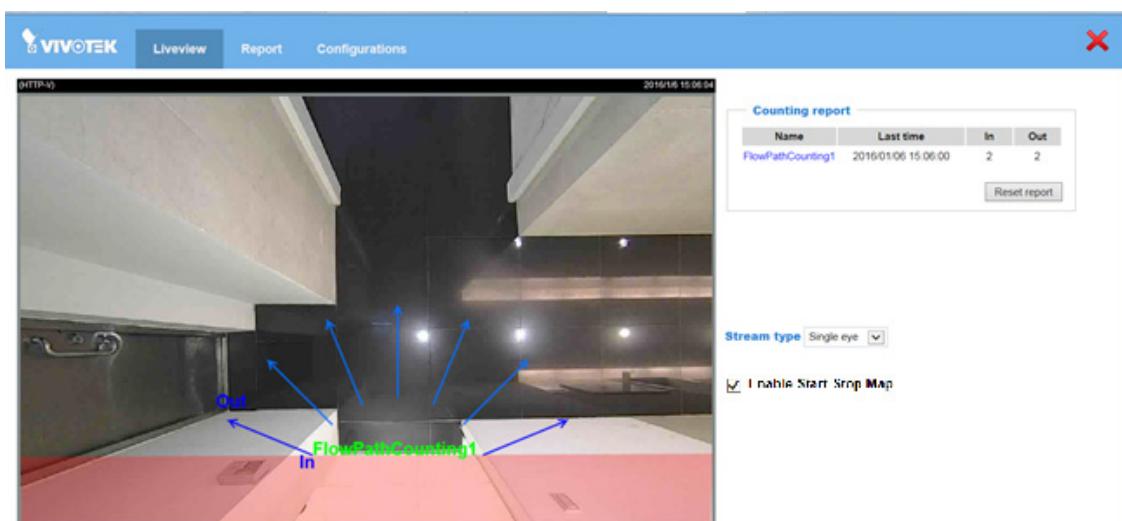
In this scenario, the arc angle of the flow path rule should be expanded to cover the possible passing patterns entering or exiting the monitored door. Besides, flow path should also be expanded to cover the width of the door. Also, the length of the flow path should be configured in a proper length. A flow path with a length too short will be very sensitive and that a length too long length will react slowly.

3-3-3. Passer-by Counting (4th type)

The configuration of Passer-by Counting is similar to the flowpath configuration as previously described. An additional Passer-by Area is configurable if this counting mode is selected.

To configure the Passer-by counting:

1. Enter a comprehensive name for the configuration, such as Queue_detect1.

2. Select the **rule type** as "Passer-by Counting."

3. Select the Sensitivity and other parameters.
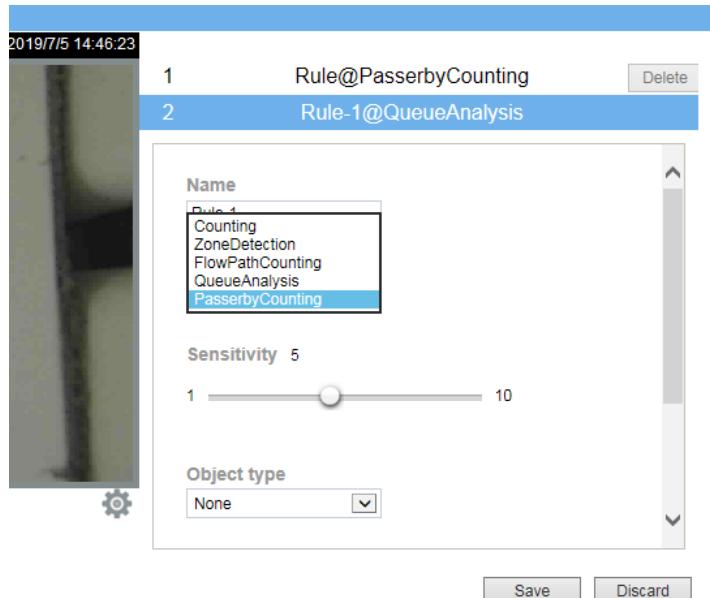
4. Configure a flowpath at an entrance. Refer to previous section for details. Click and drag the corner marks of the Passer-by Area to place it outside of an entrance.
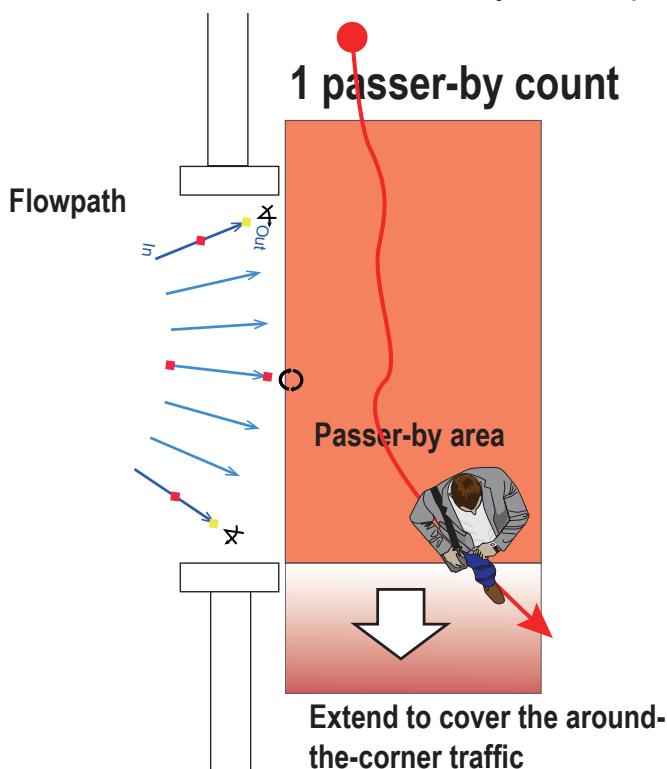
Please ensure that all foot traffic through the entrance can be covered by the flowpath and Passer-by area.

Note that a person must move across a distance of at least 50cm in the Passer-by Area to trigger a count.

3-3-4. Queue Analysis (5th type)

Queue Analysis rovides a count of people waiting in line and the duration of time of their wait.

To configure the Queue Analysis:
1. Enter a comprehensive name for the configuration, such as Queue_detect1.
2. Select the **rule type** as "Queue Analysis."
3. Select a scenario:

   3-1. Queue + Service Zone

   3-2. Queue only

   3-3. Service Zone only

   Below is a scenario using both the Service zone and Queue direction box. If you select the "Queue only" scenario, the Service zone will not be available.

Service zone

Queue direction box
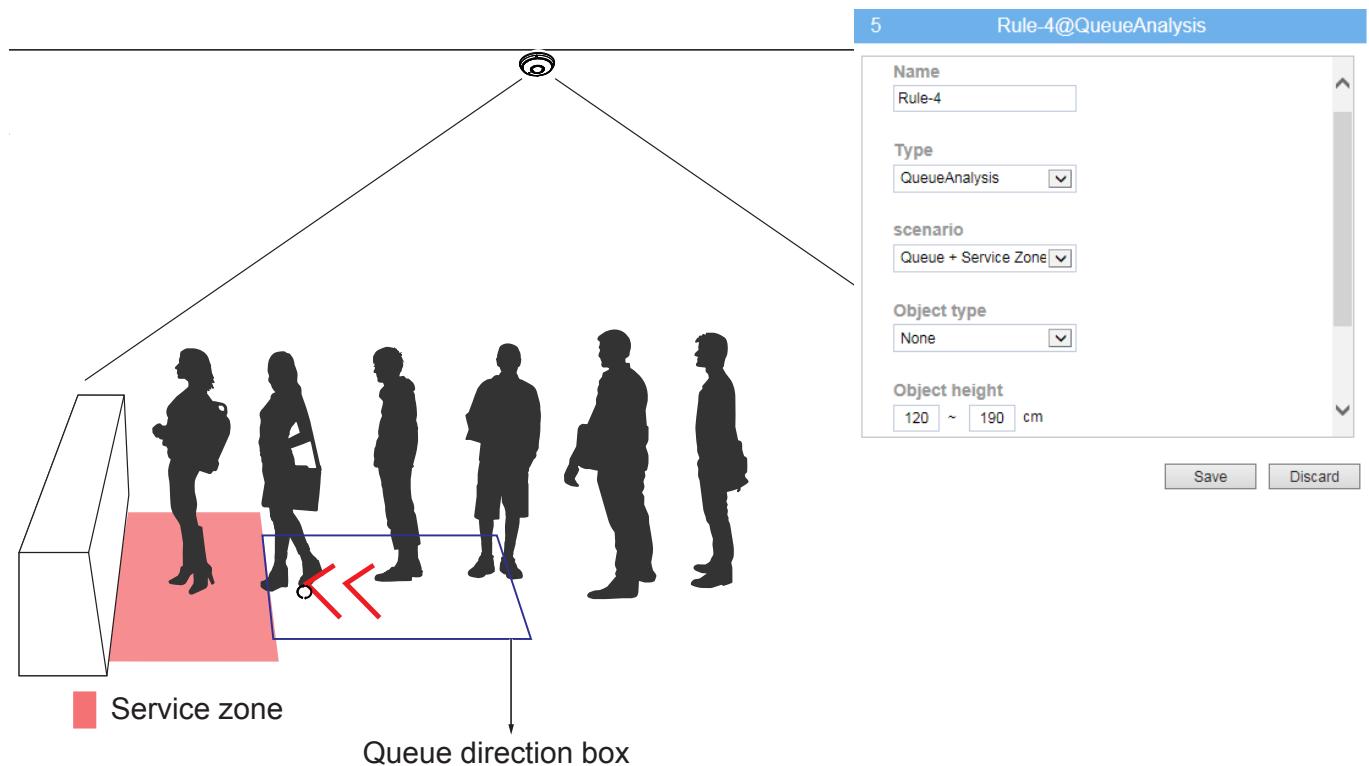
The **Service zone** is used to detect service throughput, e.g., how much time is needed to service a customer, and the utilization rate of a service counter.

The **Queue direction box** is drawn to detect how many people are waiting in line.
NOTE: Those who standing behind and outside the box will still be counted by camera firmware. The box is used to designate the possible waiting line direction.

The configuration criteria are listed below:

1. The **Service zone** should be used to cover the area right in front of the counter. The zone should cover the maneuver of one person.

2. The **Queue direction box** should have its arrow marks pointing the service provider. The Queue direction box should extend to cover the length of 1 to 3 persons standing there waiting.

When configuring the box, use the rotation button ⟳ to change its direction.

Service zone

Queue direction box
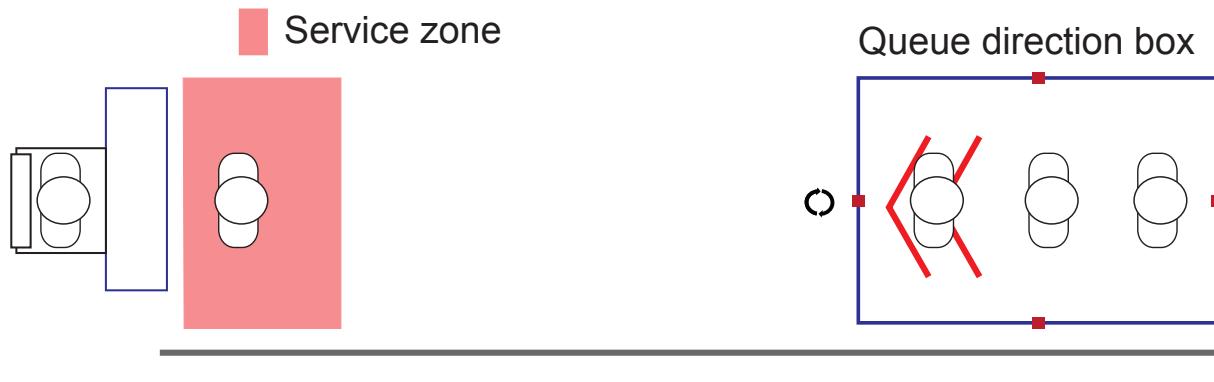
4. **Object type**: Select None or Human.

5. **Object height**: Default is 120 ~ 190cm. You can manually enter numbers ranging from 80 to 250cm.

6. **Advanced settings**:

Distance between people to be counted as one queue: Default is 50cm. You can enter a number from 0 to 500cm depending on customer behaviors.

Queue analysis delay:

Start analysis after seconds: This threshold applies when 1 person is already standing in the Service zone, and the other enters the Queue area.

Stop analysis after seconds: The threshold applies when one leaves the Queue or Service zone. The threshold avoids mis-calculation when someone abruptly leaves and re-enters the area.

Queue forming delay:

Add 1 person after enter queue for seconds: These thresholds define how an effective count starts after a time buffer.

Minus 1 person after leaving queue for seconds: These thresholds define how an effective count starts after a time buffer.

When the configuration is done, click the **Save** button, and move to the **Live view** to observe the counting results in the real scene. You can come back to Configuration > Analytics rules to make adjustments if necessary.

Shown below is a sample screen for Queue Analysis data.

QueueAnalysis

Time unit:seconds

Rule name	Length (People)	Waiting duration			Current service duration
		Maximum	Minimum	Average	
Rule-3	0	0	0	0	54
Rule-4	2	23	23	23	0

Length (People): indicates how many people are waiting in line. This number does not include one that is standing in the Service zone and currently being serviced.

Maximum: The Maximum duration of time of any person in line spent waiting.

Minimum: The Minimum duration of time of any person in line spent waiting, often of the person who newly joined the line.

Average: The Average duration of time spent waiting.

Current service duration: This number appears and disappears. It indicates the time spent in the Service zone by the person who is currently being serviced. When another person enters the Service zone, the counting restarts.

Note that if no one stands in the Service zone, the Length (People) count will not start even when there are people standing in the Queue box area. This situation may indicate that there is no service provider sitting behind the counter.

Service zone   Queue direction box
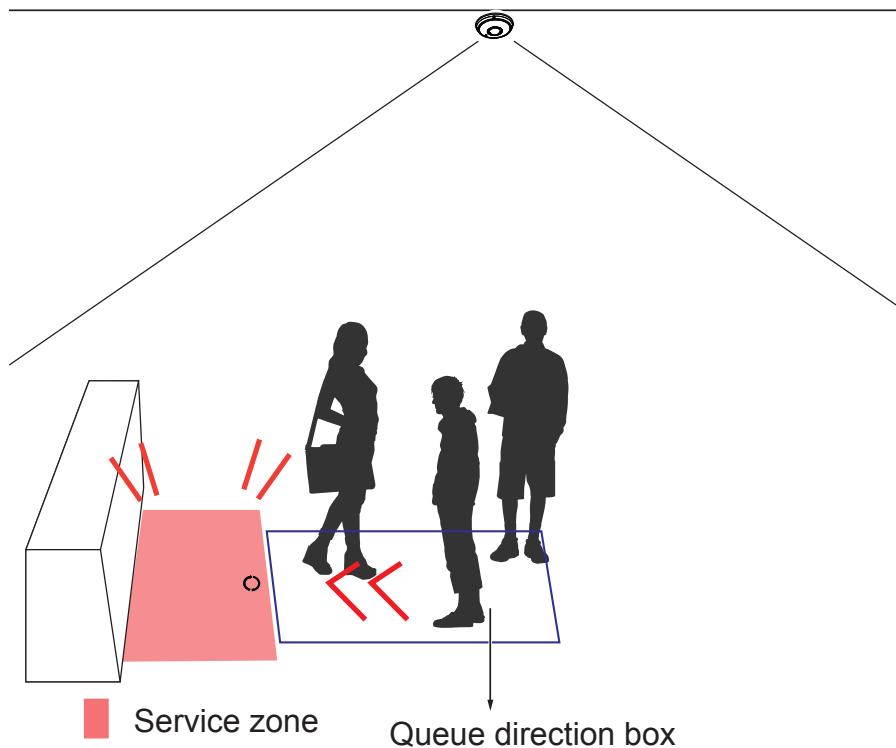
The Queue detection results, Length, Maximum Waiting Duration, Minimum Waiting Duration, Average Waiting Duration, and Current service Duration can also be used as the event triggers. For example, you can receive a notification when the Length number is too high.
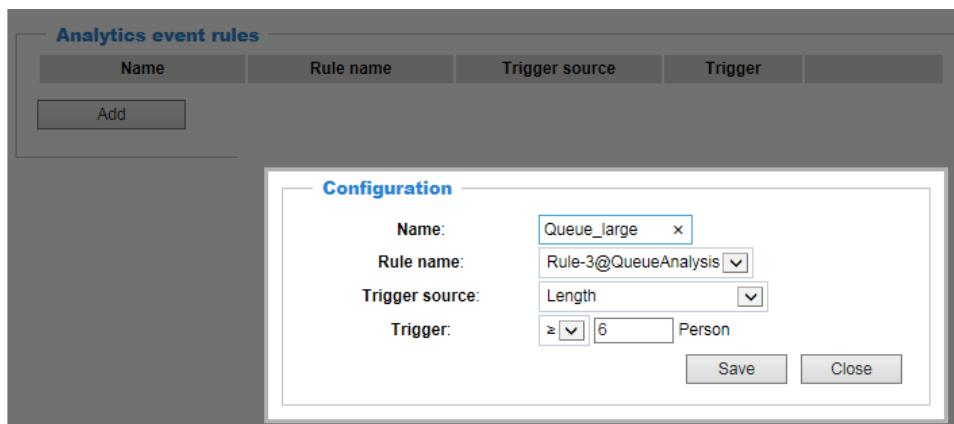
3-4. Event Rules
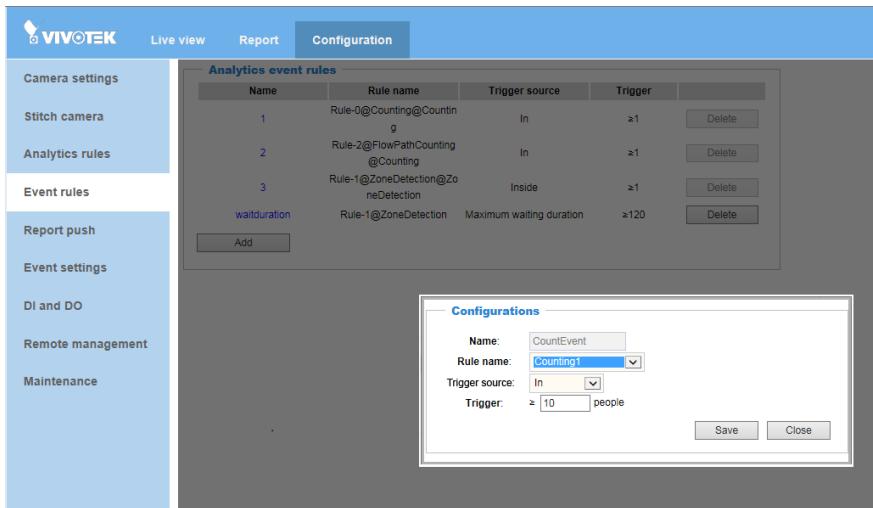
With the counting rules set up, you can configure a specific rule to be delivering a triggering condition to a receiver. For example, an event can be delivered when the number of counts exceeds a preset number. You will then know the status, say, when the number of remaining people in a building is larger than a preset number.

When configured, the **Analytics Event Rule** can be found in the Event Settings as one of the event triggers. You can then let camera send an event message along with a system log, a snapshot, or a video clip to a pre-configured receiver via an FTP, HTTP, or Email service.

You can go to the the **Configurations** > **Event Settings** > **Server** or **Media** setting page to configure an event server.
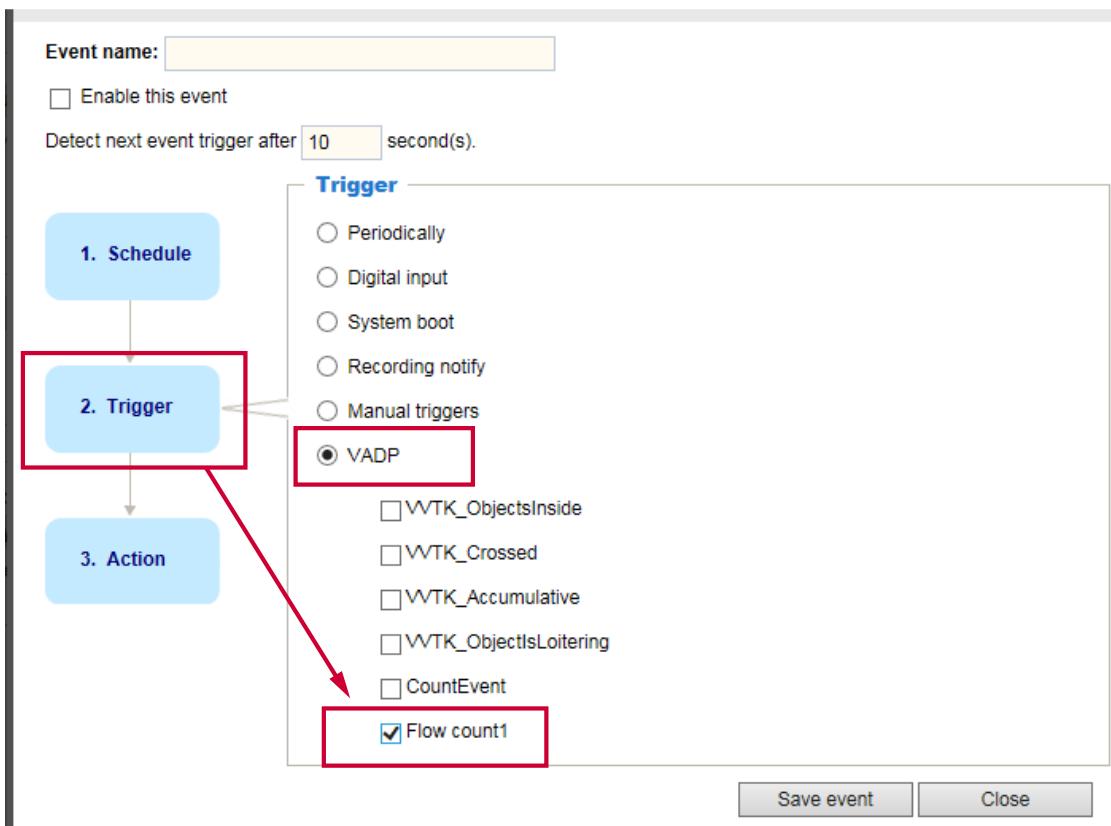
One example is to configure a zone alarm event if a specific area is populated by more than one people, such as an area in front of an ATM.
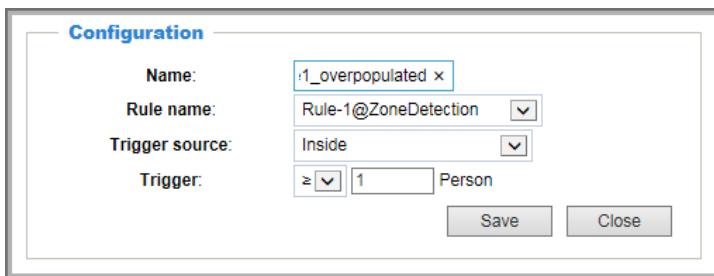
You can also select the Maximum, the Minimum, and the Average waiting duration for applications such as improving the efficiency of the checkout area. Configure Maximum waiting duraction to alert the manager if customers wait for too long in the checkout area.

3-5. Tampering detection
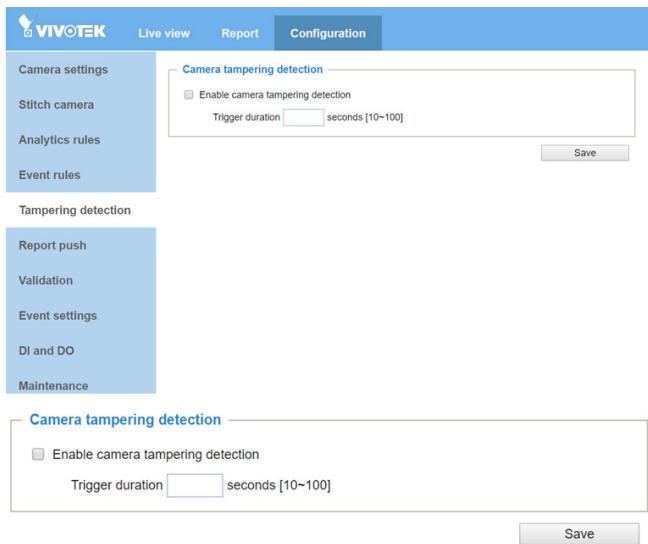
The Tampering detection enables the alarm when someone tries to block the camera lens. The Tampering detection currently does not support scene change, defocus, or loss of illumination in scene.

3-6. Report Push

Configure the report push protocols so that you can receive periodic counting reports. The reports include camera information and aggregated counts by the configured intervals for each counting rule. Click the **Add** button to begin.

Status		: success	: failed	[empty]: not yet executed
Name	User defined name.			
Address	HTTP: http://IPaddress:portURI FTP: ftp://APaddress:port -> destination Email: ServerIPaddress:port			
Delivery Schedule	The duration between next pushed aggregated report. At the same time, it is also the total duration of one report. This camera supports the delivery schedule ranging from 1 min, 5 mins, 15 mins, 30 mins, 1 hr, 12 hrs, to 1 day. All schedule starts from 00:00.			
Aggregation level	This indicates the aggregation period for each data set in the reports. Events in the same aggregation level will be accummulated as one data set. This camera supports the same options as the Delivery schedule. Note that the aggregation level must be shorter than the Delivery schedule.			
Report Type	Log, Queue raw data, Queue aggregate data, Counting/Zone			
Lite	In the Lite mode, the period of time in which no data has been collected will be ignored. This can reduce the size of each report.			
Format	XML, CSV, and JSON. The detailed contents will be introduced later.			

Localtime	Presents the input starttime, endtime, and the StartTime, EndTime in a report as camera local time. If not selected the input starttime, endtime and all time format in report is in UTC (Universal Time Coordinated) timestamp.
Include camera status flag in the report	When selected, the report will include a "status" column. 0 (0000): Normal 1 (0001): Re-send 2 (0010): Tampering 3 (0011): Tampering + Re-send 4 (0100): Power off 5 (0101): Power off + Re-send 6 (0110): Power off + Tampering 7 (0111): Power off + Re-send + Tampering \<Status\>0\</Status\> \</CountingInfo\> \<CountingInfo RuleName="Rule-2"\> \<In\>0\</In\> \<Out\>0\</Out\> \<StartTime\>2019-03-30T08:59:00+0800\</StartTime\> \<EndTime\>2019-03-30T09:00:00+0800\</EndTime\>

Server type:

Fill in the event report agent information:

Email	
Sender email	A valid sender email
Recipient email	A valid receiipient email
Server address	SMTP server IP address
User name	User name for SMTP server authentication credentials
Password	Password for SMTP server authentication credentials
Port	SMTP server port number
This server requires a secure connection (SSL): select if SSL connection is required.	
FTP	
Server address	FTP server IP address
Port	FTP server port number
User name	User name for FTP server authentication credentials
Password	Password for FTP server authentication credentials
FTP folder name	The destination folder path
filename format*	User customizable file name through variables.
HTTP	
Server address	HTTP server IP address
Port	HTTP server port number
Server uri	HTTP server route uri
User name	User name for HTTP server authentication credentials
Password	Password for HTTP server authentication credentials

SD	
Enable cyclic storage	HTTP server IP address
File name format	See below for the customizable file name syntax.

* Listed below are the variables for the customized file name.

%T	Report timestamp in UTC time
%F	Report formal in xml, json, or csv
%N	User defined server name
%y	Year in 4 digits
%m	Month of the year in 2 digits
%d	Day of the month in 2 digits
%h	Hour in the day in 2 digits
%n	Minutes in the hour in 2 digits
%M	MAC address in serial
%G	Group ID
%D	Device ID
%S	Schedule duration in second
%A	Aggregation level in second
%L	"LITE" if in the lite mode, "" otherwise.
%N	Server name

* The above names and addresses support the following numeric-alphabetic characters:
A-Z,a-z,0-9 and !#$%-.@^_~\/;:?{[]}`*)(+|

Use the **Test** button to push a test packet. When the test is successfully performed, click the **Save** button.
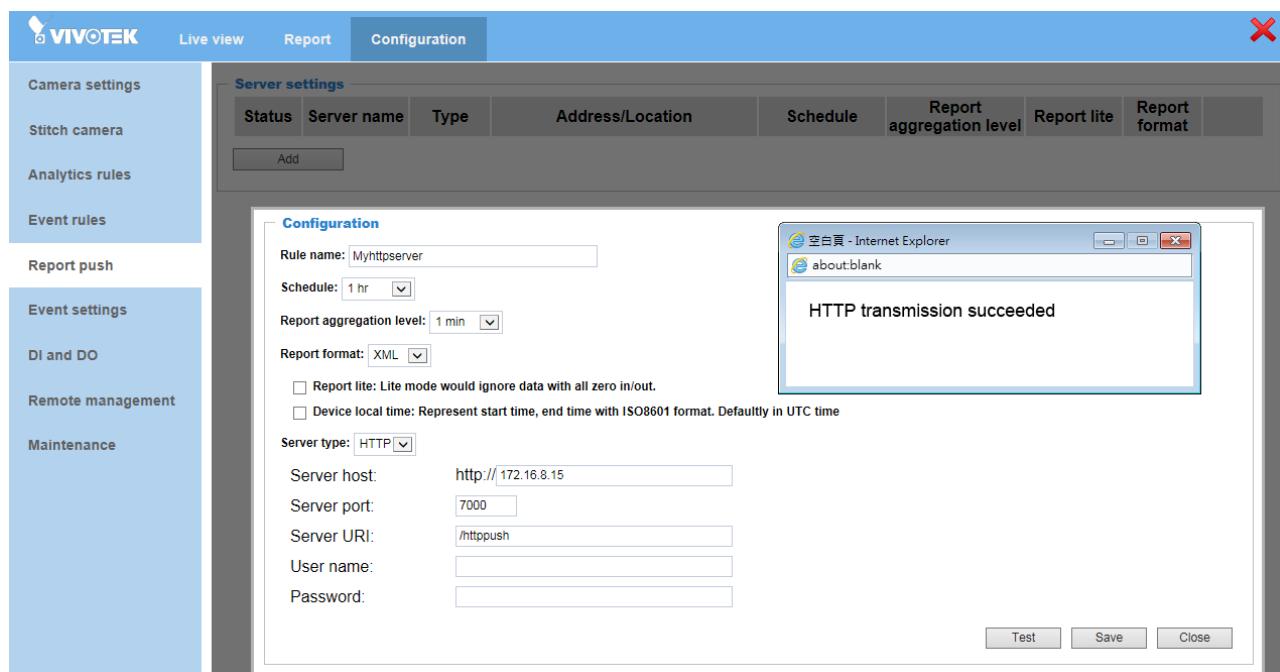
The camera will post an XML file to server, the description of XML (XSD) is as below:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeForm
Default="unqualified">
<xs:element name="Message">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Source">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="UtcTime" type="xs:string"></xs:element>
                            <xs:element name="GroupID" type="xs:string"></xs:element>
                            <xs:element name="DeviceID" type="xs:string"></xs:element>
                            <xs:element name="ModelName" type="xs:string"></xs:element>
                            <xs:element name="MacAddress" type="xs:string"></xs:element>
                            <xs:element name="IPAddress" type="xs:string"></xs:element>
                            <xs:element name="TimeZone" type="xs:string"></xs:element>
                            <xs:element name="DST" type="xs:string"></xs:element>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="Data" maxOccurs="unbounded">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="CountingInfo" maxOccurs="unbounded">
                              <xs:complexType>
                                <xs:sequence>
                                  <xs:element name="In" type="xs:string"></xs:element>
                                  <xs:element name="Out" type="xs:string"></xs:element>
                                  <xs:element name="StartTime" type="xs:string"></xs:element>
                                  <xs:element name="EndTime" type="xs:string"></xs:element>
                                </xs:sequence>
                                < xs:attribute name="RuleName" type="xs:string"/>
                              </xs:complexType>
                            </xs:element>
                        </xs:sequence>
<xs:attribute name="RuleType" type="xs:string"/>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
  </xs:schema>
```

The following CSV example shows the same event description in csv format, note that, camera will send zero counting even if there is no count for that interval if you deselect the lite mode.

UtcTime,GroupID,DeviceID,ModelName,MacAddress,IPAddress,TimeZone,DST
2015-05-28T06:30:01Z,0,0,SC8131,00:02:81:31:00:08,172.16.2.134,+8,0
RuleType,RuleName,In,Out,StartTime,EndTime
Counting,Counting1,1,2,2015-05-28T06:15:00Z,2015-05-28T06:30:00Z
Counting,Counting2,0,0,2015-05-28T06:15:00Z,2015-05-28T06:30:00Z

Below is the JSON example showing the same condition in json format. a zero counting data will still be sent if you deselect the lite mode.

```
{
        "Source":
              {
                      "UtcTime":"2015-05-28T06:30:01Z",
                      "GroupID":"0",
                      "DeviceID":"0",
                      "ModelName":" SC8131",
                      "MacAddress":"00:02:81:31:00:08",
                      "IPAddress":"172.16.2.134",
                      "TimeZone":"+8",
                      "DST":"0"
              },
        "Data":
              [
                      {
                              "RuleType":"Counting",
             "CountingInfo":
                [
                  {
                     "RuleName":"Conting1",
                     "In":1,
                     "Out":2,
                     "StartTime":"2015-05-28T06:15:00Z",
                     "EndTime":"2015-05-28T06:30:00Z"
                   },


   {
                      "RuleName":"Conting2",
                      "In":0,
                      "Out":2,
                      "StartTime":"2015-05-28T06:15:00Z",
                      "EndTime":"2015-05-28T06:30:00Z"
                  }
                ]
              }
          ]
      }
```

In addition to these, if you want to acquire the report directly from CGI, use the following command to receive the report in different formats:

http://{IP}/cgi-bin/admin/scevent_pull.cgi?
format={xml,json,csv}&
starttime={starttime timestamp} &
endtime={endtime timestamp} &
aggregation={aggregation level in seconds} &
lite={0,1}&
localtime={0,1}

A sample line looks like this:

http://172.19.11.142/Stereo-Counting/cgi-bin/report_pull.cgi?starttime=2017-11-14T00:00:00&endtime=2017-11-20T00:00:00&aggregation=3600&format=xml&lite=0&localtime=0&countingeventdb=0

The syntax is as follows:

Key	Description
starttime	Querying start time timestamp
endtime	Querying end time timestamp
aggregation	Report aggregation level for each record in seconds
format	[Option] Report format including XML(default), JSON, CSV
lite	[Option] Flag turns on to ignore in/out if zero records. [default turn off : 0]
localtime	[Option] Flag turns on to take input starttime, endtime as camera local time. [default turn off : 0 -> input starttime, endtime is in UTC timestamp]

3-7. Validation

This page allows users to upload video recording files to an FTP server for use with a Validation Tool utility. The file format is MAC_FWversion_yyyy-MM-dd_HHmmss.mp4, e.g., 0002D13D516F_SC8131-VVTK-0104a_2018-05-02_153542.mp4. The limitation of recording length is 1 min. and the size is 1.5MB. The counting-related metadata is also recorded with files.

The VIVOTEK Validation tool allows users to verify and examine the accuracy and effectiveness of stereo counting from the SC8131 and SC8132 series. The prerequiste is that users must acquire validation recordings from the installation site. A validation report can then be generated for customers.

Please contact VIVOTEK's technical support for the Validation tool, and proceed with configuring a video recording at the installation site. The validation video must contain the stereo counting metadata.
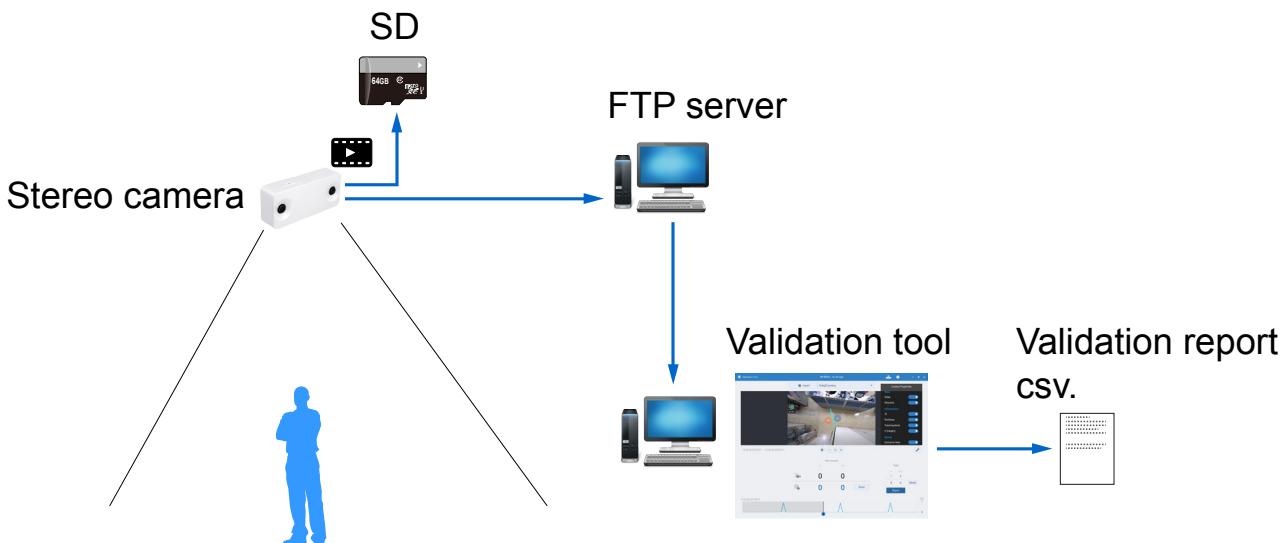
The Validation tool comes as a self-executive msi file: vivotek-validator-1.0.0.13.msi. Install the program. The Validation tool runs on a Windows 64-bit 7 or 10 operating system.
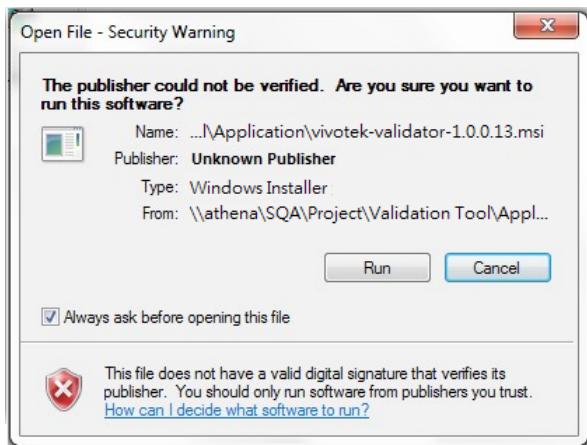
Follow the onscreen instruction to complete the installation procedure.
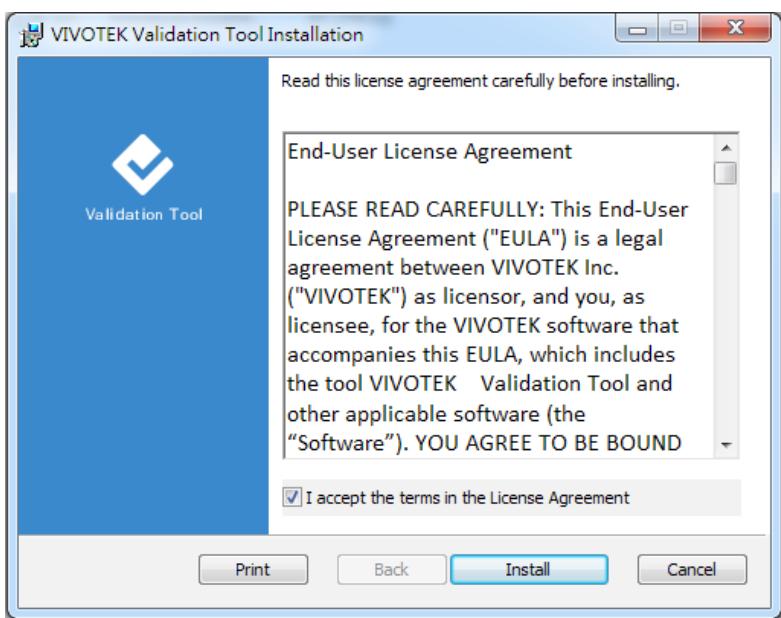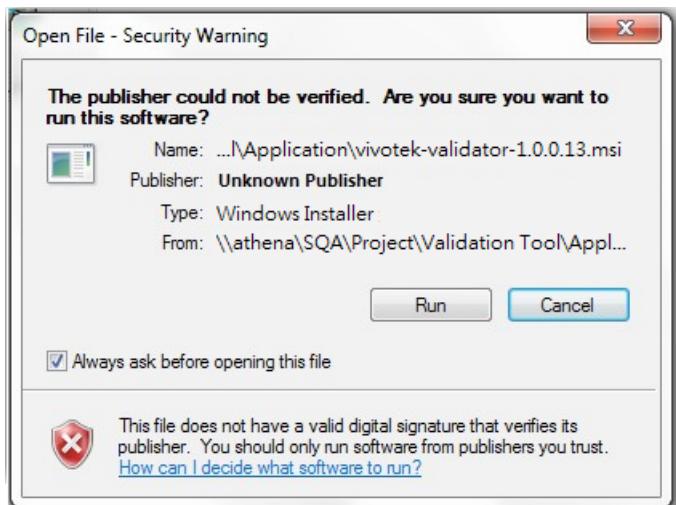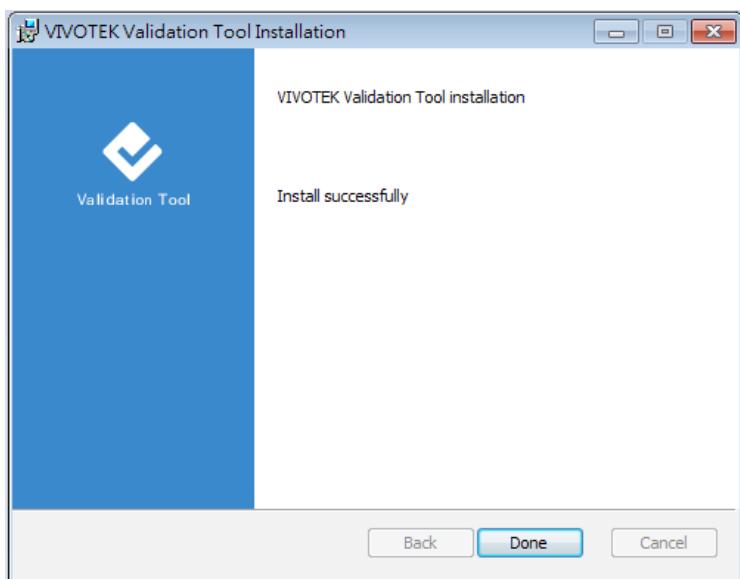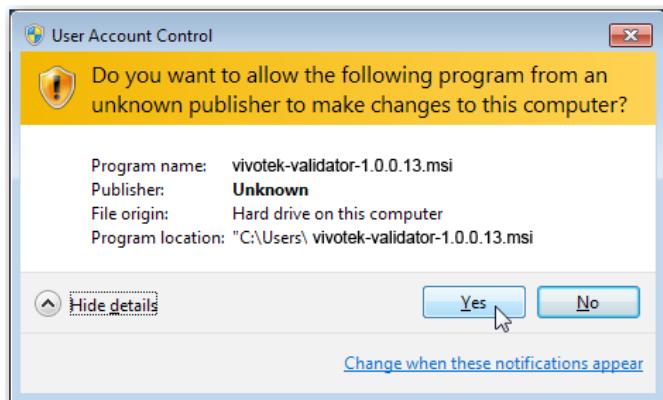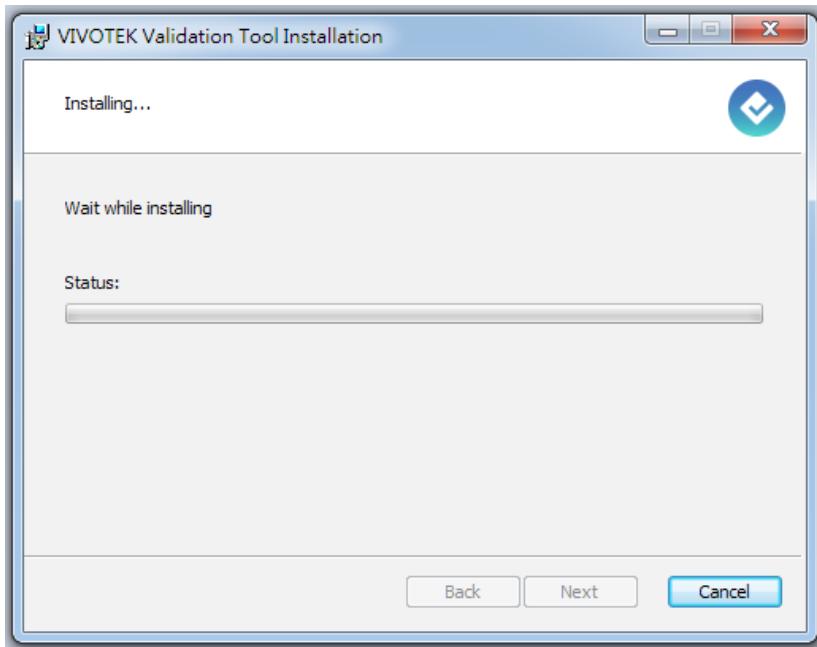
Start the program. You should have prepared some recorded validation recordings according to the documentation provided with the camera. Note that the validation recording is different from ordinary video recordings.

Click the **Import** button to locate the recordings.
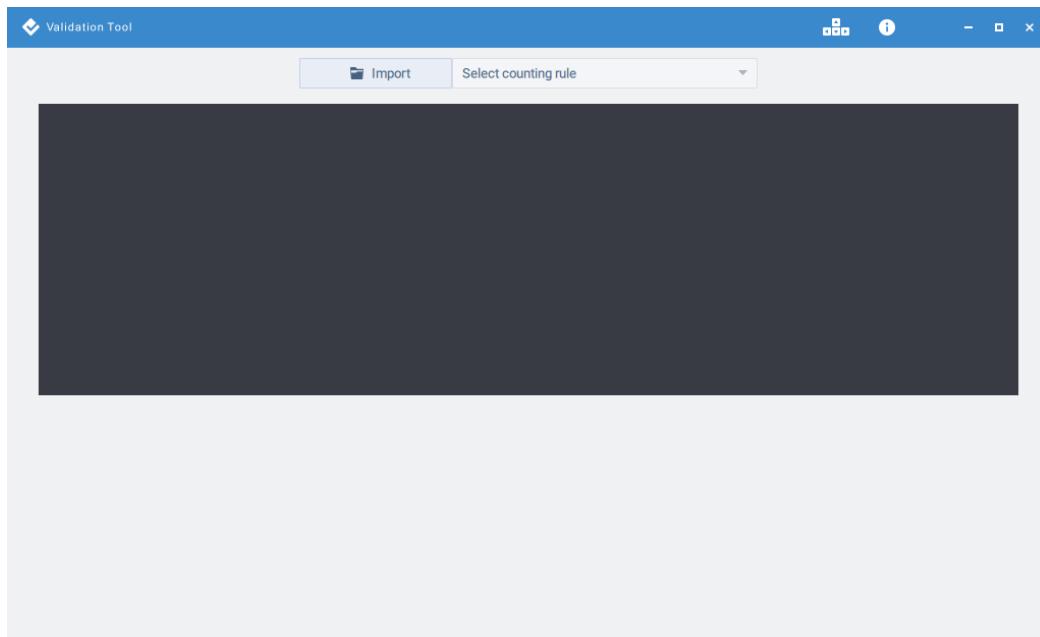
Functional Items:

Before using this utility, acquaint yourself with the following:

Item	Description
▶	Plays a selected validation recording.
❚❚	Pauses the playback of a recording.
− 1x +	Increases or decreases the playback speed.
🔧	Clicks to change the display elements on screen. Click again to close the menu.
Custom Properties / Rule / Rules / Direction / Information / ID / Positions / Tracking block / H (Height) / Scene / Exclusive Area	Rule: Counting line or flow path. Direction: the In / Out direction. ID: the identifier number. Positions: the start and end points of detected objects. Tracking block: the bounding box shown around the detected objects. Height: the height of the detected objects. Exclusive area: the exclusive, non-effective area.
⊡	Displays the available hot keys.
ⓘ	Displays software revision information.
📹	This row displays the machine counts.
👆	This row displays the counts you manually make.
Manual validate	Click to start your manual count.
Reset	Resets your manual counts to 0.
Export	Exports your validation results to a csv report file. The comparison between machine counts and manual counts will be listed.
	The activity chart roughly matches the occurrences of events (objects' appearance) in the recordings being played. The timeline indicates the objects' positions during the recording. The (In) count on the upper right indicates the number of people still staying in the In area.
Import / Rule_FLOW@FlowPathCounting / Rule_LINE@Counting	Selects a count rule (line or flowpath), if there are more than one rule.

The display elements are illustrated below:
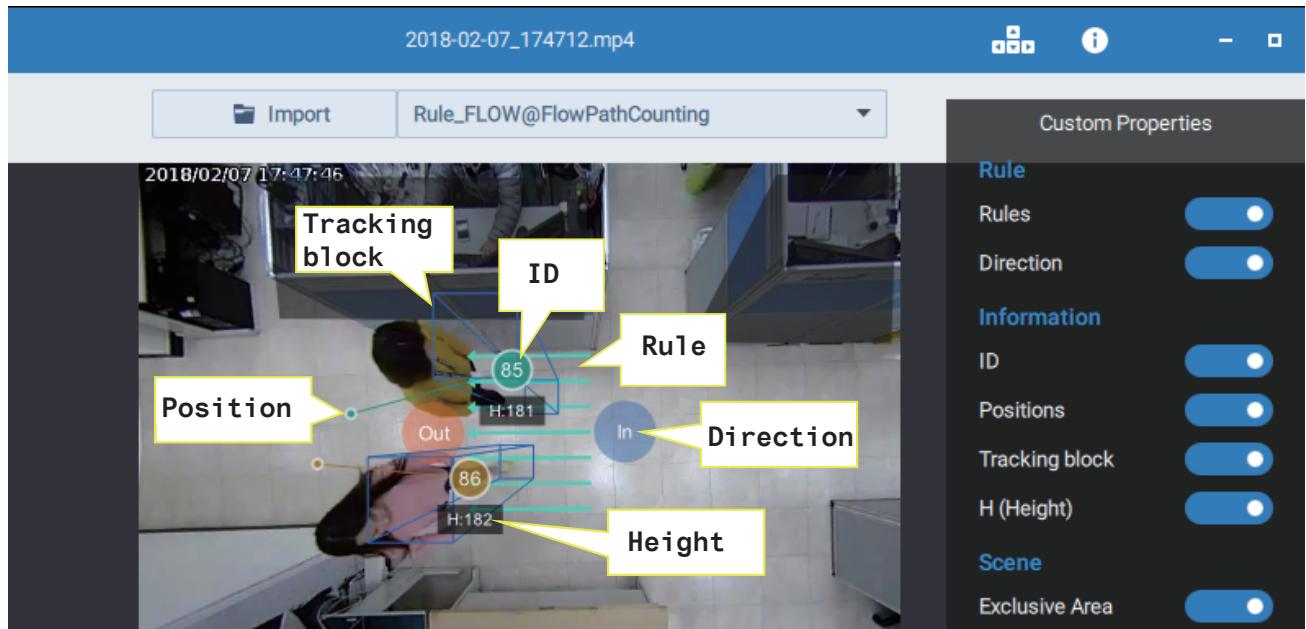
Functional Items:

Use the following keyboard keys to register and verify the counts:

Hotkey	Description
↑	Press to register an "In" count.
↓	Press to register an "Out" count.
Space	Play or Pause a video.
+ -	Speed up or speed down.
←	Moves back to the previous second.
→	Moves forward to the next second.
Shift & ←	Moves back to 3 seconds ago.
Shift & →	Moves forward to 3 seconds later.

To start validate your stereo count recordings,

1. Import a validation recording.

2. Select a counting rule.

3. Click Manual validate.

4. Use the hot keys listed above to validate the count results.

5. When done with validating the recording, click Export to generate a report file.
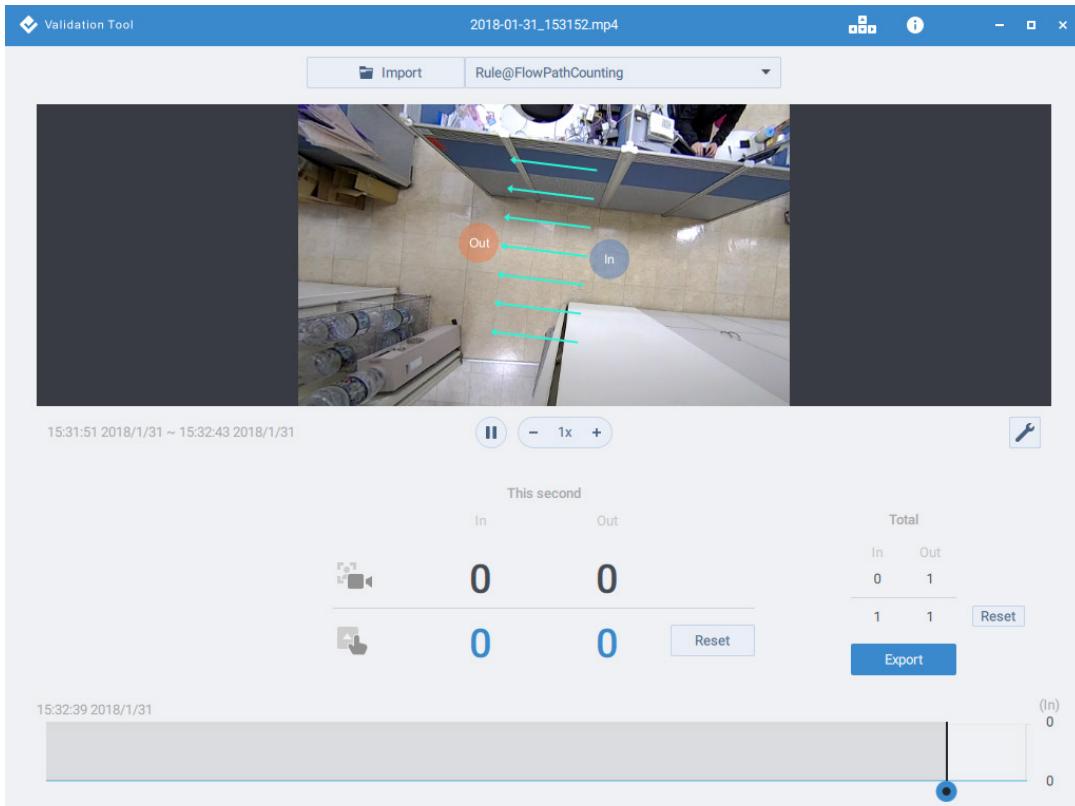
Note that you can click on the the timeline (or activity bar) to move to a specific point in time.

The csv report should look like this.

3-8. Event Settings

System Boot	Digital input	Periodic	Recording notify

Counting1(IN) ≥10	FlowPath1(IN-OUT) ≥20	FlowPath2(OUT) ≥5

Event 1
Schedule

Event 2
Schedule

Event 3
Schedule

Event Manager

Actions:
1. Digital output (DO)
2. System log
3. Snapshot (pre-/post-)
4. Recording (pre-/post-)

Targets:
1. SD card
2. Email notification
3. FTP
4. Networked storage

The camera can respond to particular situations (event). A typical application is that when a count result is reached, the camera sends buffered images to an FTP server or e-mail address as notifications. An event can be initiated by many triggering conditions, such as counting results or digital inputs. When an event is triggered, you can specify what type of action will be performed.

Event

An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window.

■ Event name: Enter a name for the event setting.

■ Enable this event: Select this option to enable the event setting.

■ Detect next event trigger after ☐ seconds: Enter the duration in seconds to pause event trigger after the current event is triggered.

Follow the steps 1~3 to arrange the three elements -- Schedule, Trigger, and Action to configure an action to take when an event is triggered. You can configure 3 event-triggered conditions.

1. Schedule
Specify the time span for the event-triggering condition. Please select the days of the week and the time in a day (in 24-hr time format) for the recording schedule.

2. Trigger
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown below. Select the item to display the detailed configuration options.

■ Periodically
  This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.
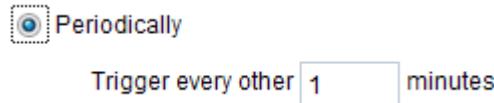
■ Digital input
  This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

■ System boot
  This option triggers the Network Camera when the power to the Network Camera is disconnected and reconnected.

■ Recording notify
  This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Manual triggers
  An event can be manually triggered by the manual trigger buttons on the main page.

■ VADP (VIVOTEK Application Development Platform)

The triggering conditions available with the counting algorithms (known as VADP) will be listed. Use the check circles to select these triggers.

The Analytics Event rules you previously configured as event triggers will also be listed here as the triggering conditions.

3. Action
Define the actions to be performed by the Network Camera when a trigger is activated.
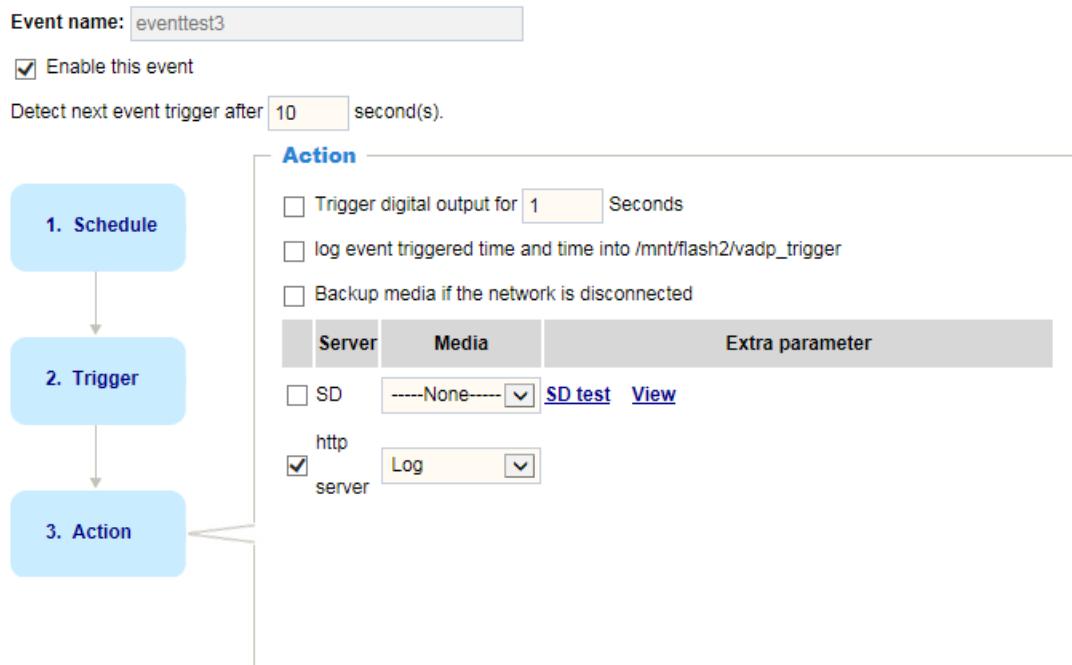
■ Trigger digital output for ☐ seconds
Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Log event triggered time and time into /mnt/flash2/vadp_trigger
Create a log of the occurrence of event to the onboard non-volatile memory.

■ Backup media if the network is disconnected
Select this option to backup media file on SD card if the network is disconnected. Please note that this function will only be displayed after you set up a networked storage (NAS). For more information about how to set up networked storage, please refer to page 199.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

See the previous section, **2-3. Report Push**, for information about Server and Media configuration.

Add server

Click **Add server** to unfold the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.

The email has been sent successfully.

Error in sending email.
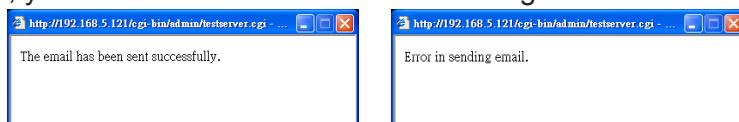
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you set up the first event server, a new item for event server will automatically show up on the Server list. If you wish to add more server options, click **Add server**.

Server type - FTP
Select to send the media files to an FTP server when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
  Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode

Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.

http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...	http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...
ftp transmission successfully.	ftp transmission failed.

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.

http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...	http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...
HTTP Transmission successfully. Thanks	HTTP Transmission failed.

Click **Save server** to enable the settings and click **Close** to exit the Add server page.

Network storage:
Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 199 for details.

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Server name:	
Server type	
○ Email	
○ FTP	
○ HTTP	
⦿ Network storage	
Network storage location:	
(For example: \\my_nas\disk\folder)	
Workgroup:	
User name:	
Password:	

[Test]   [Save server]   [Close]

■ SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 202 for detailed information.

Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent and preserved when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.
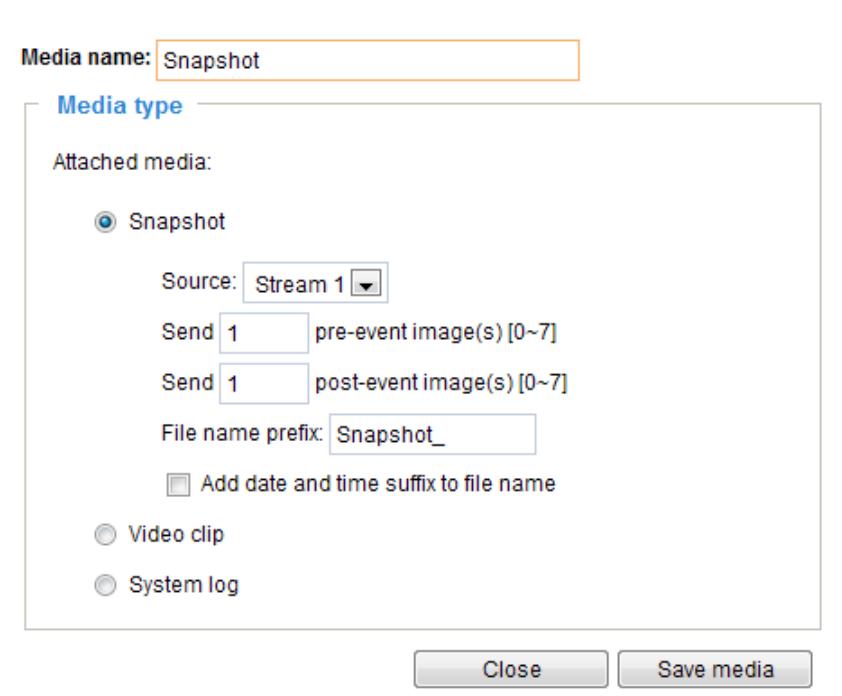
Media type - Snapshot
Select to send snapshots when a trigger is activated.

■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from stream 1 ~ 4. (The following options are available when the check circle is selected.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.

1 pic. 2 pic. 3 pic. 4 pic. 5 pic. 6 pic. 7 pic. **8 pic.** 9 pic. 10 pic. 11 pic. 10 pic. 12 pic. 13 pic. 14 pic. 15 pic.

Trigger Activation
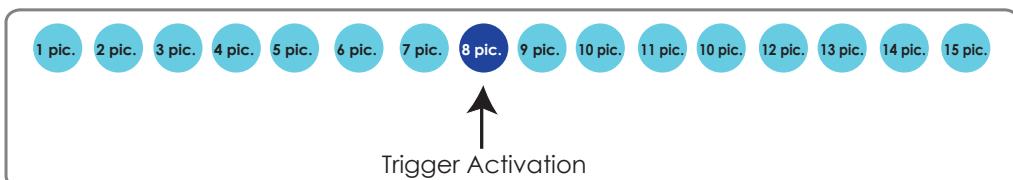
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:

Snapshot_20170320_100341

File name prefix　Date and time suffix
The format is: YYYYMMDD_HHMMSS

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a drop-down menu of existing medias will be available on the Media list. If you wish to add more media options, click **Add media** again.

Server	Media	Extra parameter
☐ SD	-----None----- ▼	SD test　View
	-----None-----	
	Snapshot	☐ Create folders by date time and hour automatically
☐ NAS	-----None----- ▼	
		View

Add server ▼　Add media ▼
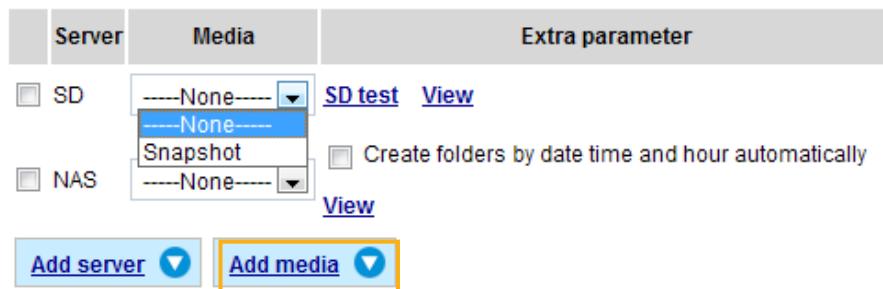
Media type - Video clip
Select to send video clips when a trigger is activated.

Media name: VideoClip

Media type

Attached media:
○ Snapshot
◉ Video clip

Source: Stream 1 ▼
Pre-event recording: 0　seconds [0~9]
Maximum duration: 5　seconds [1~20]
Maximum file size: 500　Kbytes [50~8192]
File name prefix: videoclip

○ System log

Save media　　Close

■ Media name: Enter a name for the media setting.

■ Source: Select the source of video clip.

■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ **Maximum duration**
Specify the maximum recording duration in seconds. Up to 20 seconds can be set.
For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.
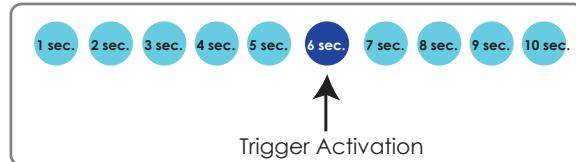
■ **Maximum file size**
Specify the maximum file size allowed.

■ **File name prefix**
Enter the text that will be appended to the front of the file name.
For example:

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

Media type - System log
Select to send a system log when a trigger is activated.

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

■ View: Click this button to open a file list window. This function only apllies when an SD card and networked storage are available.

If you click **View** button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 202. If you click **View** button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.

■ Create folders by date, time, and hour automatically: If you check this item, the system will automatically create sub-folders named by the date.

The following is an example of a file destination with recorded video clips:

The format is: YYYYMMDD
Click to open the directory

Click to delete all recorded data

Click to delete selected items
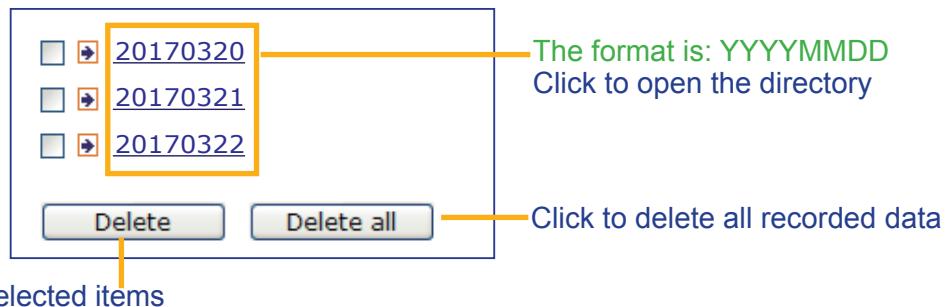
Click **20170320** to open the directory:

The format is: HH (24r)
Click to open the file list for that hour

Click to delete selected items

Click to go back to the previous level of the directory

Click to delete all recorded data

The format is: File name prefix + Minute (mm)
You can set up the file name prefix on Add media page.

Here is an example of the Event setting:

When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

The following is an example of the Event setting page:

When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mails.

If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name and click **Delete**. Note that you can only delete a server setting when the server setting is currently not applied to an event setting.

To remove a media setting from the list, select a media name and click **Delete**. Note that you can only delete a media setting when the media setting is currently not applied to an event setting.

Customized Script

This function allows you to upload a sample script (.xml file) to the camera, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK technical support.

Customized Script

Name	Date	Time
User1	2017/03/20	18:13:46
User2	2017/03/20	18:11:32

Add User1 ▾ Delete

Click to upload a file

Click to modify the script online

```
<?xml version="1.0" encoding="UTF-8"?>
<eventmgr version="0102">
<maxprocess>1</maxprocess>
<!-- from 08:30:00-20:30:00 on Monday to Friday every week -->
<schedule id="0">
<duration>
<weekday>1-5</weekday>
<time>08:30:00-20:30:00</time>
</duration>
</schedule>
<!-- Motion -->
<motion condition="0">
<status id="0">trigger</status>
<status id="1">trigger</status>
</motion>
<event id="0">
<description>Mail system log to email adddress</description>
<condition>c0</condition>
<scheduleno>0</scheduleno>
<delay>10</delay>
<!-- users can send email with title "Motion" to recipient pudding.yang@vivotek.com. The body
of mail is the log messages -->
<process>
/usr/bin/smtpclient -s "Motion" -f IP7139@vivotek.com -b /var/log/messages -S ms.vivotek.tw -
M 3 pudding.yang@vivotek.com
</process>
<priority>0</priority>
</event>
</eventmgr>
```

Upload

3-9. DI and DO

Connect DI or DO devices to the camera's terminal block, the camera will automatically detect the current connection state as pulled-high or pulled-low. You may then define the triggering condition.

Digital input: Select High or Low as the state of the signal to define the "Normal status" for the digital input. Connect the digital input lines to the Network Camera, and the camera will report the current status.

Digital output: Select Grounded or Open as the state of the signal to define the "Normal status" for the digital output. Connect the digital output lines to the Network Camera, and the camera will display the current status.

3-10. Maintenance

Export configuration file: Use this to export your current camera configuration. Use this to backup your video analytics configuration or to duplicate your configuration, such as using the same configuration for similar doors on train cabins.

Export log file: The log file mainly consists of your configuration changes and system statuses.

Upload configuration file: The Upload function can be used to import a pre-configured profile.

3-11. Remote Management

Remote Management is available by installing a remote management server instance on a Linux server that is located across the Internet. For bandwidth and latency concerns, video streaming and snapshot can be made via a cloud service, e.g., Amazon Cloud.

📝 NOTE:

Chrome, Firefox, and Safari on Windows, Mac, or Android devices can be used to access the remote management portal. Use of IE is not recommended for the lack of streaming service. Management and snapshot are still supported on IE.

3-11-1. Configuration
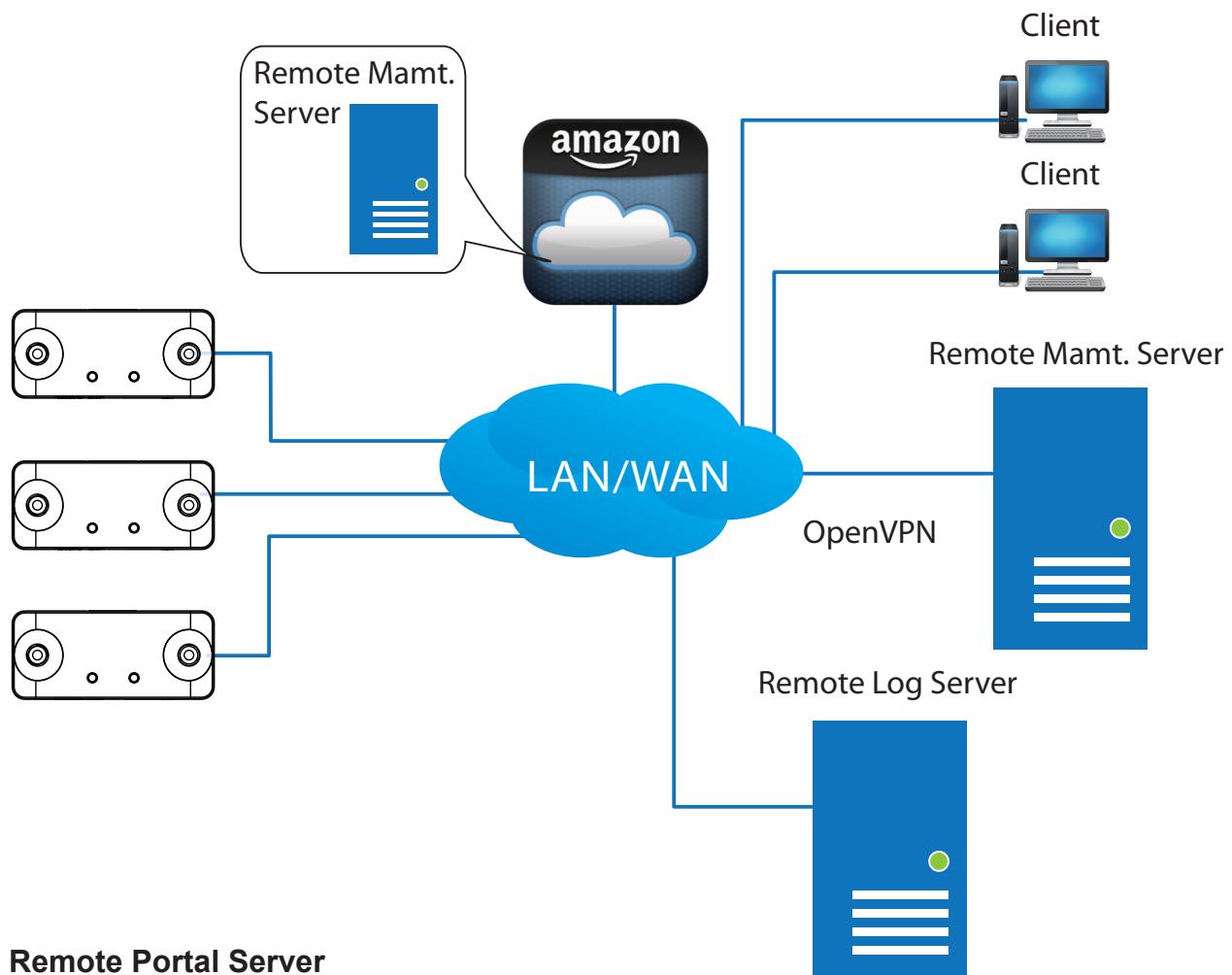
Remote Portal Server

A remote portal server is built on one running Ubuntu 14.04 TLS 54-bit (or 15.04). The ability to access the Internet from your server is a must.

You can then install the "mvaas_ezinstall.tar.gz onto your machine. Open a terminal and locate the installation file. Untar the package: tar -zxf mvaas_ezinstall.tar.gz.

Please contact VIVOTEK's technical support for the server package.

The untarred folder mvaas_easyinstall/ should contain the following:
- configuration: the main installation script
  - ./configure install : install command
    - Required system root privilege
    - Press y or [ENTER] during installation to allow
  - ./configure uninstall : uninstall command
- config: the configuration file for server installation
  - isEC2: Set it to 1 if you are operating with AWS EC2 with a public IP. Otherwise, keep this argument as 0.
  - The other items under [mongodb] are optional for user to change the mongodb account and password.

The command line execution look like the following:
$ ls
mvaas_ezinstall.tar.gz
$ tar -zxf mvaas_ezinstall.tar.gz
$ cd mvaas_easyinstall
$ vi config
…
isEC2=1
…
$ sudo ./configure install
...
Press [ENTER] to allow …
….
Are you sure to install packages .. [y/N] ? Y
…

You should then verify the execution results:

// following commands should all has one result (exactly one running process)
$ ps aux | grep register | grep -v 'grep'
$ ps aux | grep relay | grep -v 'grep'
$ ps aux | grep mongod | grep -v 'grep'
$ ps aux | grep supervisord | grep -v 'grep'
$ ps aux | grep openvpn | grep -v 'grep'
$ ps aux | grep redis-server | grep -v 'grep'
// check the logs of connections for serives and the devices
$ vi ${HOME}/register/log
$ vi ${HOME}/relay/log
// besides, you can setup your cameras to connect to this server and open a browser to connect to the portal server.

You should then enter the register server address and Device ID in the SC8131 camera's configuration page. Open a web console and go to **Stereo Analytics** > **Configuration** > **Remote management**. Enter the public IP of the remote portal server.

Note that the remote Log server can be another machine, the remote log service does not necessarily run on the same Linux server.
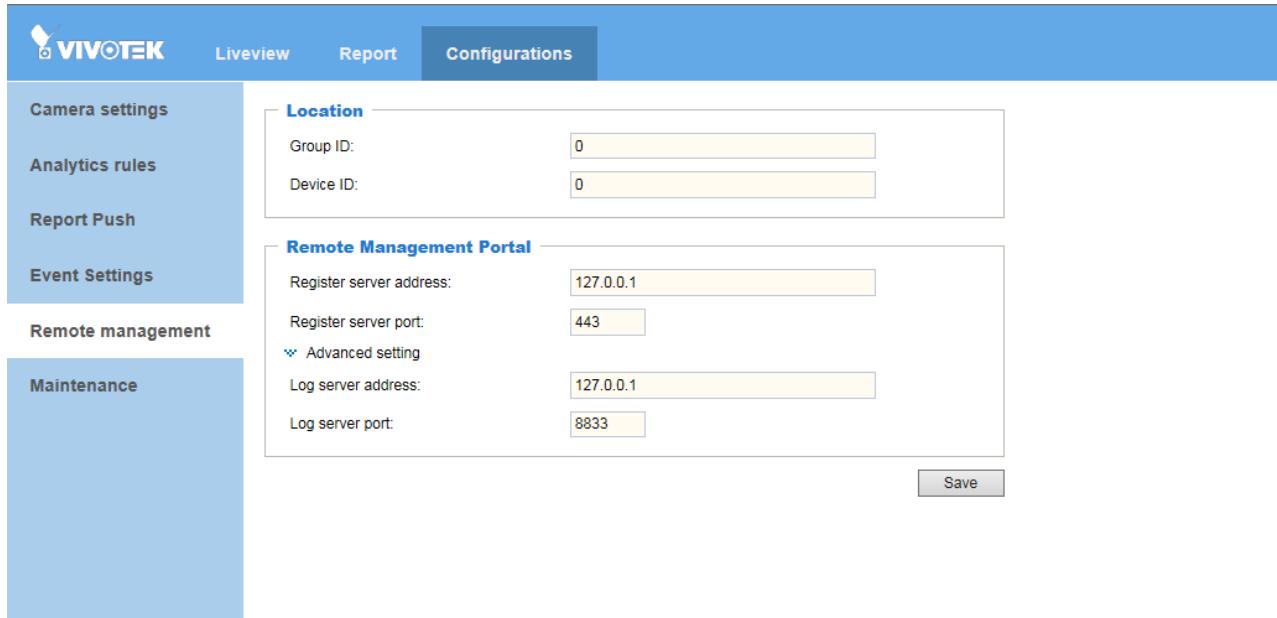
Cameras registered to the Remote Portal server will appear in its tree structure view.
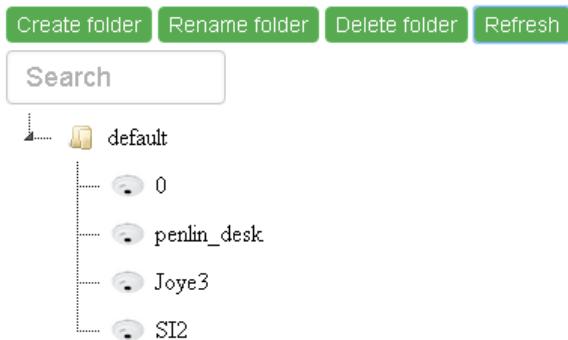
AWS, Amazon Web Services, or AWS EC2 (Elastic Cloud)

To utilize AWS cloud services, you have to register on AWS (aws.amazon.com). The procedure for registering and launching the Amazon cloud services is not a topic of this document. Please refer to the description on Amazon cloud for details.

Once you registered your AWS account, you can contact VIVOTEK's technical support for the AMI (Amazon Machine Image) share of the server instances that have already been established by VIVOTEK. You can then use the AMI snapshot to build your own Remote Portal on AWS.

OpenVPN

VPN is not a must for most services. An OpenVPN tunnel helps getting through complex routing schemes and acquire information, grouping information, live streaming, and snapshots from one or multiple SC8131 cameras. If applied, users can view the live streaming with tracking boxes, counting reports, and access the detailed configurations.

The OpenVPN package:

1. Acquire the installation package from VIVOTKE's technical support: openvpn-install-2.3.8-I601-x86_64.exe [Windows]. Note that there are many free OpenVPN client GUI versions on the Internet.
2. tunnelblick [Mac OSX] https://tunnelblick.net/downloads.html
3. config.zip. This is an OpenVPN configuration file and the operation requires SSL certifications.

To install the OpenVPN package:

1. Execute the installation program with a system manager privilege.
2. Unzip the config.zip into C:Program Files\OpenVPN\config\ to override certifications and configuration files if any previous instances should exist.
3. Execute the openvpn-gui.exe with a system manager privilege.
4. Change the VPN server IP address in the config file.
5. Click Connect in the OpenVPN Client GUI and later you should be able acquire the VPN IP (e.g., 10.8.0.14).
6. You should update the VPN server IP in the config file and change it to that of the Remote Portal server.

If you need to open a web console with a camera, you need to install an OpenVPN client on the computer from which you access the camera.
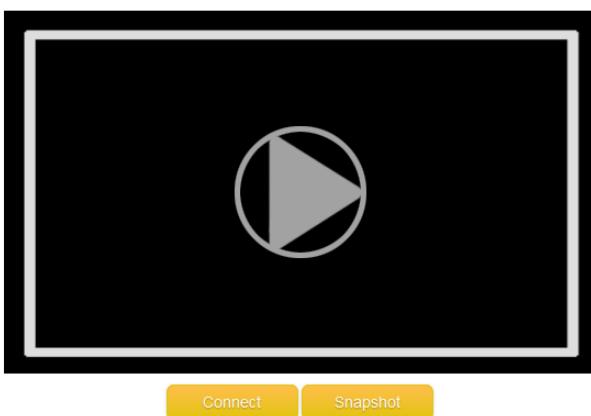
Refer to the instructions that came with your OpenVPN GUI for information on how to create public and private keys, CA certificates/keys for the server and clients.
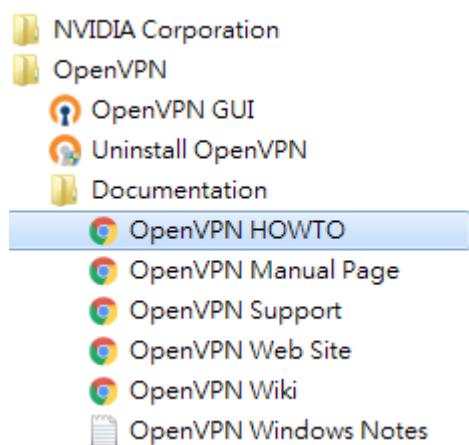
If using the OpenVPN tunnelblick:

1. Download and install this version from https://tunnelblick.net/downloads.html
2. Unzip the config.zip into anywhere you prefer and edit the client.ovpn to update the remote address to that of your Remote Portal server address.

```
proto udp

remote 52.33.127.104  1194
nobind
resolv-retry infinite
persist-key
persist-tun
```

3. Double click this client.ovpn file to let tunnelblick load it

To install the OpenVPN tunnelblick:

4. From the top tool bar, click Client to open the VPN server.
5. Wait until it connects to the server.
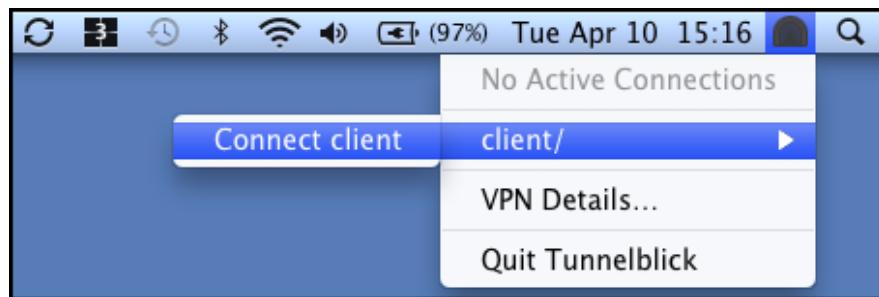
3-11-2. Open the Remote Portal

To access the Remote Portal:

1. Open a Chrome or Firefox browser and enter the Remote Portal server's IP address in the URL field.
2. Enter the default user name and password as: amin / 12345678. You can change the user name and password later.
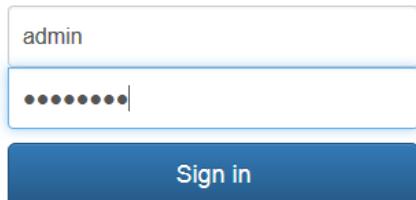
3. The portal main page displays. You can now start creating virtual folders on the device tree. Use the Create folder, Rename folder, Delete, and Refresh buttons to create a tree structure that best reflects your camera delpoyment.
4. By default, all registered cameras will be placed under the default folder. When folders are created, you can click and drag cameras to different folders.
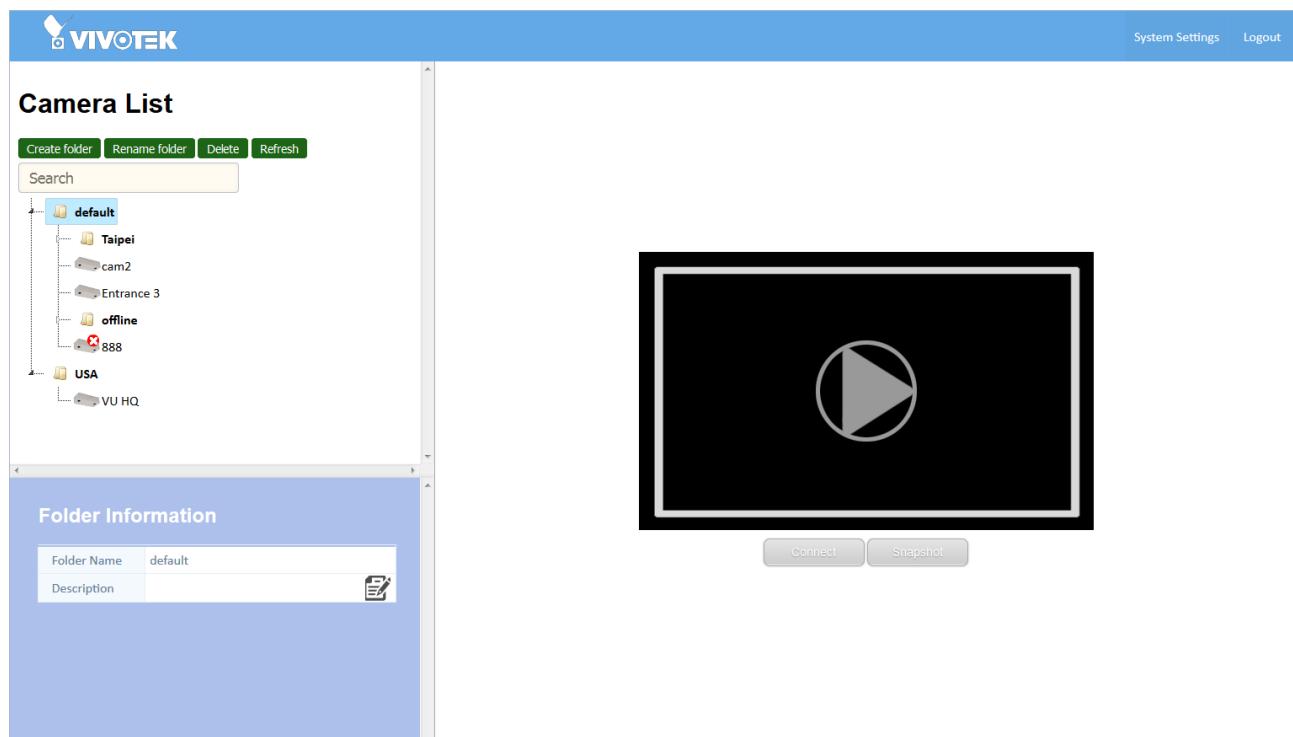
5. A single click on a camera displays its basic information, including its Group ID, and Device ID. When selected, the Playback, Connect and Snapshot buttons will also be available.

Playback: click to obtain a live view.
Connect: opens a web console with the camera.
Snapshot: takes a snapshot.
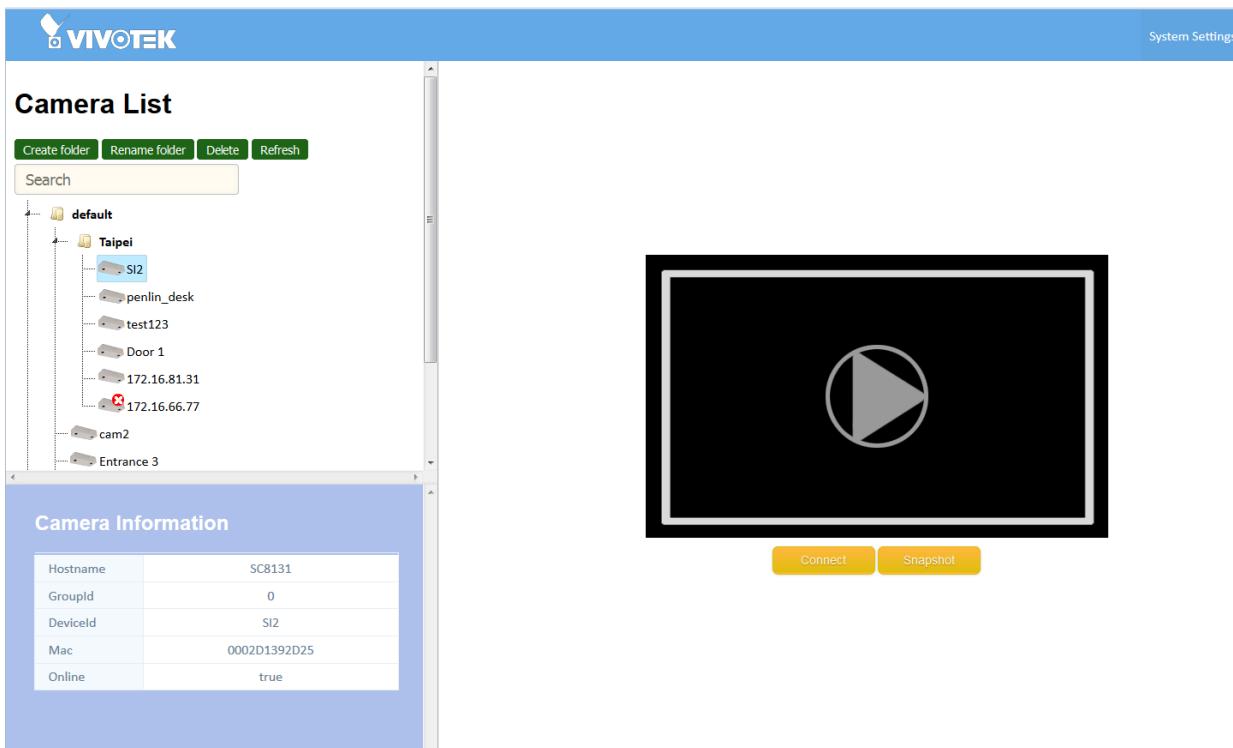
6. Click on System Settings on the upper right of the screen to change the default passowrd.
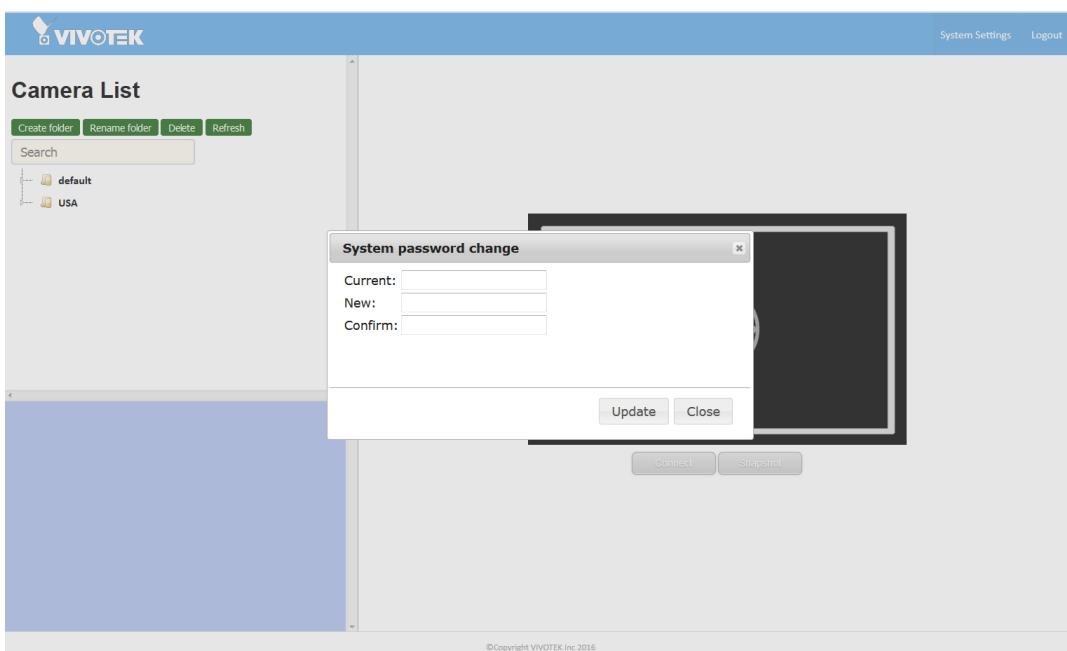
4. Stereo Camera CGI Commands

In addition to using web UI to set the camera, you can use CGI command to configure the related settings.

Algorithm Settings

Syntax:

http://<ip>/cgi-bin/admin/trackerctrl.cgi? <parameter>=<value>[&<parameter>=<value>…]

PARAMETER	VALUE	DEFAULT	DESCRIPTION
camheight	1.0~5.0 (Floating number)	2.4	Set camera's mounting height in meter.
minheight	0.1~5.0 (Floating number)	0.9	Minimum height of objects which will be considered for tracking.
maxheight	0.1~5.0 (Floating number)	2.1	Maximum height of objects which will be considered for tracking.
zoominfactor	1.0~1.8 (Floating number)	1.0	Digital zoom in the field of view.
algconfidence	0~30	5	User can adjust confidence level to filter out the controversial points of depth.

Example

Request:

http://<ip>/cgi-bin/admin/trackerctrl.cgi?camheight=2.6&minheight=0.5&maxheight=2.0

Event Push Settings

Syntax:

http://<ip>/cgi-bin/admin/scevent_update.cgi?target=<value>&action=<value>&<parameter>=<value>…

PARAMETER	VALUE	DEFAULT	DESCRIPTION
target	0~5		Specify the target server index
action	add, remove, update		add: set up a new server push with specified target number [note. specified target number must be not already running] update: modify a running server push with specified target number [note. specified target number must be running] remove: remove the running server push with a specified target number
name	string[40]	<blank>	Name for this server push. %N in FTP fileformat would be replaced with this value.
protocol	http, email, ftp		The protocol types of server
url	string[128]	<blank>	Valid IP address or domain name of server (only including the base domain http://test.httpserver.com:8080/vivotek/push)
port	1~65535		Port number of server to receive the pushed reports
uri	string[256]	<blank>	HTTP, FTP: the URI of the location for push server (e.g. http://test.httpserver.com:8080/vivotek/push) SMTP: receiver email account
usr	string[64]	<blank>	Required username for server authorization
pwd	string[64]	<blank>	Required password of corresponding usr for server authorization
schedule	0,		Schedule time in seconds. only following

	60, 300, 900, 1800, 3600, 43200, 86400		schedules are accepted : enum{60, 300, 900, 1800, 3600, 43200, 86400}
aggregation	60, 300, 900, 1800, 3600, 43200, 86400		Aggregation level in seconds. only the same options with schedule are accepted.
format	xml, json, csv		Report format. only accept enum{xml, json, csv} three types
lite	0,1	0	1: turn on lite mode for this server push 0: turn off lite mode for this server push
sender	string[64]	<blank>	The sender email account. [only required for protocol=email]
fileformat	string[64]	report_%T.%F	The push report filename format. %T: Report timestamp in UTC time %F: Report format in xml, json or csv %N: User defined server name %M: Mac address in serial %G: Group ID %D: Device ID %S: Schedule duration in second %A: Aggregation level in second %L: "LITE" if in lite mode, "" otherwise [only required for protocol=ftp]

Example

Request:

http://<ip>/cgi-bin/admin/scevent_update.cgi?target=0&action=add&name=HTTP&aggregation=60&schedule=60&format=xml&lite=0&protocol=http&url=172.16.2.42&uri=/test.cgi&usr=test&pwd=123&port=80

✏ **NOTE:**

If you should need to contact VIVOTEK technical support for help with the configuration, please provide the following:

1. SC8131 firmware version.

2. Installation information, e.g., height and position (taking pictures of the camera and the installation site is highly recommended).

3. Snapshots of the environments.

4. Recorded video (in the side-by-side view) from the SC8131. The preferred configuration for stream 1 is CBR, target bit rate 8Mb/s, at 30fps, frame rate priority. Use IE10 to record stream 1 for our reference.

5. Export the camera's configuration profile.

- You can install VIVOTEK's VAST software to help collect data from one or multiple stereo cameras, and these data can be collected to form comparative charts in a chronological view. Meta data is collected through RTSP, and CGI requests can be made via HTTP.
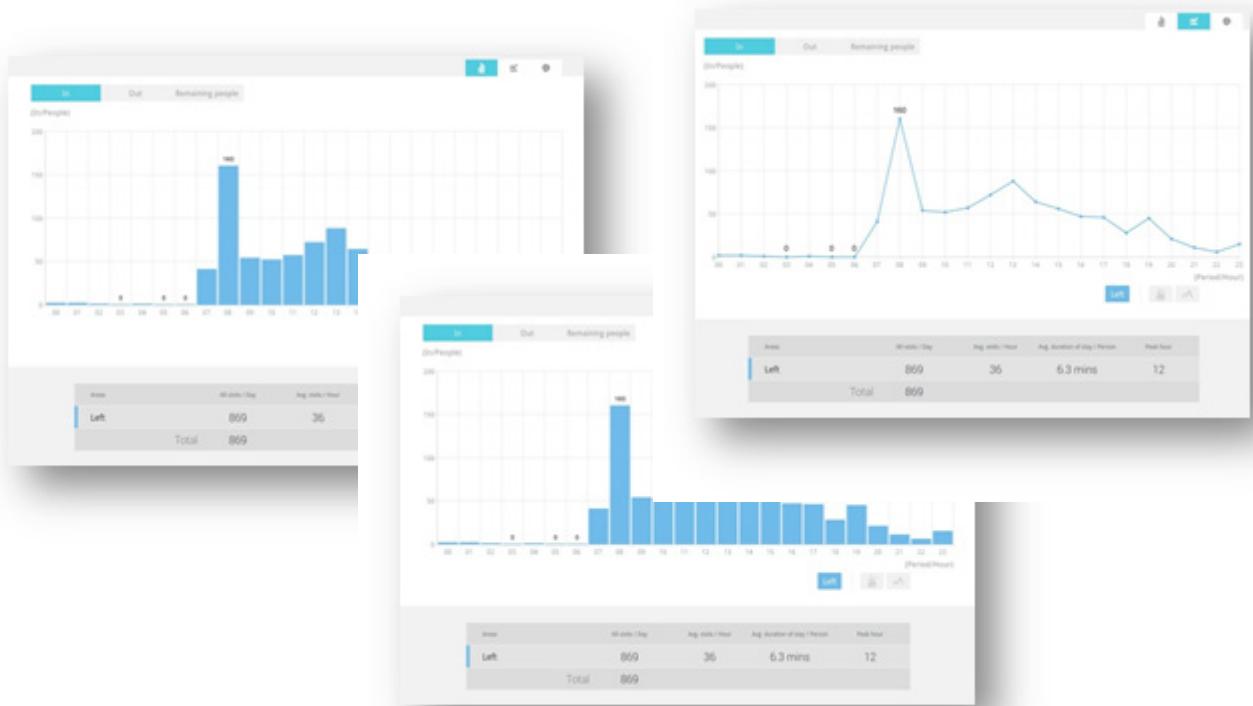
Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.
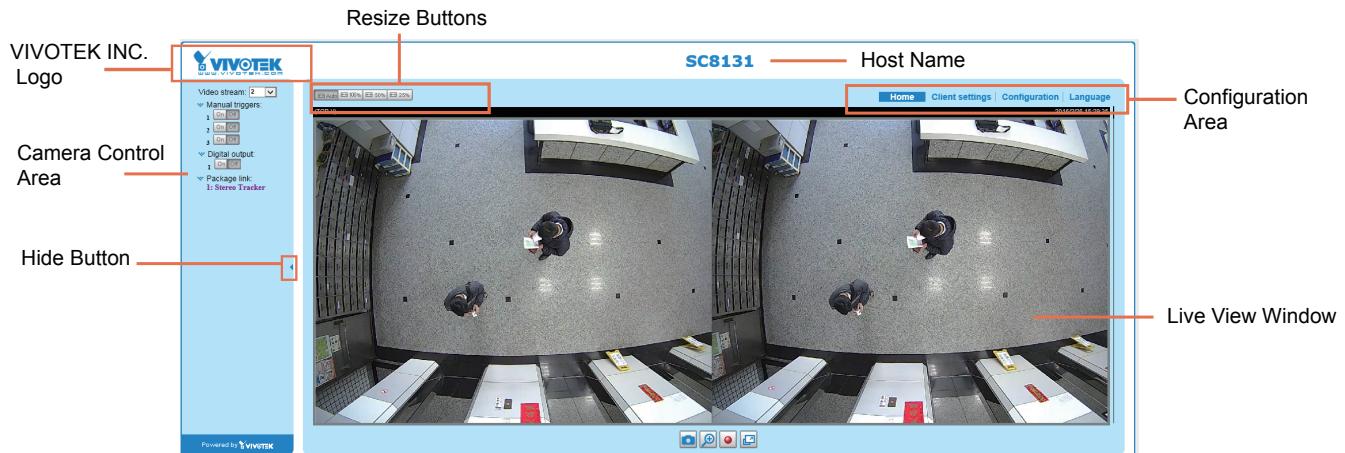
VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 139.

Camera Control Area

Video Stream: This Network Camera supports multiple streams (stream 1 ~ 3) simultaneously. You can select any of them for live viewing. For more information about multiple streams, please refer to page 157 for detailed information.

Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting on Application page before enable this function. A total of 3 event settings can be configured. For more information about event setting, please refer to page 99. If you want to hide this item on the homepage, please go to **Configuration> System > Homepage Layout > General settings > Customized button** to deselect "show manual trigger button".

Digital Output: Click to turn the digital output device on or off.

Package link: Click to open the Stereo Tracker monitoring and configuration utility.

Refer to page 51 for the configuration details about the embedded **Stereo Tracking** and **Counting** functionality.

Configuration Area

<u>Client Settings</u>: Click this button to access the client setting page. For more information, please refer to Client Settings on page 132.

<u>Configuration</u>: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 138.

<u>Language</u>: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. Please note that you can also change a language on the Configuration page; please refer to page 138.

Hide Button

You can click the hide button to hide the control panel or display the control panel.

Resize Buttons

 :
Click the Auto button, the video cell will resize automatically to fit the monitor.
Click 100% is to display the original homepage size.
Click 50% is to resize the homepage to 50% of its original size.
Click 25% is to resize the homepage to 25% of its original size.

Live Video Window

■ The following window is displayed when the video mode is set to H.264:

<u>Video Title</u>: The video title can be configured. For more information, please refer to Video Settings on page 151.

<u>H.264 Protocol and Media Options</u>: The transmission protocol and media options for H.264 video streaming. For further configuration, please refer to Client Settings on page 132.

<u>Time</u>: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 151.

<u>Title and Time</u>: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 152.

✏ **NOTE:**

・ For a megapixel camera, it is recommended to use monitors of the 24" size or larger, and are capable of 1600x1200 or better resolutions.

Video Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

📷 Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

🔍 Digital Zoom: Click and uncheck "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.
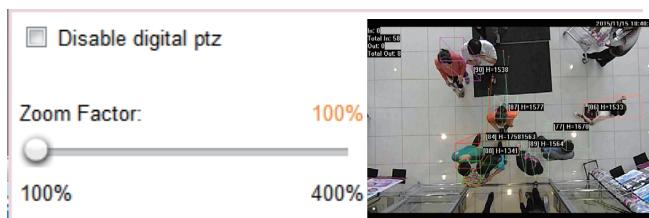
⏸ Pause: Pause the transmission of the streaming media. The button becomes the ▶ Resume button after clicking the Pause button.

⏹ Stop: Stop the transmission of the streaming media. Click the ▶ Resume button to continue transmission.

⏺ Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the ⏹ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 133 for details.

⛶ Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Media > Image on page 152.

Time: Display the current time. For more information, please refer to Media > Image on page 152.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 152.

Video Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the █ Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 133 for details.

Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.
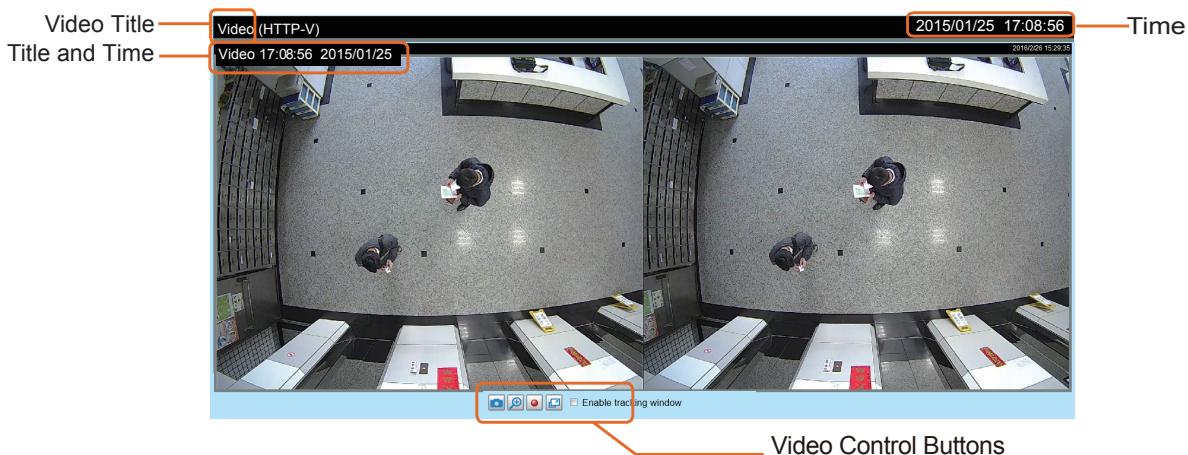
Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264 Protocol Options

H.264 Protocol Options
- ○ UDP Unicast
- ○ UDP Multicast
- ◉ TCP
- ○ HTTP

Depending on your network environment, there are four transmission modes of H.264 streaming:

UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 169.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

MP4 Saving Options

Users can record live video as they are watching it by clicking [●] Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files. The location can be changed.

File name prefix: Enter the text that will be appended to the front of the video file name. A specified folder will be automatically created on your local hard disk.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.

CLIP_20110628-180853

File name prefix   Date and time suffix
The format is: YYYYMMDD_HHMMSS

Local Streaming Buffer Time

Due to the possiblity of encountering unsteady bandwidth flow, the live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on console PC's cache memory for a configurable period of time before being played on the live view window. This helps you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay for 3 seconds.

Joystick Settings
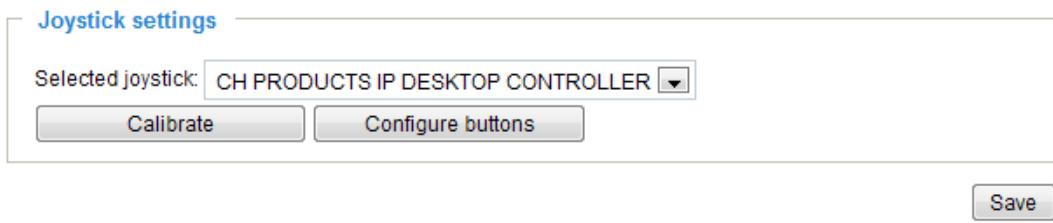
Enable Joystick

Connect to the USB plug of the joystick to a USB port on your management computer. Supported by the plug-in in the main page (Microsoft's DirectX), once the plug-in in the main page is loaded, it will automatically detect if there is any joystick on the computer. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices. Please follow the instructions
below to enable joystick settings.

1. Right-click on a live view window. Select Joystick Settings. If your joystick is working properly, it will be displayed on the drop-down list.

c. Select the joystick you want to configure. Check **Enable Joystick**, then click **Configure Buttons** to open Buttons configuration window.
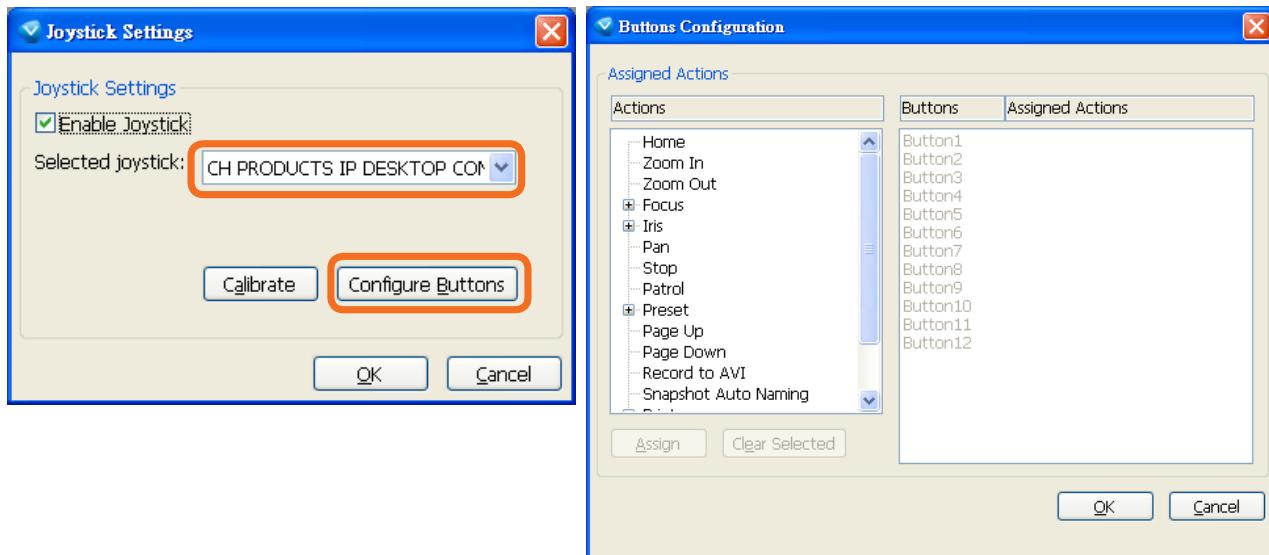
Buttons Configuration

In Button Configuration window, the left column shows the actions you can assign, and the right column shows the functional buttons and assigned actions. The number of buttons may differ from different joysticks.

Please follow the steps below to configure your joystick buttons:

1. Choosing one of the actions and click **Assign** will pop up a dialog. Then you can assign this action to a button by pressing the joystick button or select it from the drop-down list. For example: Assign **Home** (move to home position) to Button 1.
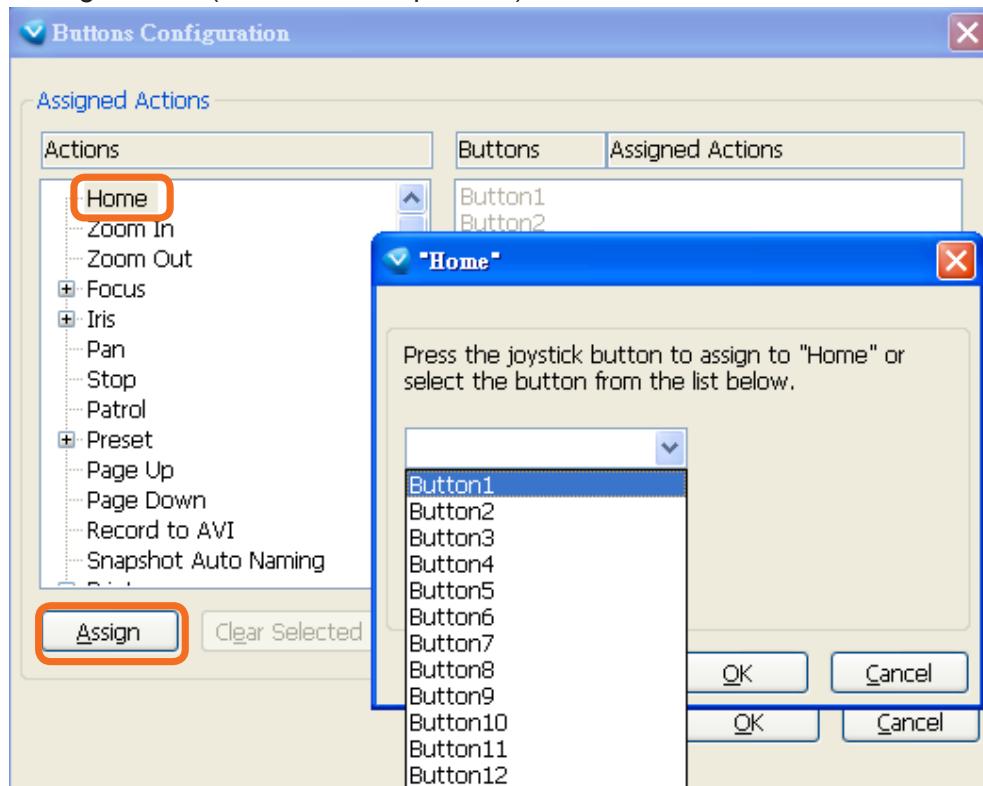
2. Click **OK** to confirm the configuration.
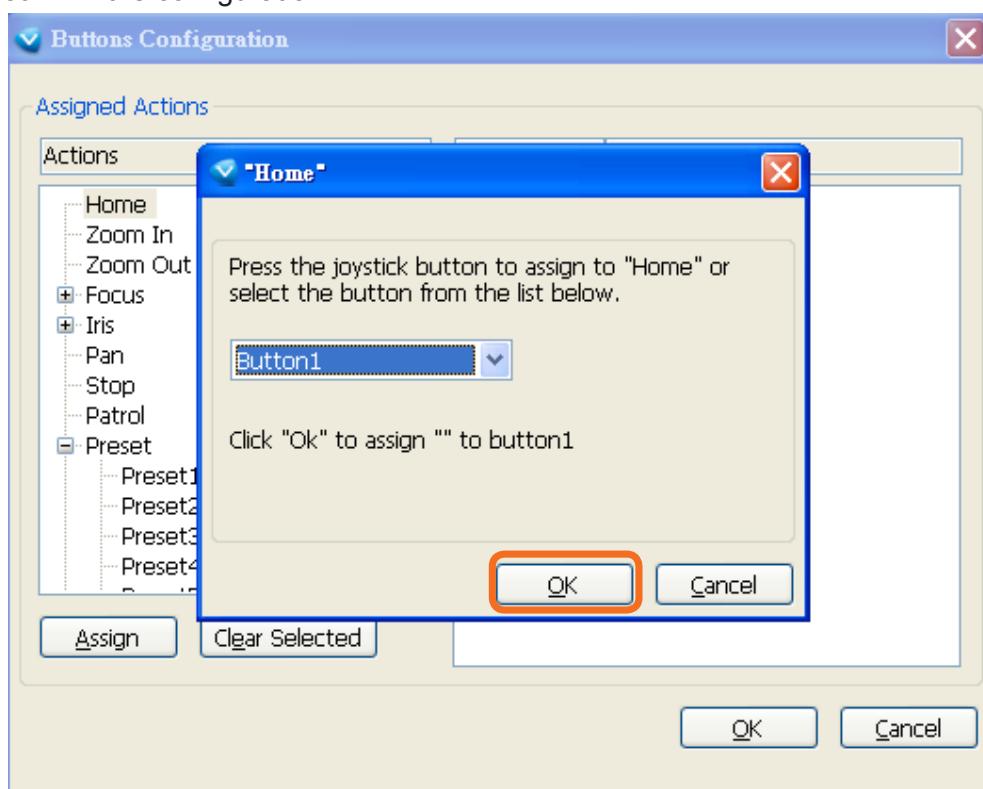
3. The Assigned Action will appear beside Button 1 in the right column as shown in the following diagram. Note that a button can only be assigned with an action. If you want to modify the settings, select the action on the list and click **Clear Selected**.
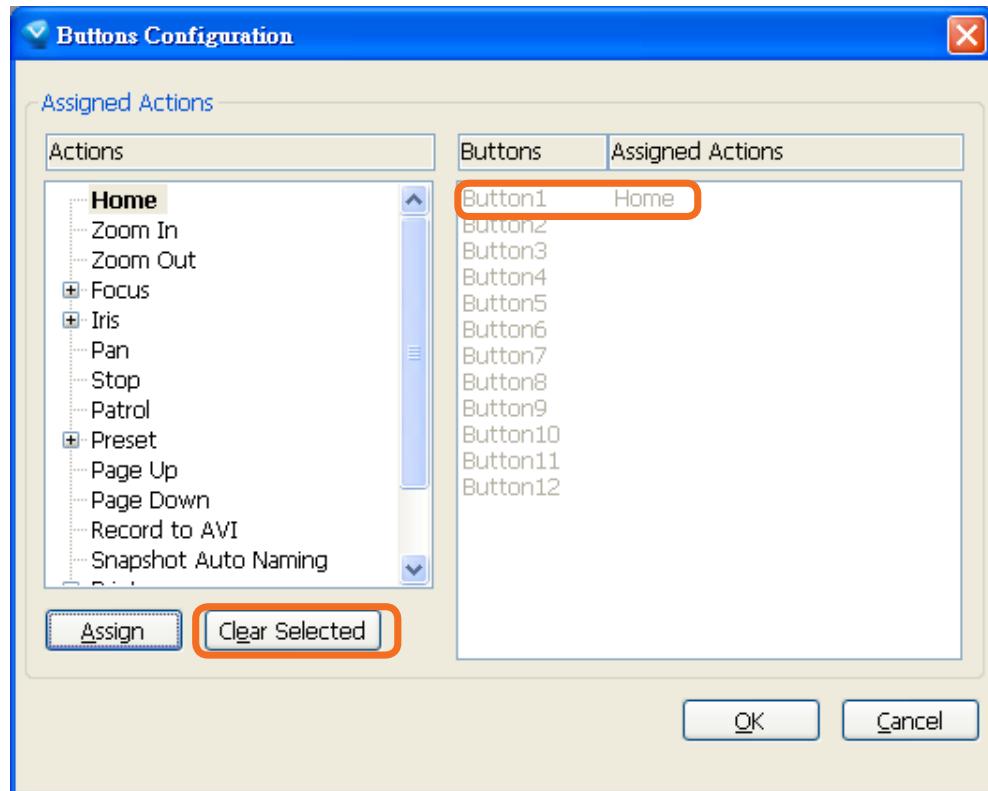
4. If you want to assign additional actions, repeat step a.~c. When all settings are complete, click **OK** to save the settings or click **Cancel** to discard the settings.
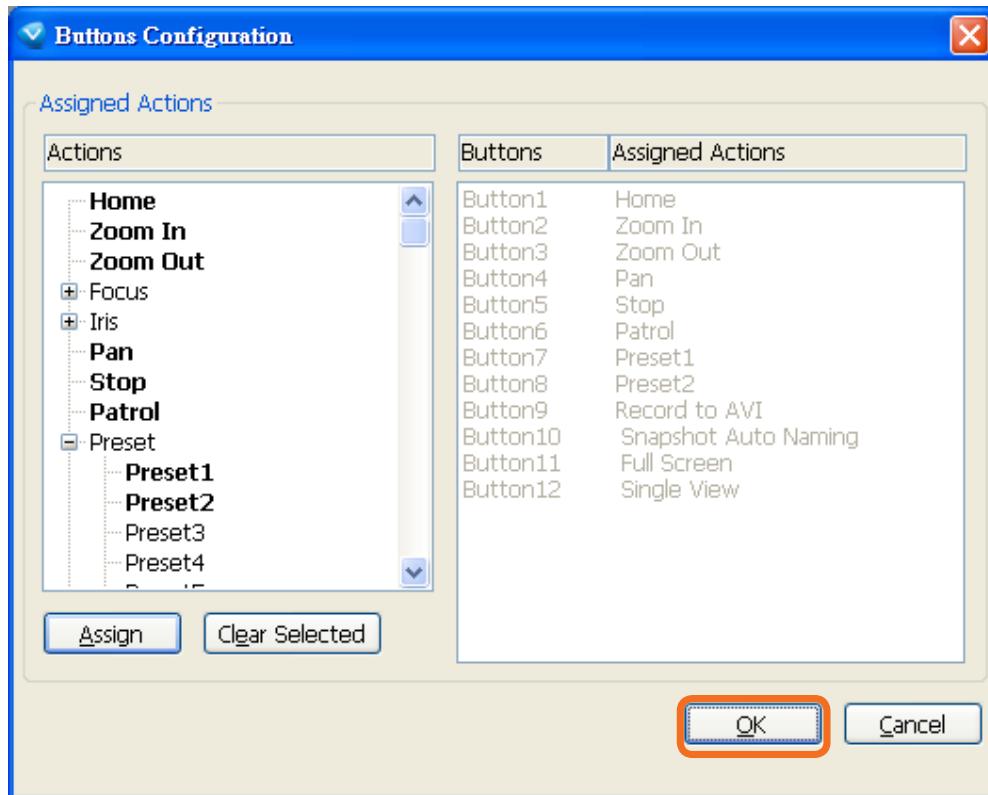
5. Click **OK** to save the settings or click **Cancel** to discard the settings.
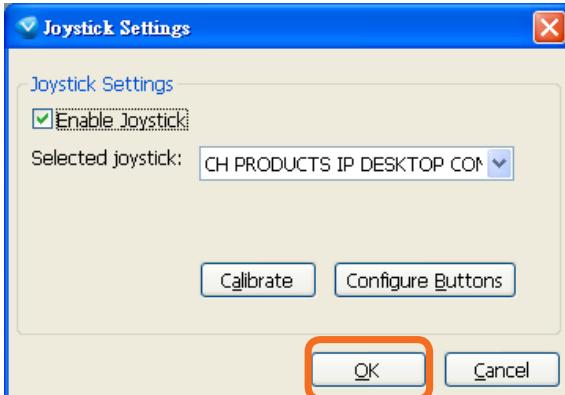
✎ **NOTE:**

- If you want to assign Preset actions to your joystick, the preset locations should be configured in advance.
- If your joystick is not working properly, it may need to be calibrated. Click the Calibrate button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.
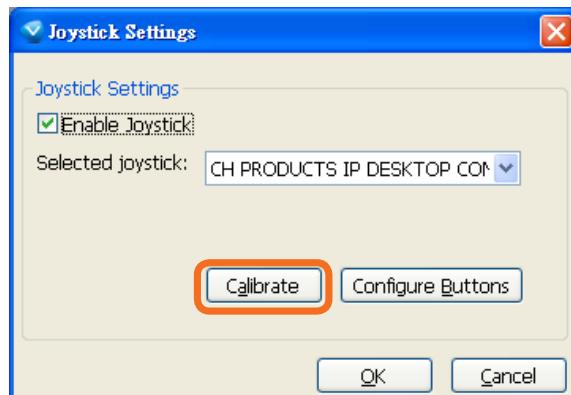
- The joystick will appear in the Game Controllers list in the Windows Control panel. If you want to check out for your devices, go to the following page: Start -> Control Panel -> Game Controllers.

Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort.

In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the main page interface:
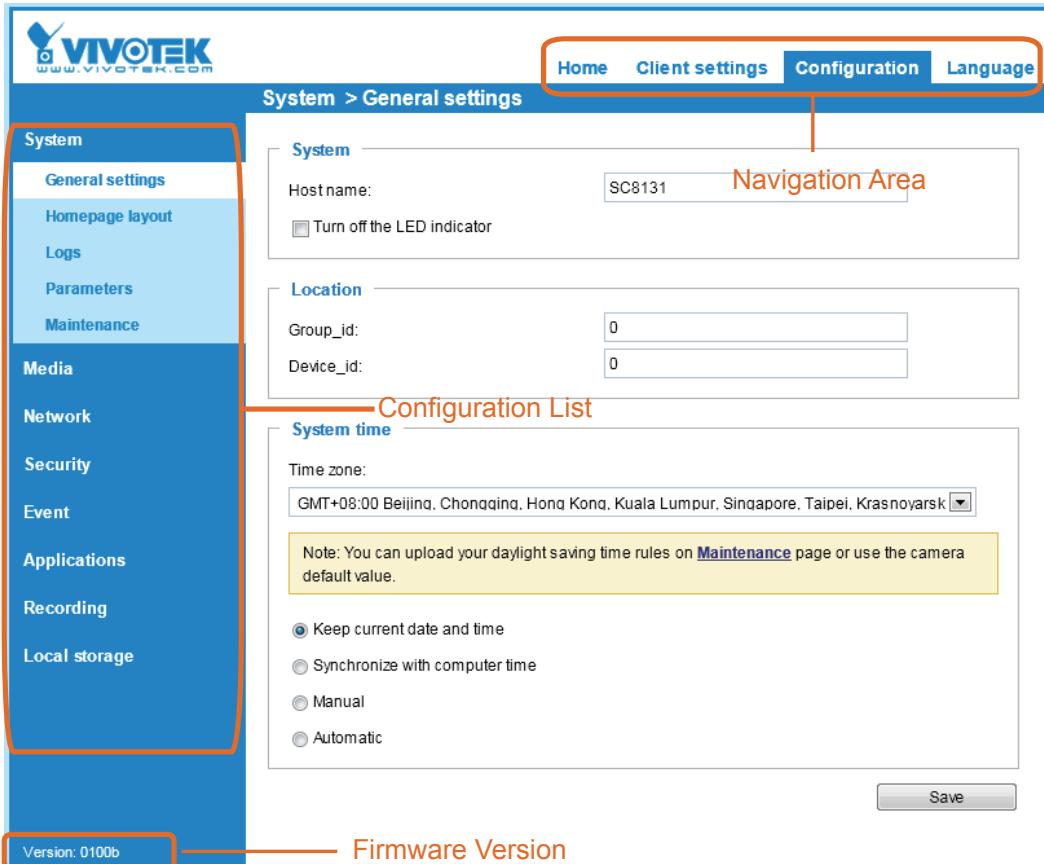
Each function on the configuration list will be explained in the following sections.

Navigation Area provides an instant switch among **Home** page (the monitoring page for live viewing), **Client settings**, **Configuration** page, and multi-language selection.

System > General settings

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System, and System Time. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page, and also on the view cell of ST7501 and VAST management software.

Turn off the LED indicators: If you do not want others to notice the network camera is in operation, you can select this option to turn off the LED indicators.

Location

Group_id; Device_id: These IDs are used to identify the individual cameras deployed at the same installation site. For example, multiple stereo cameras can be installed in the same shop. You can identify the owner of analytics reports, e.g., collected via an HTTP server, using their unique IDs.

System time

Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Synchronize with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 148 for details.

System > Homepage layout

This section explains how to set up a customized homepage layout.

General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

<u>Logo graph</u>
Here you can change the logo that is placed at the top of your homepage.

Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

<u>Customized button</u>
If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** field. Click **Save** to enable the settings.
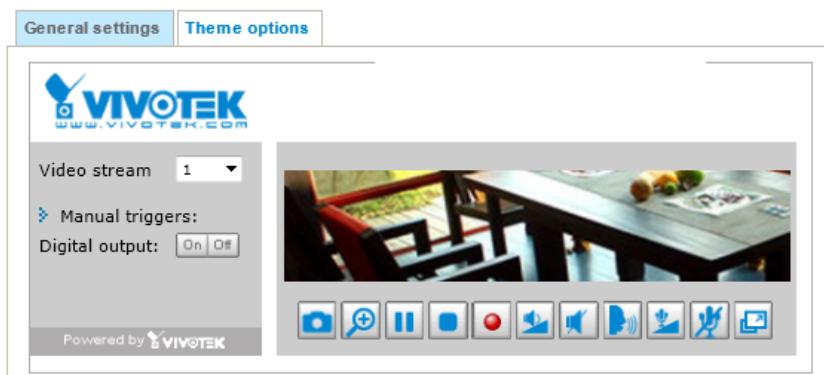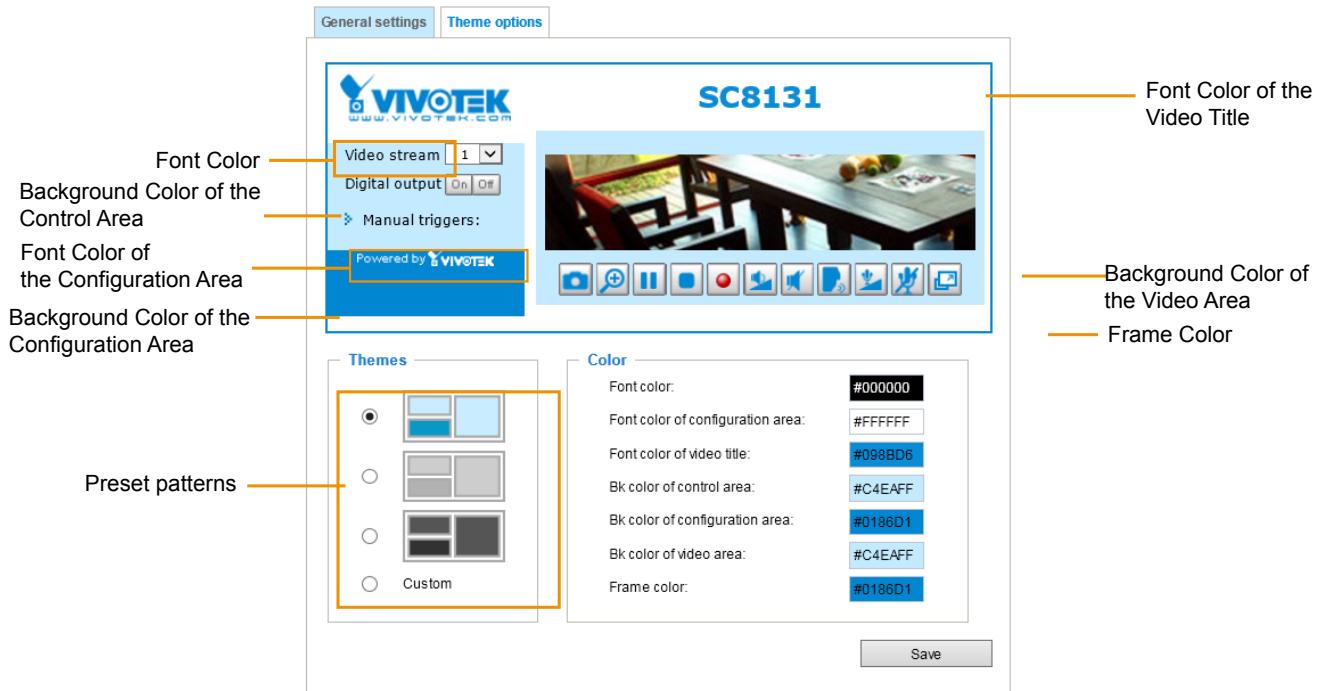
System > Logs

This section explains how to configure the Network Camera to send the system log to a remote server as backup.

Log server settings

Follow the steps below to set up the remote log:

1. Select **Enable remote log**.
2. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

System log

This column displays the system log in a chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

You can install the included VAST recording software, which provides an Event Management function group for delivering event messages via emails, GSM short messages, onscreen event panel, or to trigger an alarm, etc. For more information, refer to the VAST User Manual.
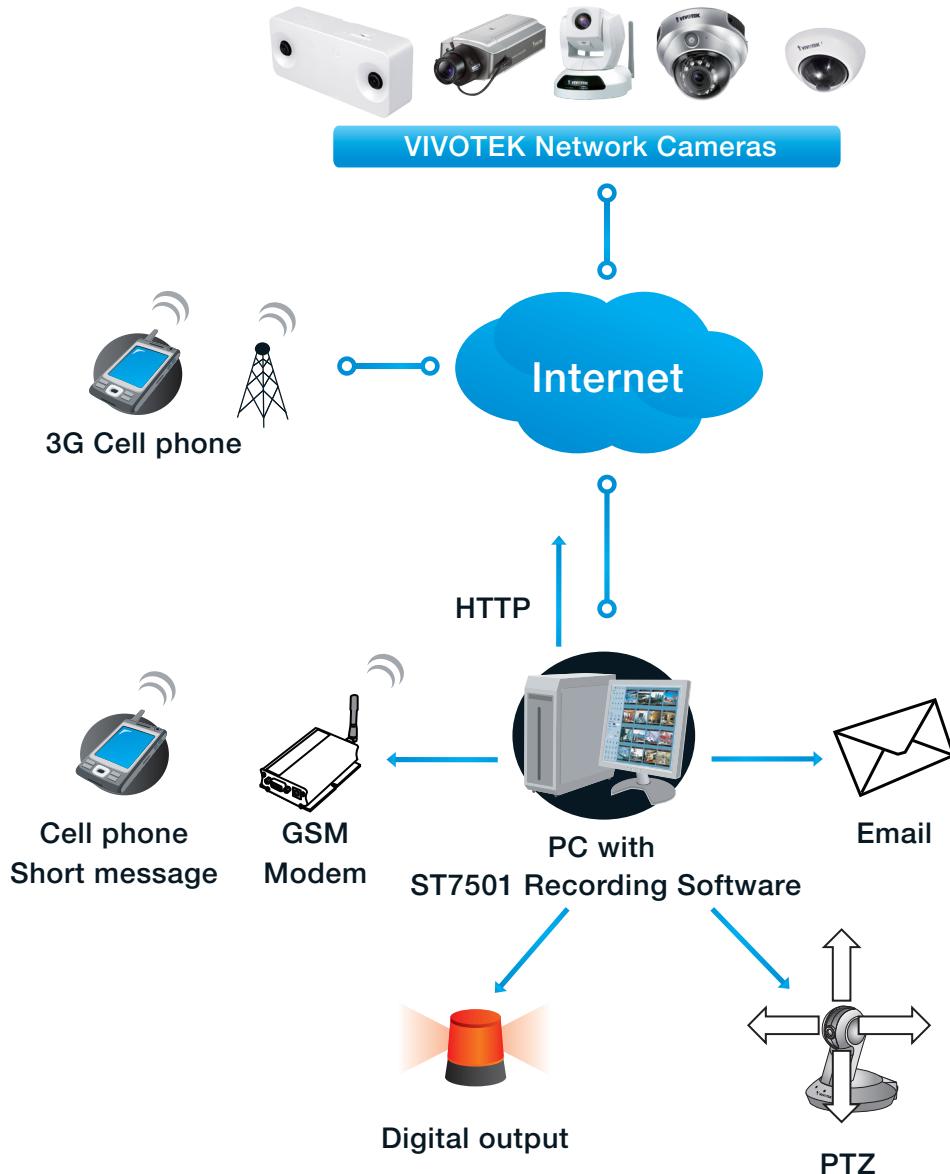
Access log


```
System log    Access log

Jan 5 11:36:28 [RTSP SERVER]: Start one session, IP=172.16.2.52
Jan 5 11:49:15 [RTSP SERVER]: Start one session, IP=192.168.4.105
Jan 5 13:11:20 [RTSP SERVER]: Start one session, IP=192.168.4.105
```

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

System > Parameters

The View Parameters page lists the entire system's parameters. If you need technical assistance, please provide the information listed on this page.


```
Parameters

system_hostname='SC8131'
system_ledoff='0'
system_date='2015/04/20'
system_time='11:46:20'
system_location_groupid='0'
system_location_deviceid='0'
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-16
system_updateinterval='0'
system_info_modelname='SC8131'
system_info_extendedmodelname='SC8131'
system_info_serialnumber='0002AB81C112'
system_info_firmwareversion='SC8131-VVTK-0100b'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
```

System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

General settings > Upgrade firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.

Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and locate the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see "Reboot system now!! This connection will close". After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.

> Reboot system now!!
> This connection will close.

The following message is displayed when you have selected an incorrect firmware file.

> Starting firmware upgrade...
> Do not power down the server during the upgrade.
> The server will restart automatically after the upgrade is completed.
> This will take about 1 - 5 minutes.
> Wrong PKG file format
> Unpack fail

General settings > Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.

> The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
> If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

General settings > Restore

This feature allows you to restore the Network Camera to factory default settings.

Network: Select this option to retain the Network Type settings (please refer to Network Type on page 162).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

Custom Language: Select this option to retain the Custom Language settings.

VADP: Retain the VADP modules (3rd-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.

Import/Export files

This feature allows you to Export / Update daylight saving time rules, custom language file, configuration file, and server status report.

Export daylight saving time configuration file: Click to set the start and end time of DST (Daylight Saving).

Follow the steps below to export:
1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will prompt as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.
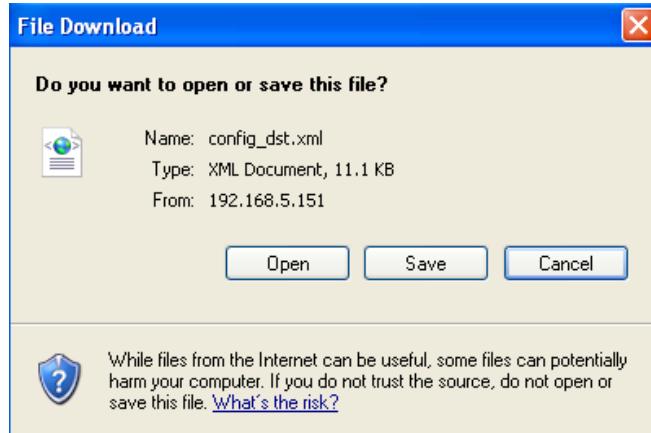
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.
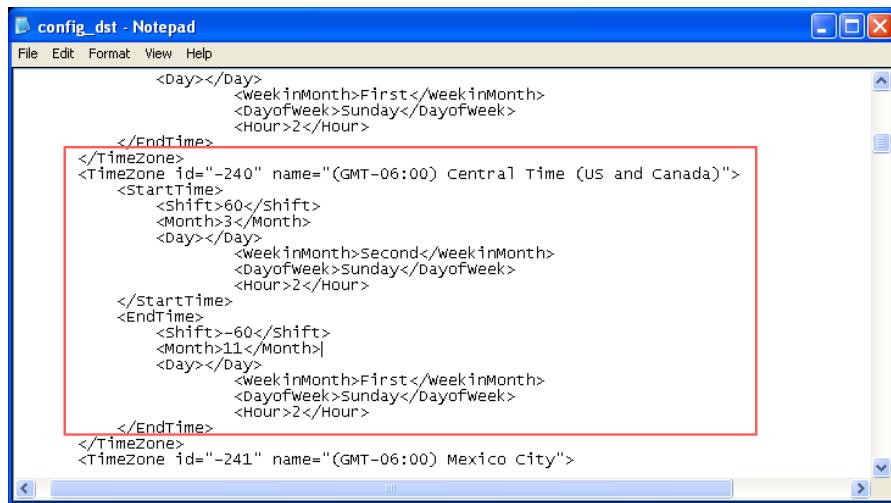
Update daylight saving time rules: Click **Browse…** and specify the XML file to update.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.
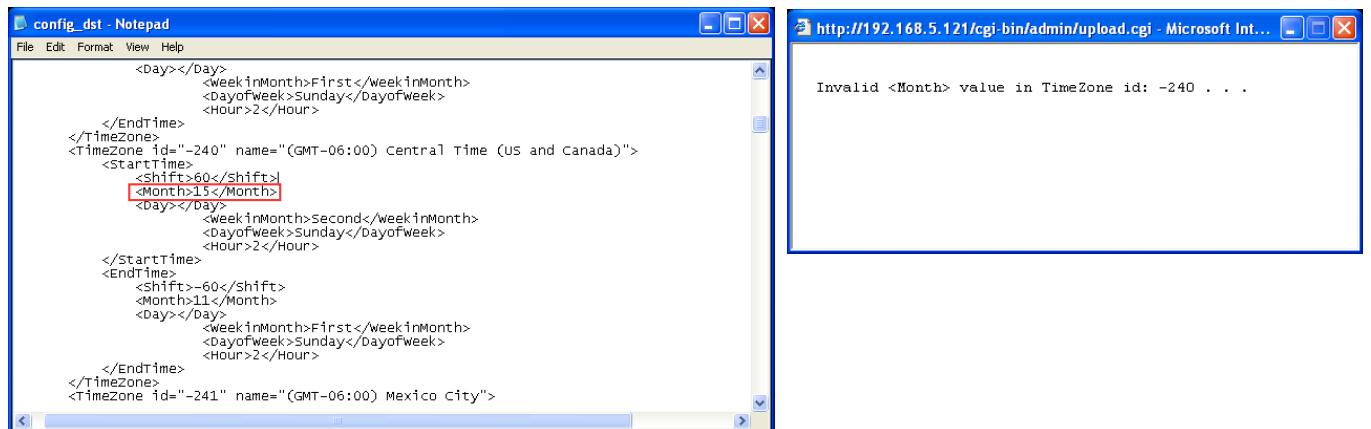
The following message is displayed when attempting to upload an incorrect file format.

Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 简体中文, and 繁體中文.

Update custom language file: Click **Browse…** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server staus report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message ... and so on.

☀ Tips:

If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

Applicable scenario:
(1) Power disconnected during firmware upgrade.
(2) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

You can use the following methods to activate the camera with its backup firmware:
(1) Press and hold down the reset button for at least one minute.
(2) Power on the camera until the Red LED blinks rapidly.
(3) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When tthis process is completed, the LED status should return to normal.

Media > Image

This section explains how to configure the image settings of the Network Camera. It is composed of the following four columns: General settings, Picture settings, Exposure, and Privacy mask.

General settings

Video title

Show_timestamp_and_video_title_in_video_and_snapshots: Enter a name that will be displayed on the title bar of the live video as the picture shown below.

Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

Timestamp and video title font size: Select the font size for the time stamp and title.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Image settings

On this page, you can tune the White balance, Image adjustment and WDR enhanced .

Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations
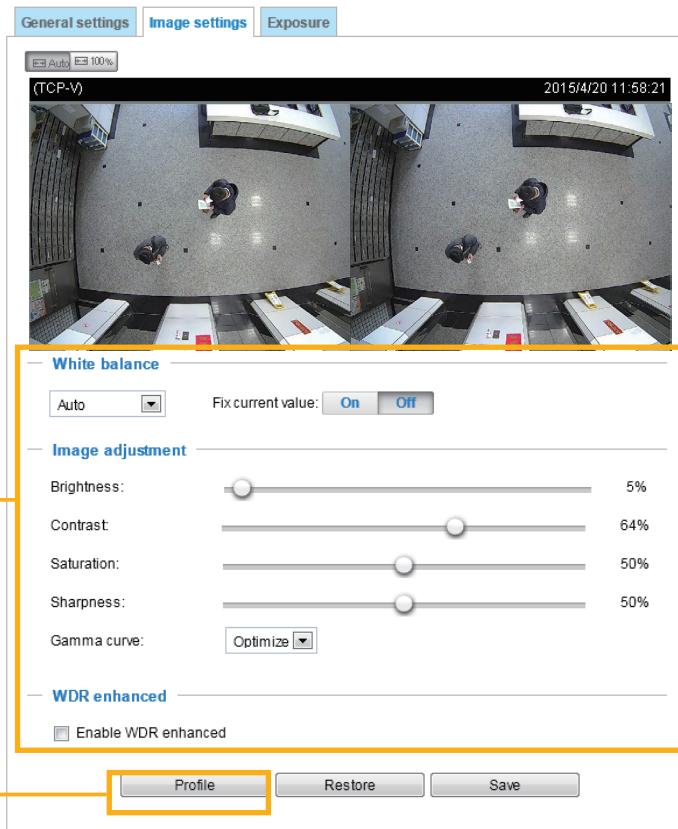
White balance: Adjust the value for the best color temperature.
■ You may follow the steps below to adjust the white balance to the best color temperature.

1. Place a sheet of paper of white or cooler-color temperature color, such as blue, in front of the lens, then allow the Network Camera to automatically adjust the color temperature.
2. Click the **On** button to **Fix current value** and confirm the setting while the white balance is being measured.

■ You may also manually tune the color temperature by pulling the RGain and BGain slide bars.

Image Adjustment
■ Brightness: Adjust the image brightness level, which ranges from 0% to 100%.

■ Contrast: Adjust the image contrast level, which ranges from 0% to 100%.

■ Saturation: Adjust the image saturation level, which ranges from 0% to 100%.

■ Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.

■ Gamma curve: Adjust the image sharpness level, which ranges from 0.45 to 1.
   You may let firmware **Optimize** your display or select the **Manual** mode, and pull the slide bar pointer to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

Note that the **Preview** button has been cancelled, all changes made to image settings is directly shown on screen. You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting. You can also click on **Profile** to adjust all settings above in a pop-up window for special lighting conditions.

Activated period: Select the mode this profile to apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

Noise reduction
■ Check to enable noise reduction in order to reduce noises and flickers in image. This applies to the onboard Noise Reduction feature. Use the pull-down menu to adjust the reduction strength. Note that applying this function to the video channel will consume system computing power.

Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level or disable the function.

Exposure

On this page, you can set the Measurement window, Exposure level, Exposure mode, and Iris mode. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.

Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations
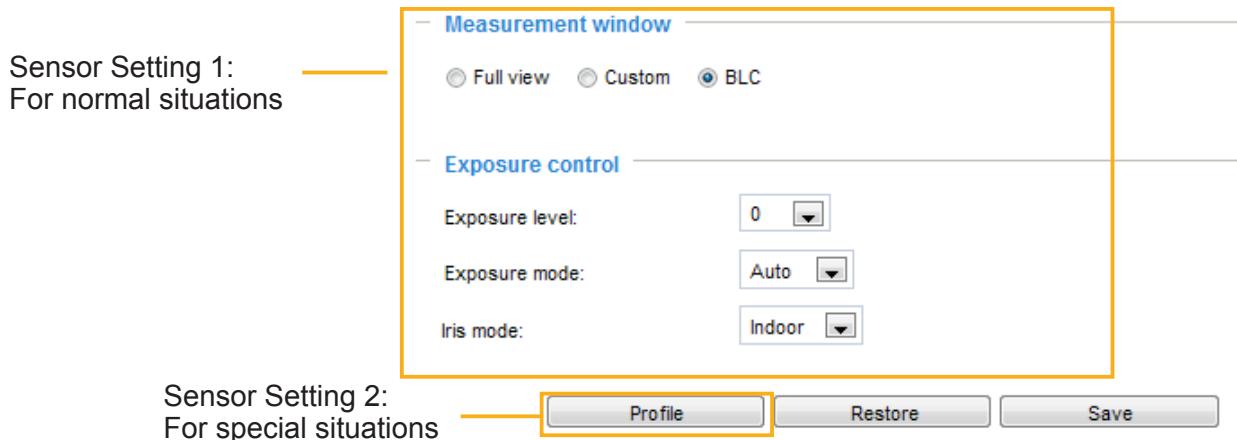
Measurement Window: This function allows users to configure measurement window(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background, you may want to exclude the bright sunlight shining through a building's corridor.

■ Full view: Calculate the full range of view and offer appropriate light compensation.

■ Custom: This option allows you to manually add specific windows as measuring areas. The measuring window refers to "weighed window" where the lighting condition within the particular area is taken into account. Camera firmware then adopts the weighed averages method to calculate the value.

A total of 10 inclusive windows can be created for a view.

Note that the title pane of the Include window is not included into the calculation.
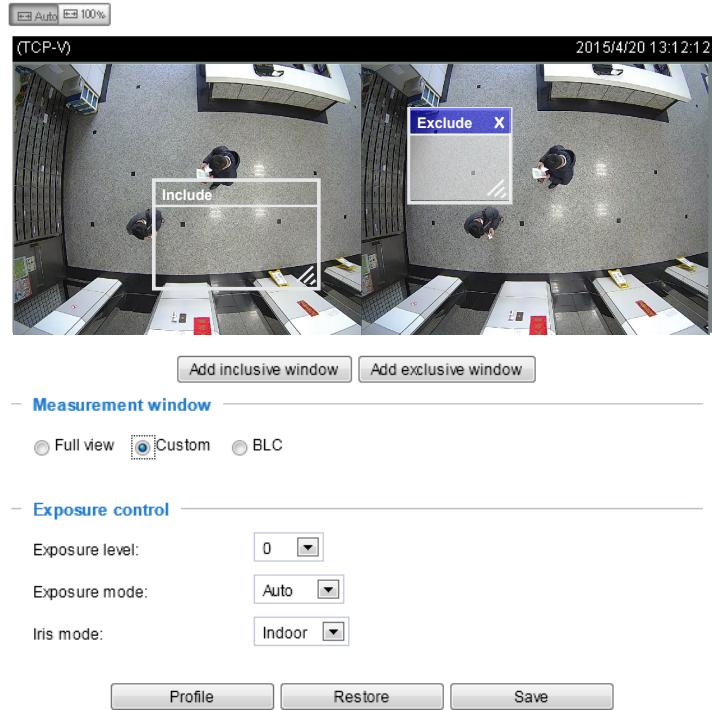
■ BLC: When selected, a BLC window will appear on screen meaning that the center of the scene will be taken as a weighed area. This option enables light compensation for images that are too dark or too bright to recognize; for example, for the dark side of objects that is posed against bright sunlight.

Exposure control:

■ **Exposure level**: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright). You can click on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automatically tune to an optimal imaging result. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

■ **Exposure mode**:   Select **Auto** or **Fixed iris** mode according to your needs.

Fixed: Select **Fixed** to configure a fixed exposure time and gain. Then, tune the slide bar to set the Exposure time and Gain Control to the best image quality. A shorter exposure time allows less amount of light to enter the sensor; while a higher gain control value generates certain amount of noises.

Auto: If you set Exposure mode as **Auto**, the Exposure time and Gain control will not be

configurable since the sensor library will automatically adjust the value according to the ambient light. Then you can configure iris mode as "indoor" or "outdoor" to reach the best image quality.

■ Iris mode (When the Auto Exposure mode is selected): Select Indoor or Outdoor iris mode to adapt to the installation. The preset iris aperture setting will apply.

You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile of exposure settings page as shown below.

Activated period: Select the mode this profile to apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to for the configuration take effect.

Please follow the steps below to configure a profile:
1. Check **Enable this profile**.
2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.
3. Configure Exposure control settings in the folowing columns. Please refer to previous dicussions for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.
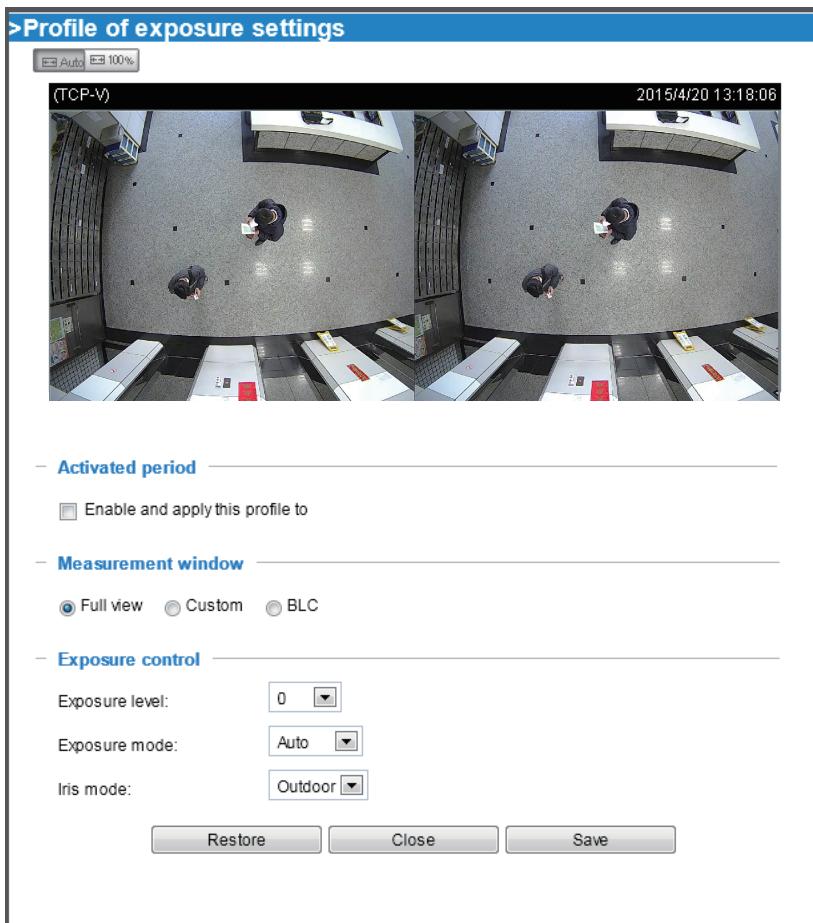
Media > Video

Stream settings
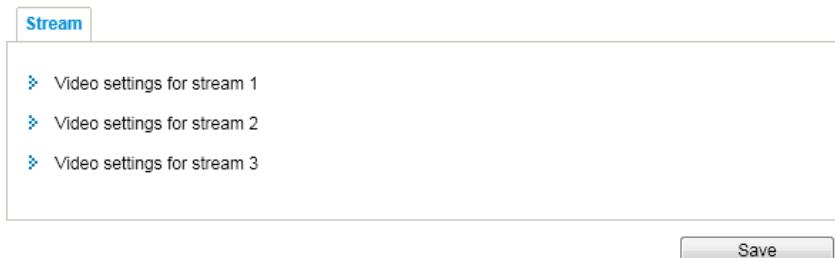
This Network Camera supports multiple streams with frame sizes ranging from 320 x 240 to 2560 x 960 pixels.

The definition of multiple streams:

■ Stream 1: Users can define the frame size, video quality, and frame rate of up to 30fps. The default display mode is the Side by Side mode.

■ Stream 2: The default frame size for Stream 2 is set to a smaller 1280 x 960 size for viewing on mobile devices in the Single Eye mode.

■ Stream 3: The default frame size for Stream 3 is set to a smaller 2560 x 960 size for viewing on mobile devices in the Side by Side mode.

The Depth mode displays the depth measurements via the triangulation correlation of the sum of pixel differences. The 3D values acquired through the images on the dual lens appear in the Depth mode as a color map in that lighter the color of an object, the closer it is to lens.

Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above Viewing Window sections.
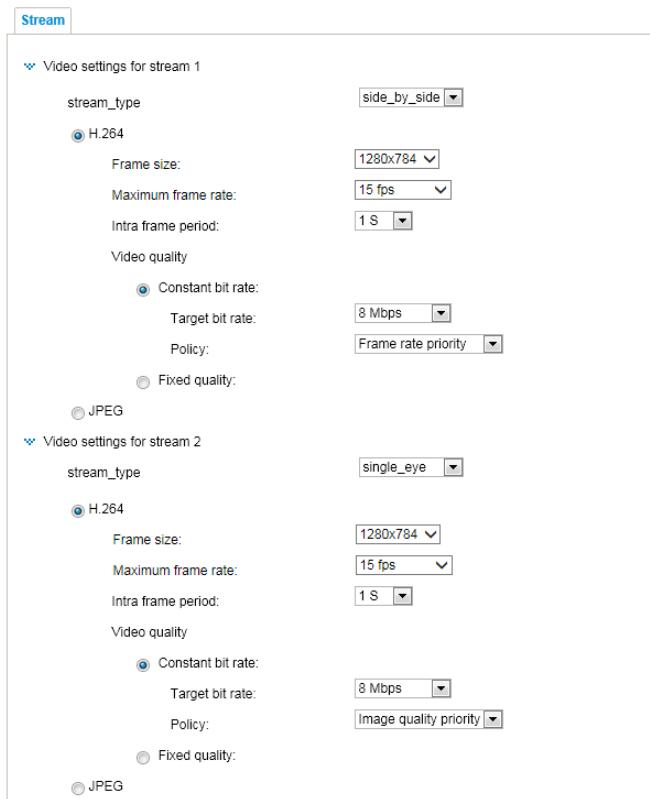
This Network Camera provides real-time H.264 and MJPEG compression standards (Dual Codec) for real-time viewing. If the **H.264** mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance:
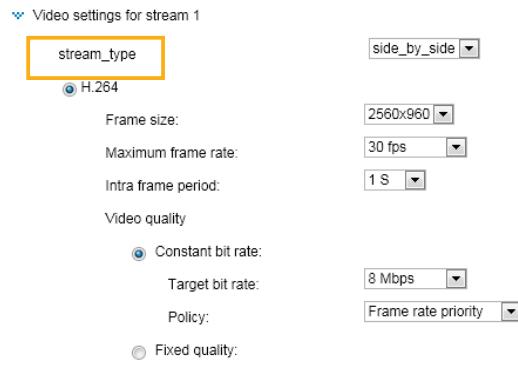
■ Frame size

You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. A higher quality stream can also be recorded to an NVR. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. You can also select **Customize** and manually enter a value.

■ Intra frame period

Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

Constant bit rate:

- Constant bit rate: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8, 12, 14,.. up to 32Mbps. You can also select **Customize** and manually enter a value.

  - Target bit rate: select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 32Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.

  - Policy: If Frame Rate Priority is selected, the Network Camera will try to maintain the frame rate per second performance, while image quality will be compromised. If Image quality priority is selected, the Network Camera may drop some video frames in order to maintain image quality.

- Fixed quality: On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

  - Maximum bit rate: With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps. In low light conditions, lot of noises can be generated and the frame sizes can significantly increase. Placing a bit rate limitation can limit the size of frames.

  You may also manually enter a bit rate number by selecting the **Customized** option.

If the **JPEG** mode is selected, the Network Camera sends consecutive JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:
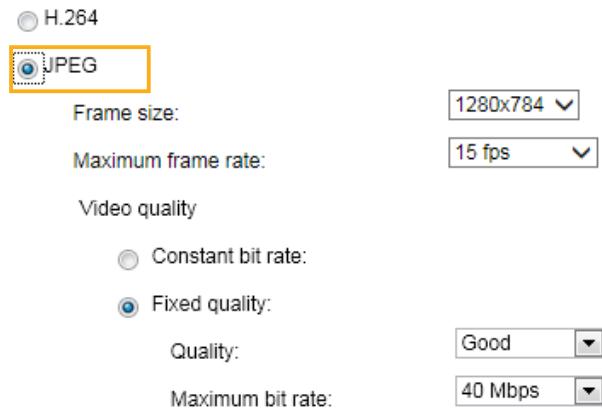
■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Video quality
Refer to the previous page setting an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for the H.264.

For Constant Bit Rate and other settings, refer to the previous page for details.

> ✎ **NOTE:**

► *Video quality and fixed quality refers to the* **compression rate***, so a lower value will produce higher quality.*

► *Converting high-quality video may significantly increase the CPU load, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

Network Type

LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Please rememer to click on the **Save** button when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.

1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 43 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

Primary DNS: The primary domain name server that translates host names into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer names and IP addresses.

Secondary WINS server: The secondary WINS server that maintains the database of computer names and IP addresses.

PPPoE (Point-to-point over Ethernet)
Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.
1. Set up the Network Camera on the LAN.
2. Go to Stereo Tracker > Configurations > Event settings > Add server (please refer to Add server on page104) to add a new email or FTP server.
3. Go to Stereo Tracker > Configurations > Event settings > Add media (please refer to Add media on page 108).
   Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

```
┌─ Network type ──────────────────────────────────┐
│                                                  │
│  ○ LAN                                           │
│  ◉ PPPoE                                          │
│       User name:        [_____]       │
│       Password:         [_____]       │
│       Confirm password: [_____]       │
│  ☐ Enable IPv6                                    │
│                                                  │
└──────────────────────────────────────────────────┘
                                    [  Save  ]
```

5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

📝 **NOTE:**

► If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.

► If UPnP^{TM} is not supported by your router, you will see the following message:
Error: Router does not support UPnP port forwarding.

► Steps to enable the UPnP^{TM} user interface on your computer:
Note that you must log on to the computer as a system administrator to install the UPnP^{TM} components.

1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.
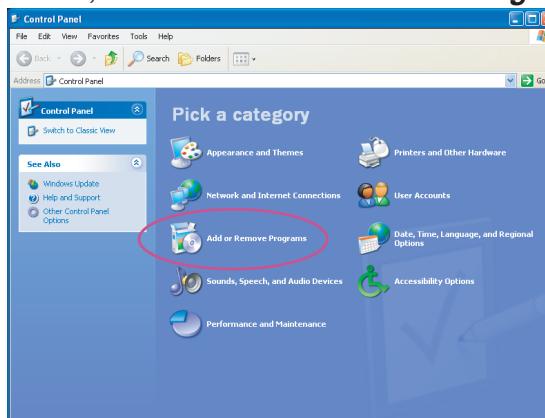
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.
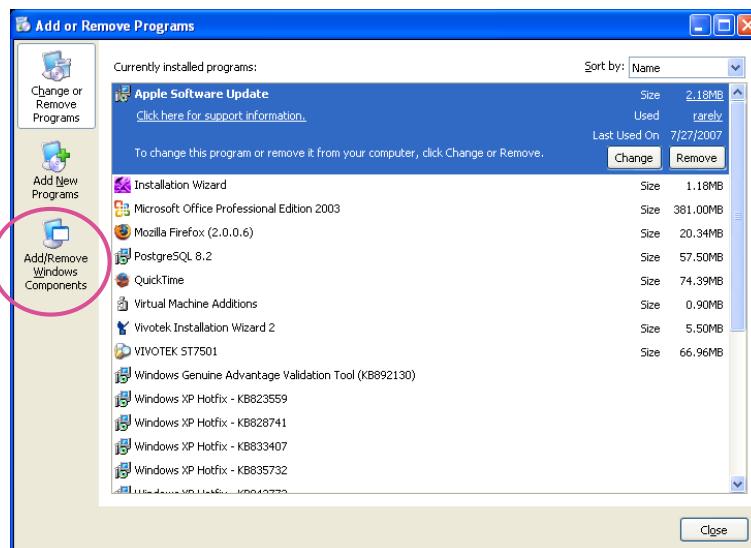
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.
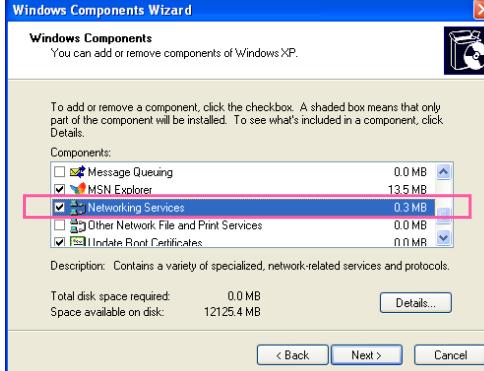
4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.
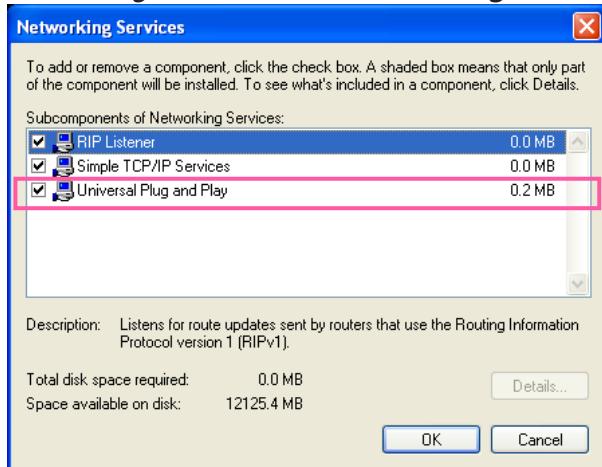
5. Click **Next** in the following window.
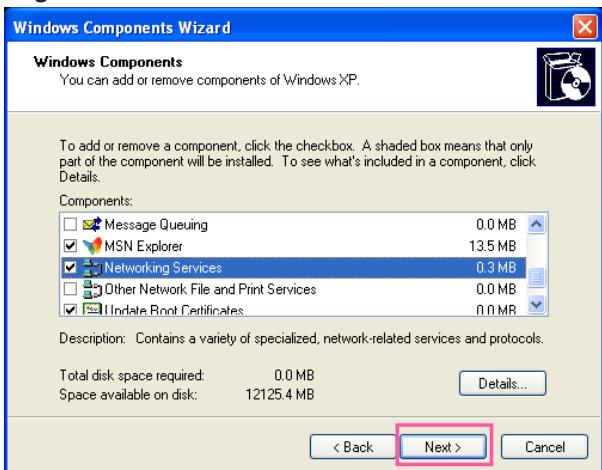
6. Click **Finish**. UPnP^{TM} is enabled.

► How does UPnP^{TM} work?
  UPnP^{TM} networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

► Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 148 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.

Enable IPv6

Select this option and click **Save** to enable IPv6 settings.

Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.
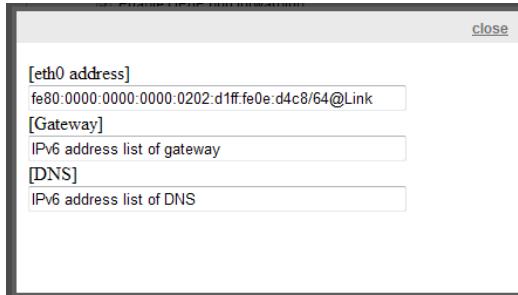
If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

Refers to Ethernet

[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global — Link-global IPv6 address/network mask

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link — Link-local IPv6 address/network mask

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

http://**[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]**/

↑

IPv6 address

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:
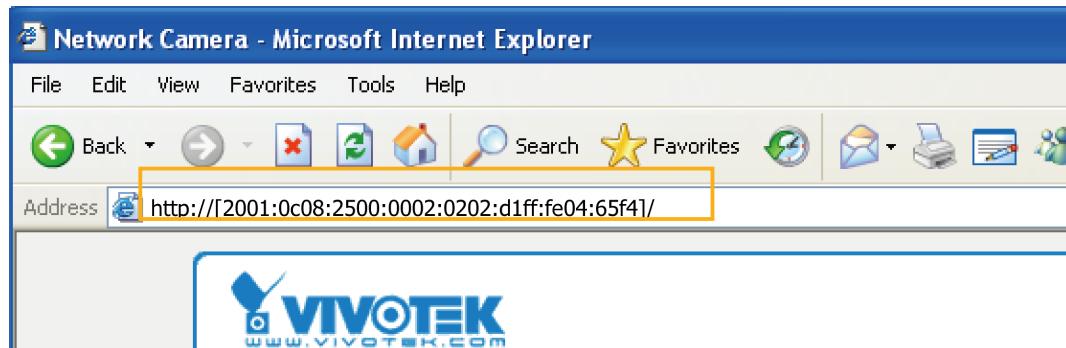
 NOTE:

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to* **HTTP** *streaming on page 168 for detailed information.)*

http://**[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]**/:8080

↑   ↑

IPv6 address   Secondary HTTP port

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*

[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/64@Link
[ppp0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299/10@Link
2001:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global
[Gateway]
fe80::90:1a00:4142:8ced
[DNS]
2001:b000::1

Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:

☑ Enable IPv6

IPv6 information

☑ Manually setup the IP address

Optional IP address / Prefix length [   ] / 64

Optional default router [   ]

Optional primary DNS [   ]

Port

Network type	Port

HTTPS port: 443

FTP port: 21

Websocket port: 777

[Save]

HTTPS port: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

FTP port: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

Websocket port: The Websocket enables two-way communications between browser-based applications with servers that does not rely on opening multiple HTTP connections, in order to avoid long polling. The protocol consists of an opening handshake followed by basic message framing, layered over TCP. The protocol provides an alternative to HTTP polling from a web page to a remote server.

For a management session across a firewall or router (over the Internet), it is necessary to open a **Websocket port 888** on your router using the NAT traversal method for transferring metadata for counting. The default Websocket port is also user configurable.

Network > Streaming protocols

HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 178 for details.

Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:
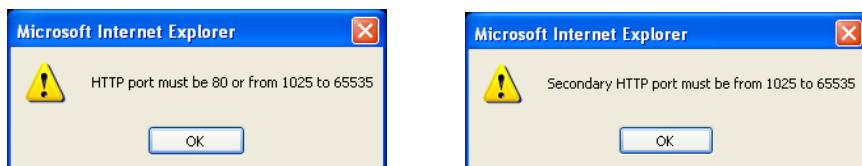
To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

On the LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream #: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 159.

When using **Mozilla Firefox** to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream #>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.
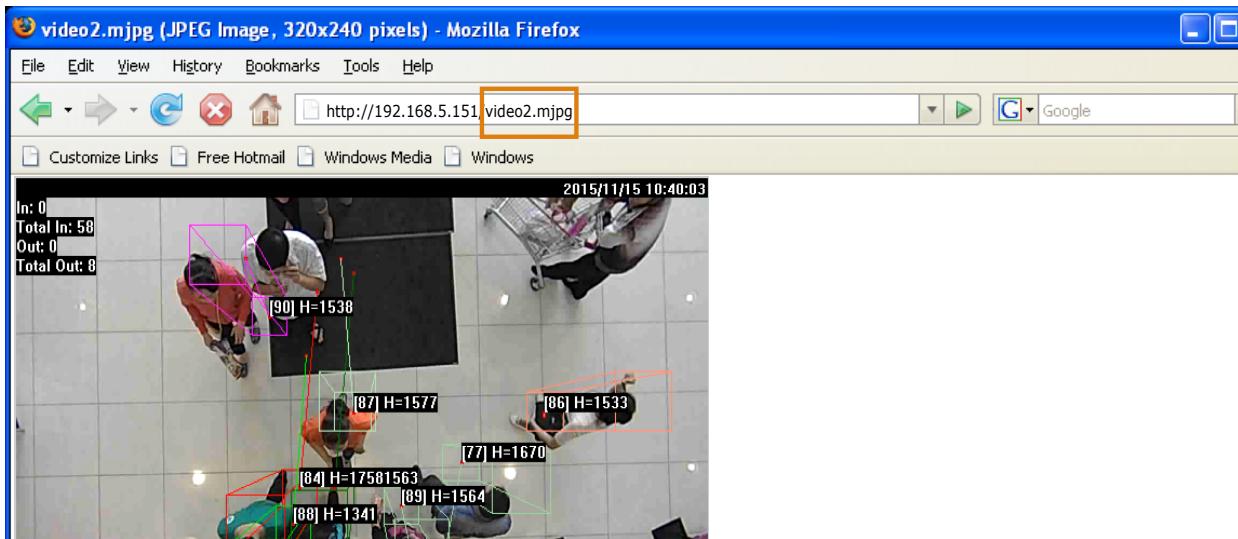
📝 **NOTE:**

► Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 or 2> will fail to access the Network Camera.

► Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 207.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 178 for details.

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed below:

	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream #: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream #>

For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.
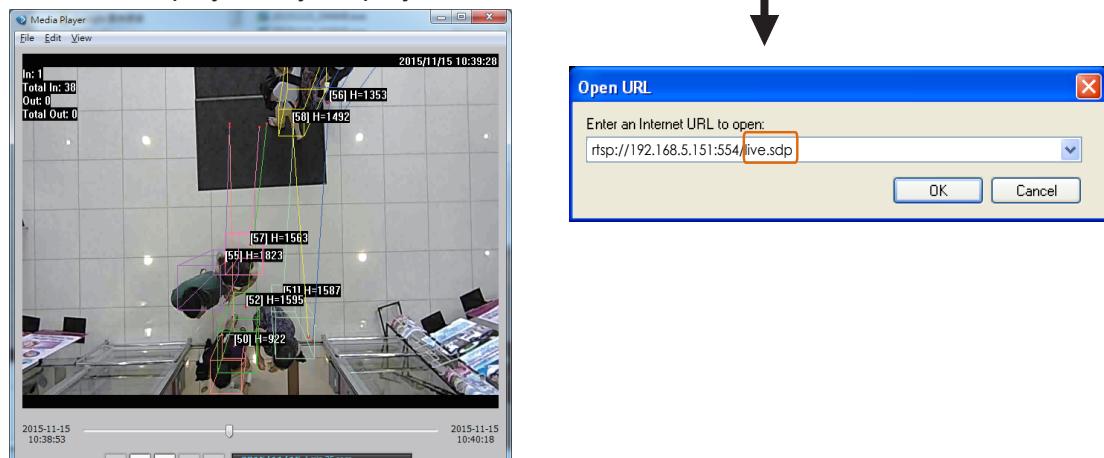
RTSP port /RTP port for video, audio/ RTCP port for video, audio
■ RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

■ The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

■ The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:
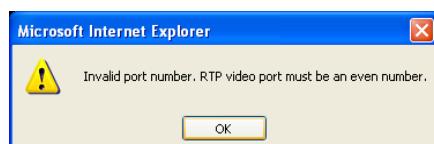
Multicast settings for stream 1, 2: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 or 2.

```
Multicast settings for stream 1:
    Always multicast
    Multicast group address:        239.128.1.99
    Multicast video port:           5560
    Multicast RTCP video port:      5561
    Multicast audio port:           5562
    Multicast RTCP audio port:      5563
    Multicast TTL [1~255]:          15

Multicast settings for stream 2:
    Always multicast
    Multicast group address:        239.128.1.100
    Multicast video port:           5564
    Multicast RTCP video port:      5565
    Multicast audio port:           5566
    Multicast RTCP audio port:      5567
    Multicast TTL [1~255]:          15
```

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:

```
Microsoft Internet Explorer                        [X]

    ⚠    Invalid port number. Multicast stream 1 video port must be an even number.

                    [   OK   ]
```
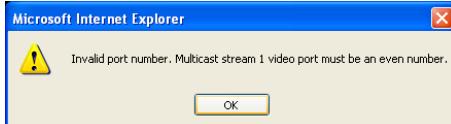
Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

Network > DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.
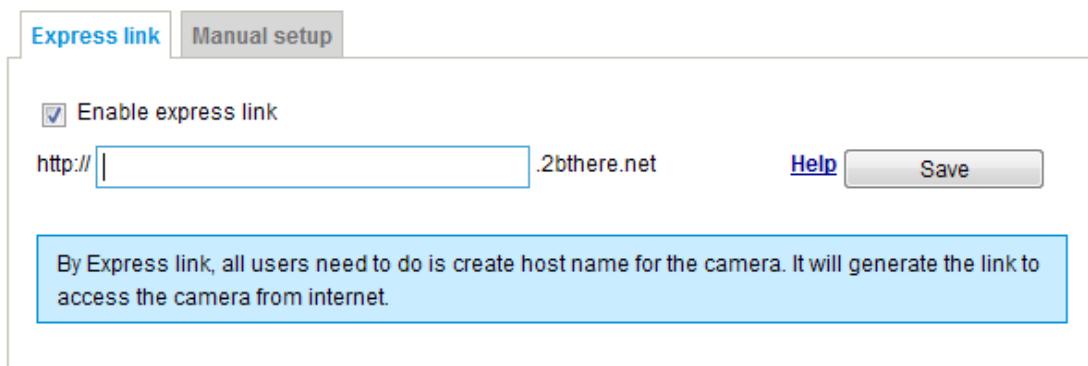
Please follow the steps below to enable Express Link:
1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will display a message as shown below.
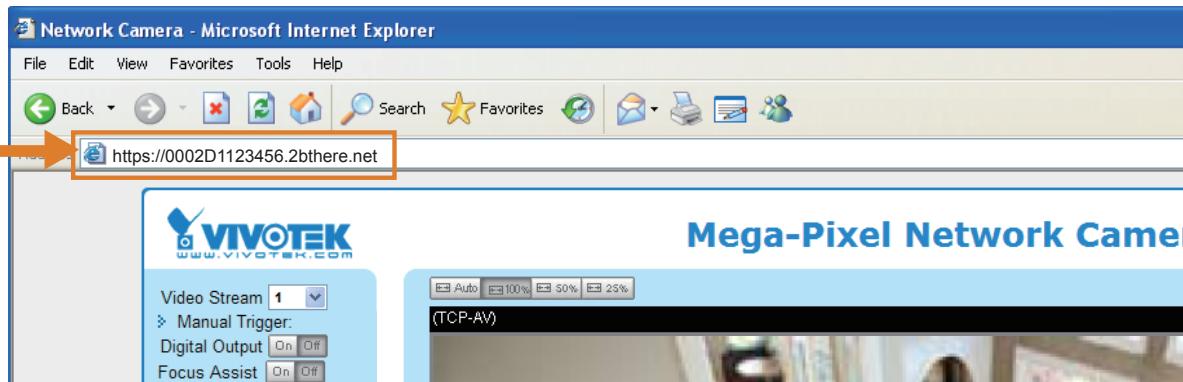
Manual setup

DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns. org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net
1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > QoS (Quality of Service)

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
■ The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
■ The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:
■ All network switches and routers in the network must include support for QoS.
■ The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

If you assign Video the highest level, the switch will handle video packets first.

> 📝 **NOTE:**
>
> ► A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.
>
> ► Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.
>
> ► Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

Network > SNMP (Simple Network Management Protocol)

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

■ Encryption password: Enter a password for encryption (at least 8 characters).

Security > User accounts

This section explains how to enable password protection and create multiple accounts.

Root Password

The administrator account name is "root", which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the "root" account first.
1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user's name and password in their respective fields to access the Network Camera.

Privilege Management
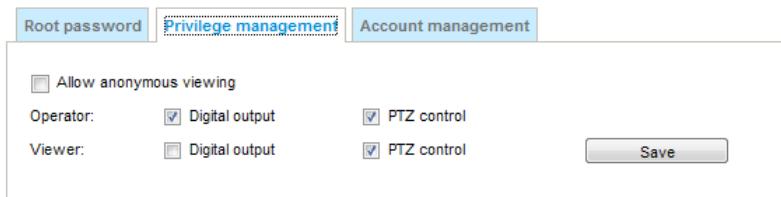
<u>Digital Output & PTZ control</u>: You can modify the management privilege for operators or viewers. Select or deselect the checkboxes, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 138).

<u>Allow anonymous viewing</u>: If you check this item, any client can access the live stream without entering a User ID and Password.

Account Management
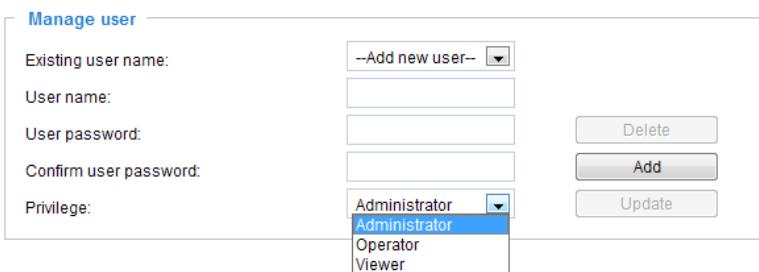
Administrators can create up to 20 user accounts.
1. Input the new user's name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Although operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 207. Viewers can only access the main page for live viewing.

Here you also can change a user's access rights or delete user accounts.
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL)

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate

1. Select this option from a pull-down menu.
2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Create certificate** to generate a certificate.

4. The Certificate Information will automatically be displayed as shown below. You can click **Certificate properties** to view detailed information about the certificate.

5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.

6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.
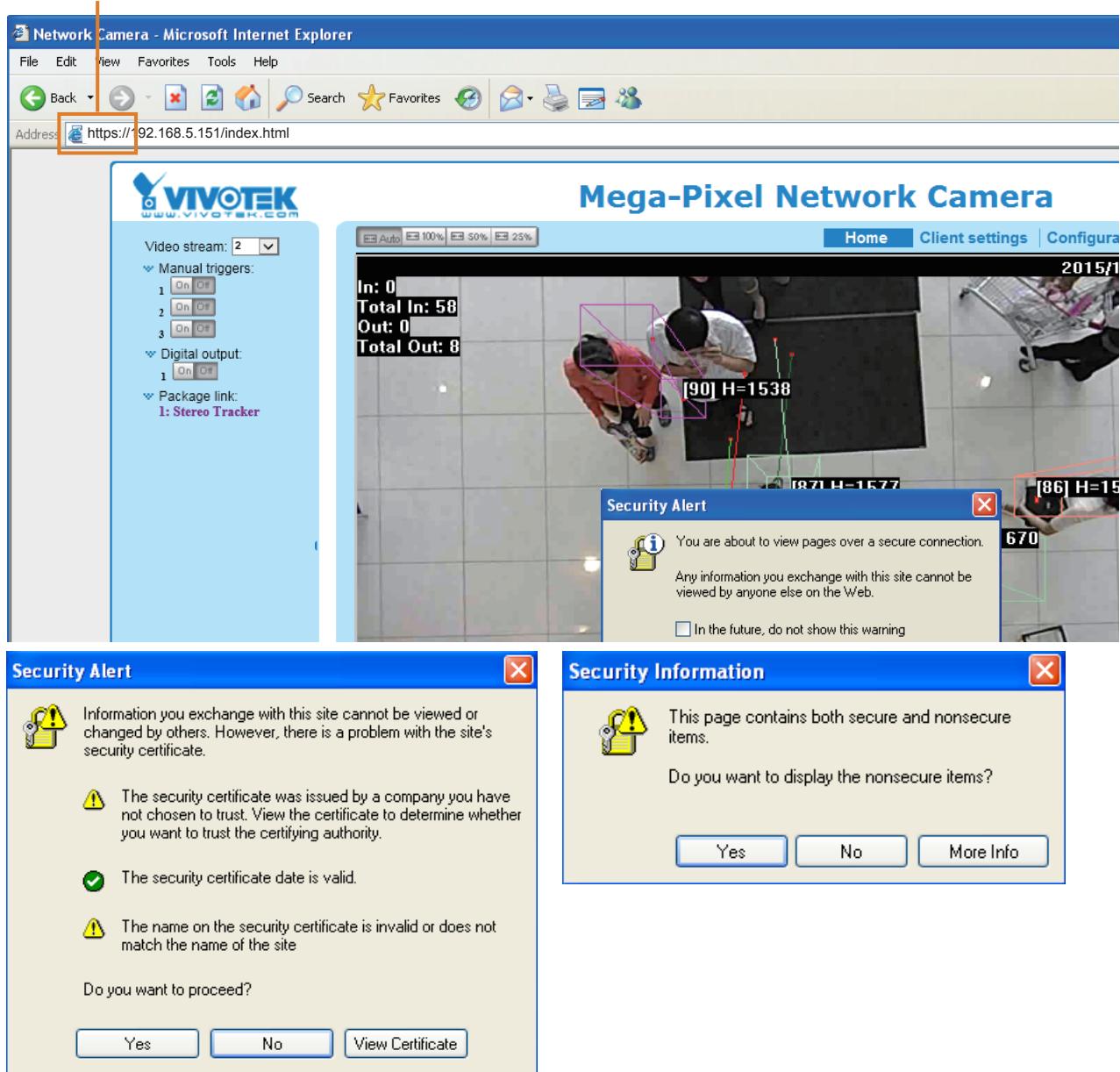
Create certificate request and install

1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.
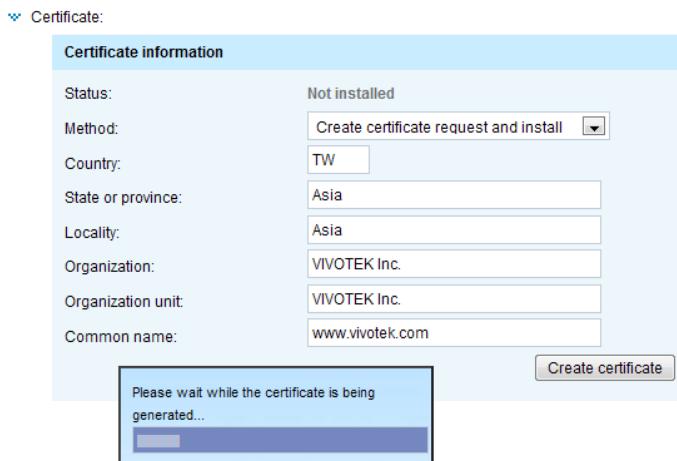
4. The Certificate request window will prompt.
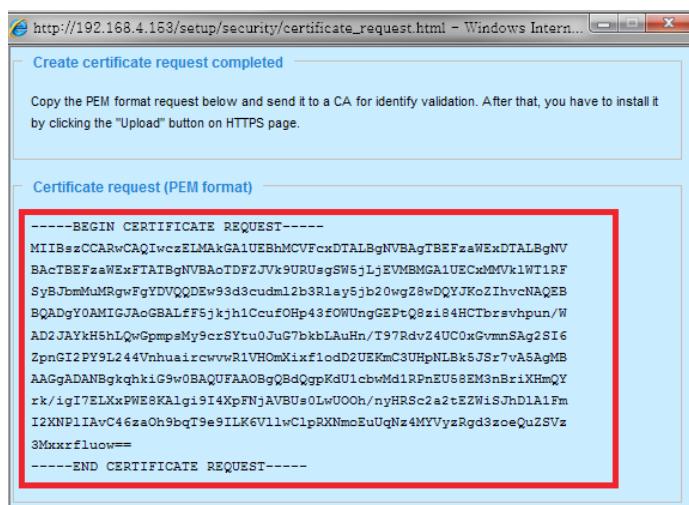
If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.
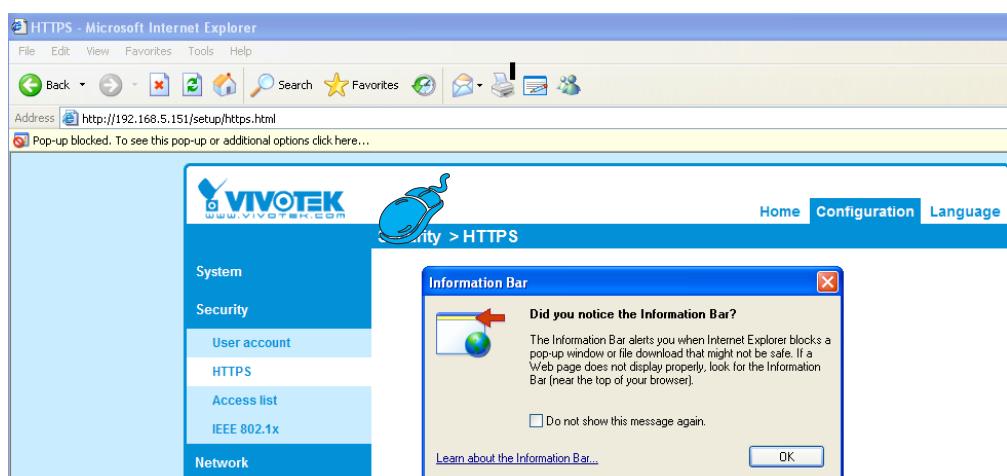
5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.
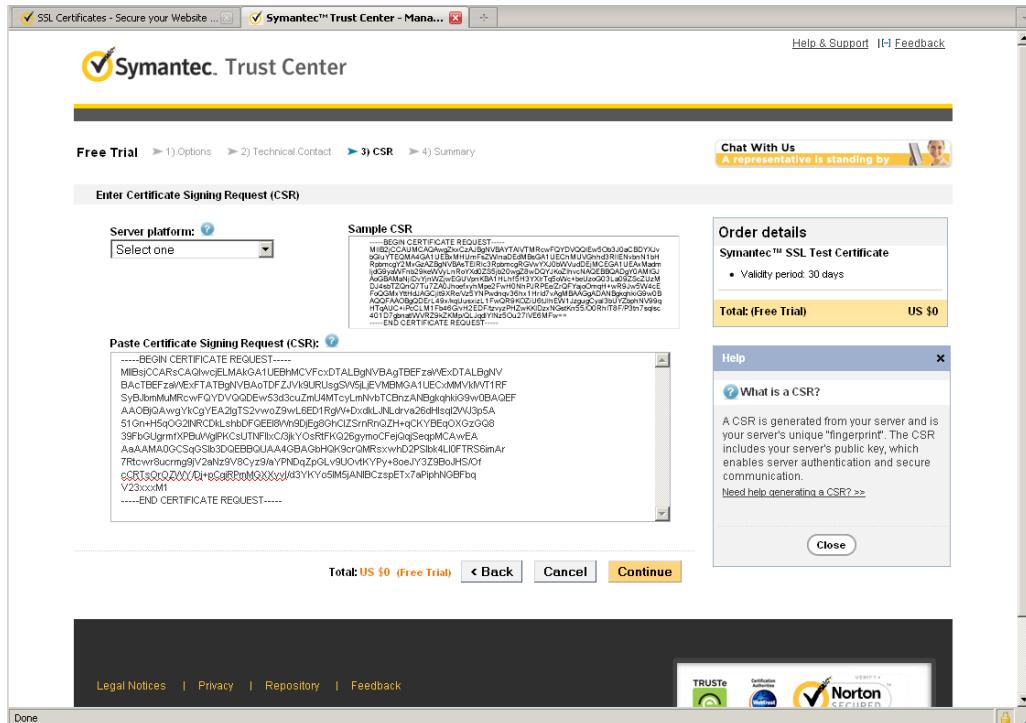
6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.
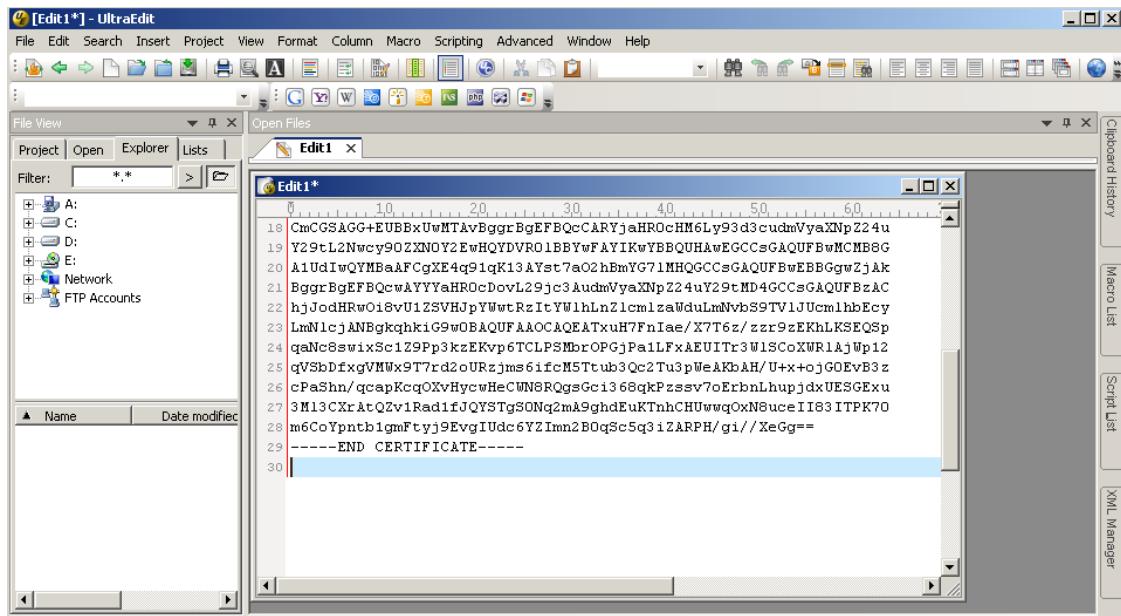
8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.
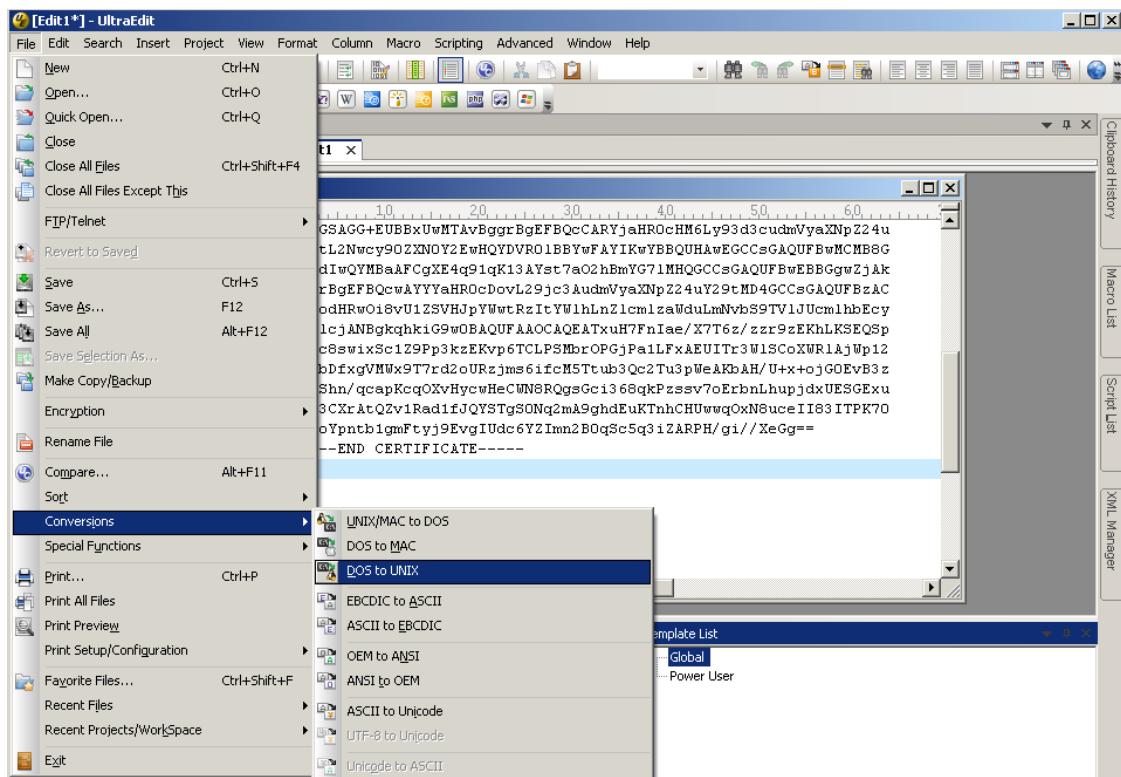
9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."
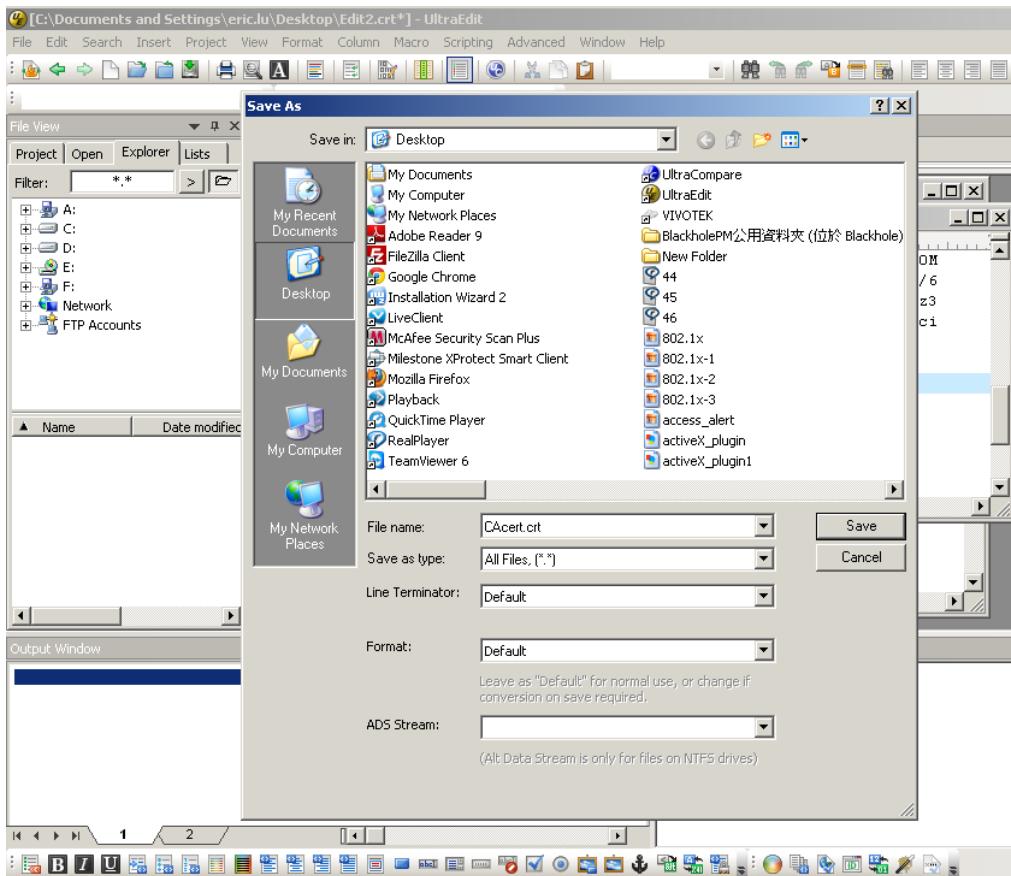
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.
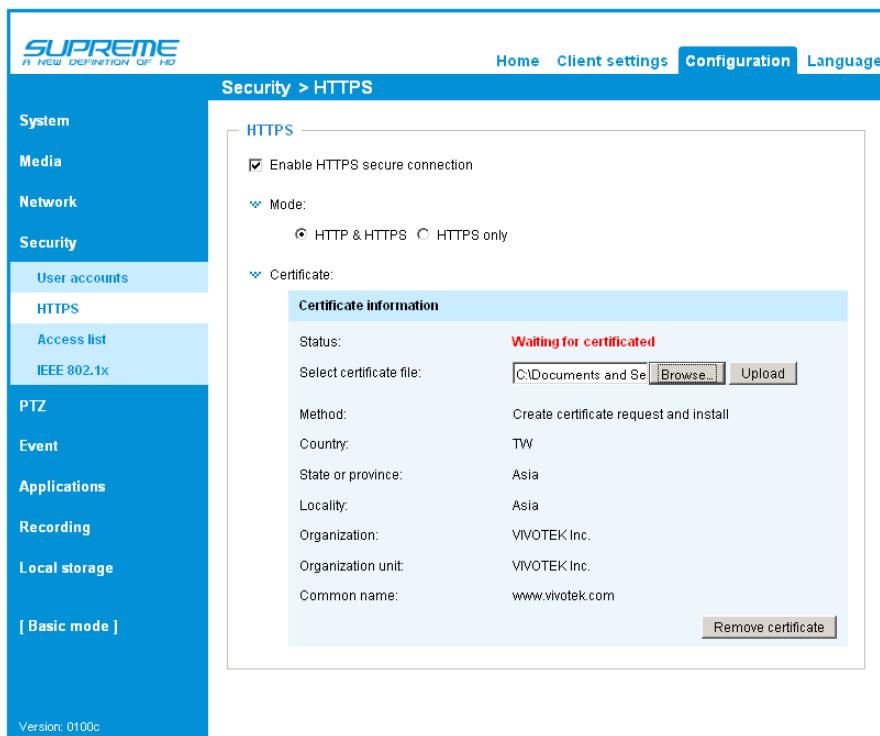
11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the "Save" button for the configuration to take effect.
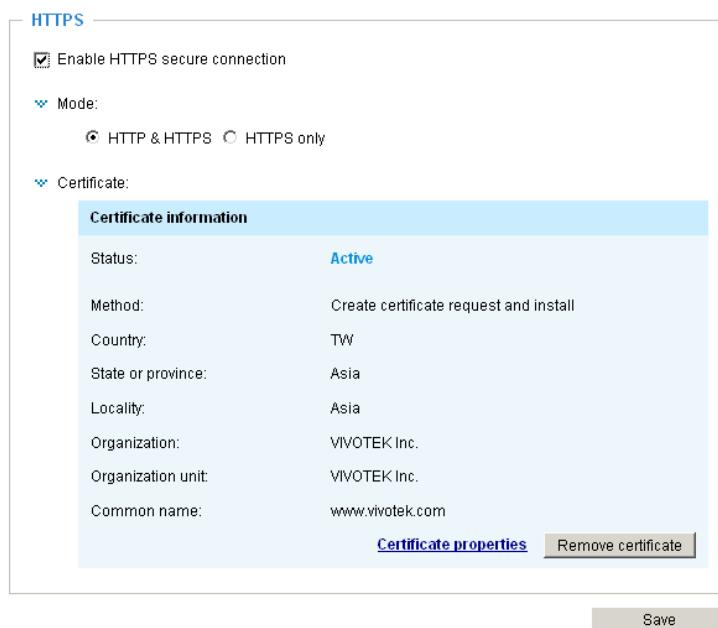
12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.
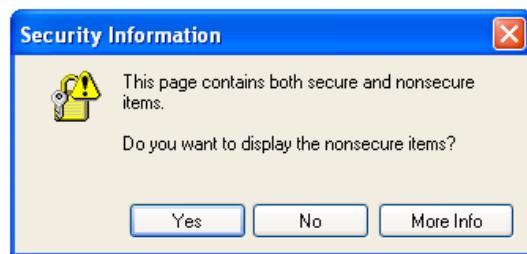
Security > Access List

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

General settings

Maximum number of concurrent streaming: 10   Connection management

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including all video streams). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explorer or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections. For example:

	IP address	Elapsed time	User ID
☐	172.16.2.53	00:00:05	
☐	192.168.4.104	01:49:35	

Refresh   Add to deny list   Disconnect   Close

Note that only consoles that are currently displaying live streaming will be listed in the View Information list.

■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations that allow clients access to the live video without a user name and password:
1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 178.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 169.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 178.

■ Refresh: Click this button to refresh all current connections.

■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

Filter

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can.

Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > General settings on page 161 for detailed information.

There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format.
For example:

IP address range 192.168.2.x will be bolcked.

If IPv6 filter is preferred, you will be prompted by the following window. Enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule only applies to IPv4 addresses.
For example:

Administrator IP address
Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Security > IEEE 802.1X

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

Authentication Server
(RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user's access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:
1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., your network administrator) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

📝 **NOTE:**

► The authentication process for 802.1x:

1. The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).
2. A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.
3. The switch also forwards the RADIUS Server's certificate to the Network Camera.
4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.
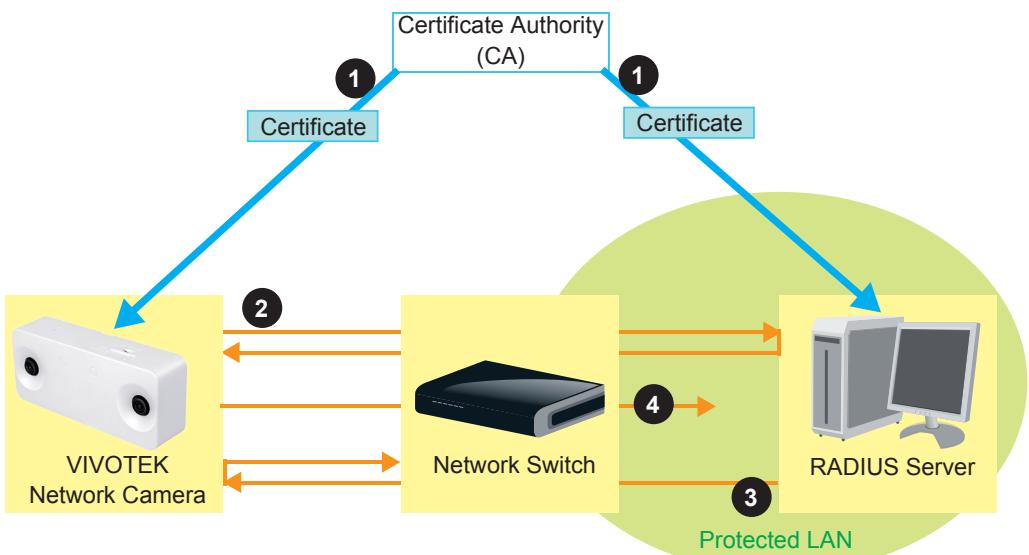
Applications > DI and DO

Digital input

Normal status:	⦿ High ◯ Low
Current status:	**High**

Digital output

Normal status:	⦿ Open ◯ Grounded
Current status:	**Open**

Save

Connect DI or DO devices to the camera's terminal block, the camera will automatically detect the current connection state as pulled-high or pulled-low. You may then define the triggering condition.

Digital input: Select High or Low as the state of the signal to define the "Normal status" for the digital input. Connect the digital input lines to the Network Camera, and the camera will report the current status.

Digital output: Select Grounded or Open as the state of the signal to define the "Normal status" for the digital output. Connect the digital output lines to the Network Camera, and the camera will display the current status.

Package management
(VADP, VIVOTEK Application Development Platform)

Users can store and execute VIVOTEK's or 3rd-party software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting/tracking, or as an agent for edge recording, etc.

- Once the software package is successfully uploaded, the module configuration (vadp. xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined VADP requirements. Please contact technical support or the vendor of your 3rd-party package for the parameters contained within.

- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.

- Note that for some cameras the flash is too small to hold VADP packages. These cameras will have its "Save to SD card" checkbox selected and grayed-out for all time.

- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:
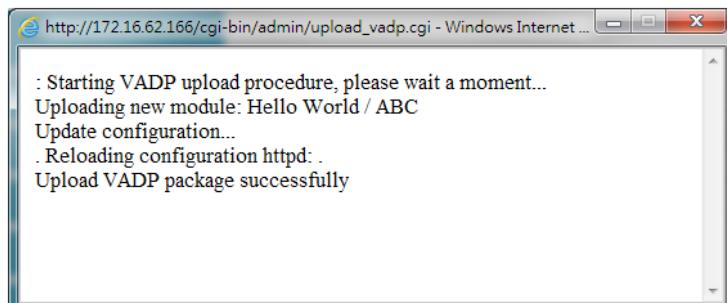
To start a module, select the checkcircle in front, and click the **Start** button.

If you should need to remove a module, select the checkcircle in front and then click the **Stop** button. By then the module status will become **OFF**, and the **X** button will appear at the end of the row. Click on the **X** button to remove an existing module.

When prompted by a confirm message, Click **Yes** to proceed.
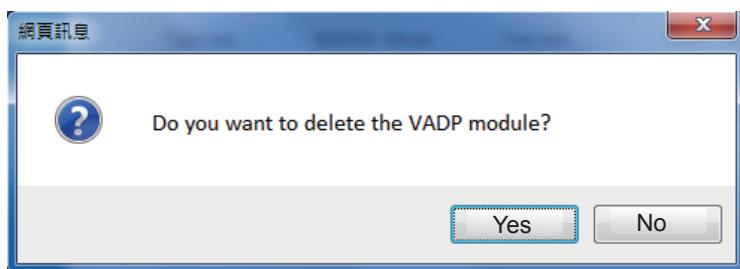
Note that the actual memory consumed while operating the module will be indicated on the **Memory status** field. This helps determine whether a running module has consumed too much of system resources.

Online Registration

Software package may require a license key. Follow the below procedure for applying a license key.

Already a VVTK member
- or -
login to VVTK website
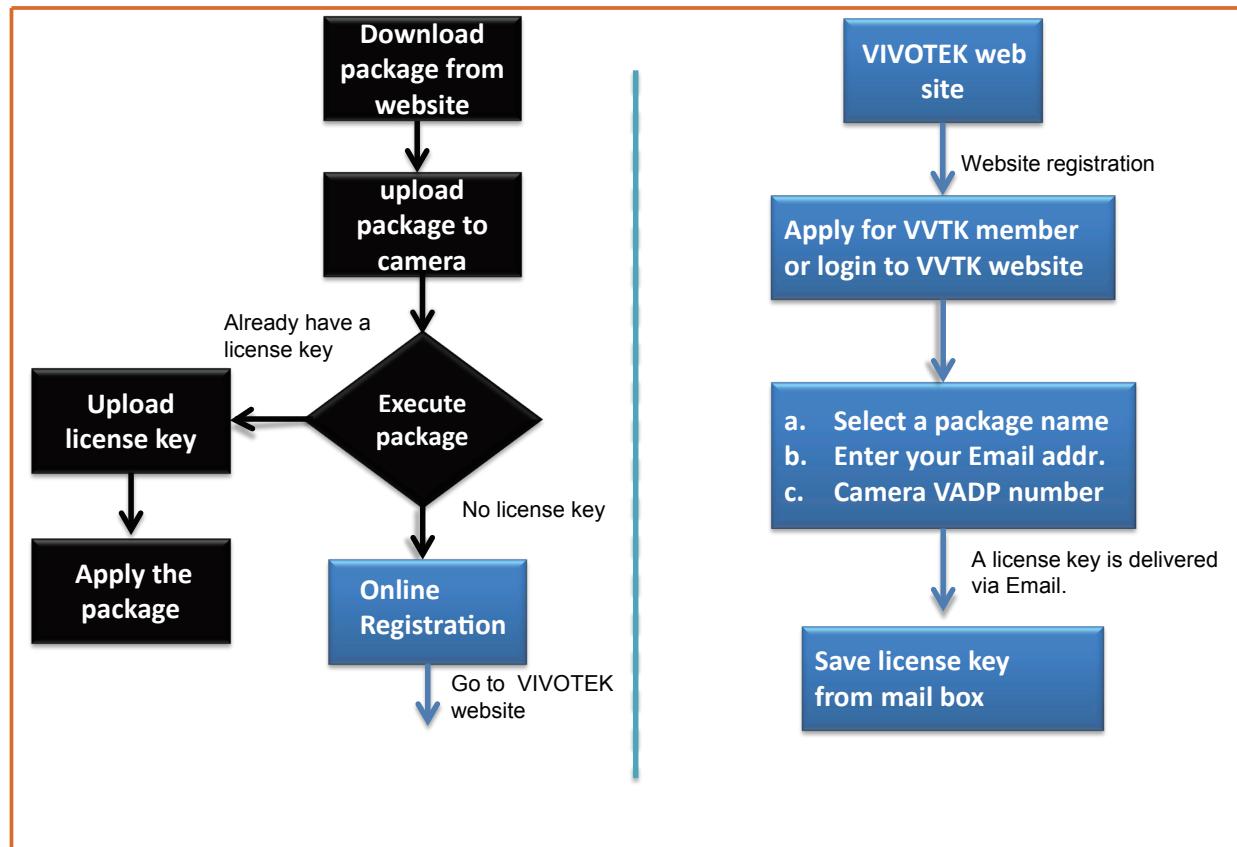
On the License page, use the Manual or Automatic option to register and activate the license for using VIVOTEK's VADP modules. The Automatic method requires an Internet connection.
Without Internet connection, you should acquire the license key elsewhere, and manually upload to the network camera.

Follow the onscreen instruction on VIVOTEK's website for the registration procedure.

Status	License

Manual License

To receive a license key for VADP application, go to **http://www.vivotek.com** and join the VVTK member. This device's VADP number is:

`BbM79RE=OdGu1PIUEqJRFgc6sacoRs7g4PX(`

Select file   [Browse···] No file selected.   [Upload]

Stereo Tracker - the Embedded VADP Module

📝 **NOTE:**

- Refer to page 43 for the contents of Stereo Tracking and Counting configuration.
- The Event trigger and DI/DO configuration can also be accessed from the Stereo Tracker configuration pages.

Recording > Recording settings

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

Insert your SD card and click here to test

NOTE:

► Please remember to format your SD card via the camera's web console (in the Local storage . SD card management page) when using it for the first time. Please refer to page 202 for detailed information.

Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:

Select this option will activate the frame rate control according to alarm trigger.
The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've configured on the Video quality page. Please refer to page 159 for more information.

If you enable adaptive recording and enable time-shift cache stream on Camera A, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidth and storage space.
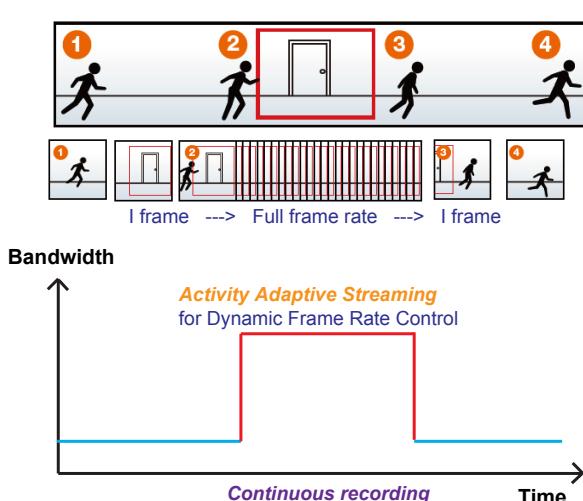
NOTE:

► To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.

► When there is no alarm trigger:
   - JPEG mode: record 1 frame per second.
   - H.264 mode: record I frame only.

► When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.

The alarm trigger includes: motion detection and DI detection. Please refer to Event Settings on page 198.

■ Pre-event recording and post-event recording
   The Network Camera has a buffer that temporarily holds data up to a certain limit. Enter a number to define the duration of recording before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

■ Source: Select a video stream as the recording source.

NOTE:

► To enable recording notification please configure **Event settings** first . Please refer to page 198.

Please follow the steps below to set up the recording.

1. Trigger
 Select a trigger source.

■ Schedule: The server will start to record files on the local storage or a networked attached storage (NAS).

■ Network fail: Since network fail, the server will start to record files on the local storage (SD card).

2. Destination

You can select the SD card or network attached storage (NAS) for the recorded video files. If you have not configured a NAS storage, see details in the following.
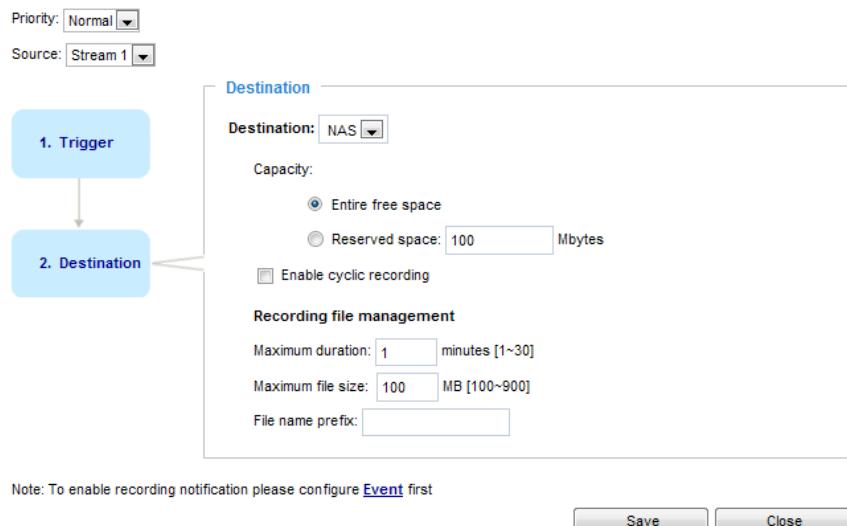
NAS server

Click **Add NAS server** to open the server setting window and follow the steps below to set up:
1. Fill in the information for your server.
   For example:
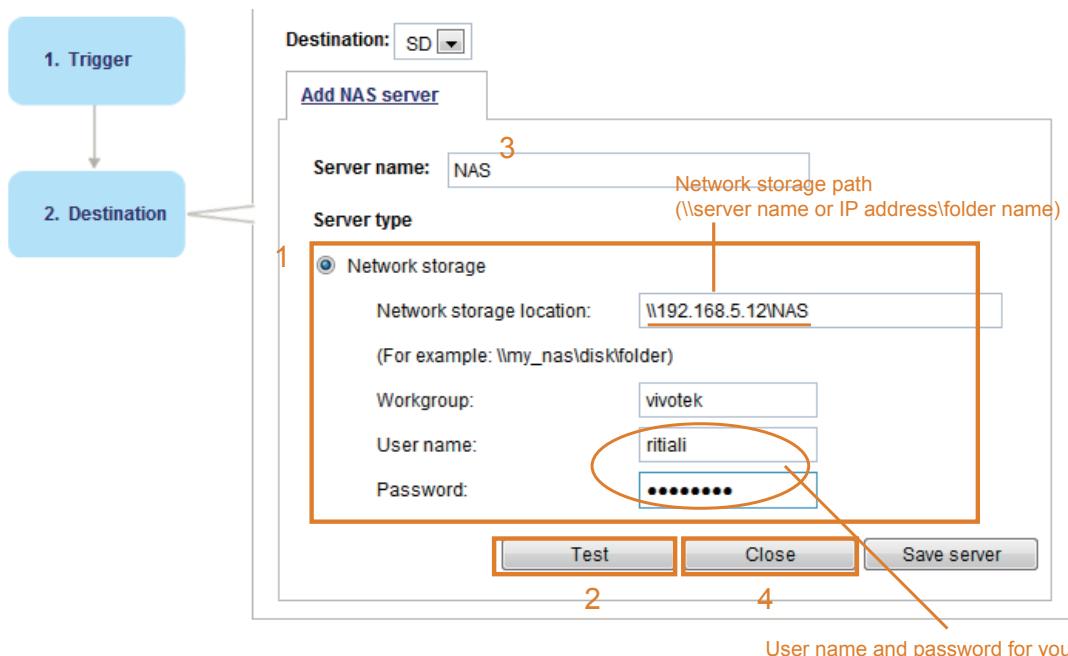
2. Click **Test** to check the setting. The result will be shown in the pop-up window.
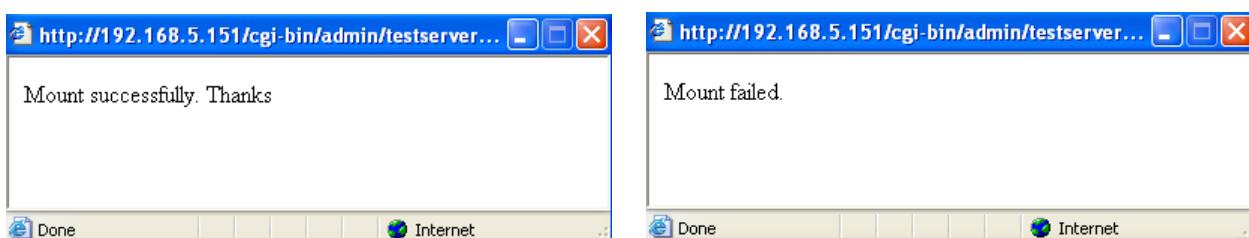
If successful, you will receive a test.txt file on the network storage server.
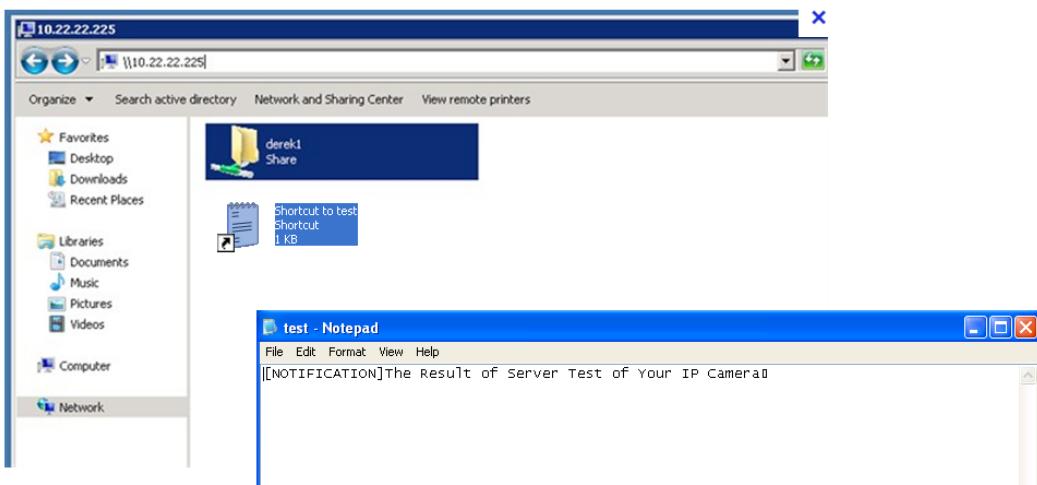
3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.
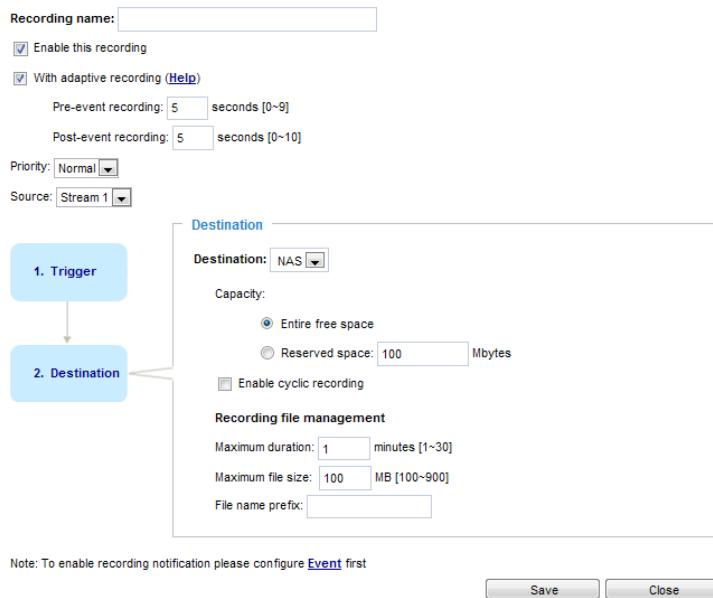
■ Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

■ Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MegaBytes.

■ Recording file management: You can manually assign the Maximum duration and the Maximum file size for each recording footage. You may need to stitch individual files together under some circumstances. You may also designate a file name prefix by filling in the responsive text field.

■ File name prefix: Enter the text that will be appended to the front of the file name.

If you want to enable recording notification, please click *__Event__* to configure event triggering settings. Please refer to Stereo Tracker > Configurations > Event settings on page 100 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.

- ■ Click __recording__ **(Name)**: Opens the Recording Settings page to modify.
- ■ Click __ON__ **(Status)**: The Status will become __OFF__ and stop recording.
- ■ Click __NAS__ **(Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 111 for details.

Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

> 📝 **NOTE:**
>
> - The latest firmware release supports mod.sdp that supports the playback of video recorded in the SD card. The playback speed is configurable [playspeed=n, n=(0.1~10.0)]. The default speed is 1. Please refer to the URL command for more information.

SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.

SD card format

The Linux kernel EXT4 file system format applies to SD card larger than 32GB. However, if EXT4 is applied, the computers running Windows will not be able to access the contents on the SD card.

SD card control

- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter "7 days", the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** column.

■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search for contents created at a specific point in time.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

✎ NOTE:

- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera filesystem takes up several megabytes of memory space. The storage space cannot be used for recording.
- Using an SD card that already contains data recorded by another device should not be used in this camera.
- Please do not modify or change the folder names in the SD card. That may result in camera malfunctions.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ◆ to sort the search results in either direction.

Numbers of entries displayed on one page

Enter a key word to filter the search results

Highlight an item

■ View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file. For example:
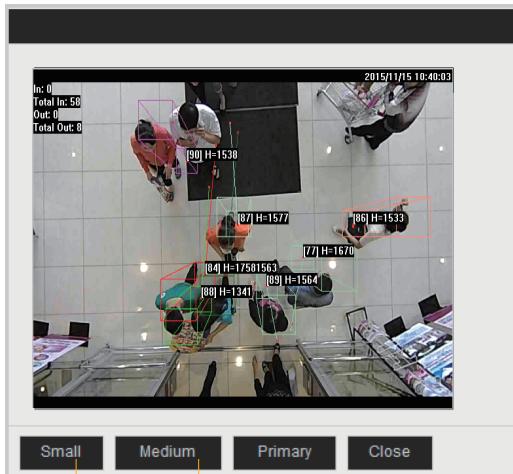
Click to adjust the image size

■ Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

■ JPEGs to AVI: This functions only applies to "JPEG" format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

■ Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections. For example:

■ Remove: Select the desired search results, then click this button to delete the files.

Appendix

URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

http://<servername>/cgi-bin/viewer/video.jpg

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

HTTP/1.0 <HTTP code> <HTTP text>\r\n

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

http://mywebserver/cgi-bin/viewer/video.jpg

3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://*<servername>*/cgi-bin/*<subdir>*[/*<subdir>*...]/*<cgi>*.*<ext>*
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, videoin	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/anonymous/getparam.cgi?[*<parameter>*]

[&<parameter>…]

http://*<servername>*/cgi-bin/viewer/getparam.cgi?[*<parameter>*]

[&<parameter>…]

http://*<servername>*/cgi-bin/operator/getparam.cgi?[*<parameter>*]

[&<parameter>…]

http://*<servername>*/cgi-bin/admin/getparam.cgi?[*<parameter>*]

[&<parameter>…]

Where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: <length>\r\n

\r\n

<parameter pair>

where <parameter pair> is

=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:

http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/anonymous/setparam.cgi? *<parameter>=<value>*

[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://*<servername>*/cgi-bin/viewer/setparam.cgi? *<parameter>=<value>*

[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://*<servername>*/cgi-bin/operator/setparam.cgi? *<parameter>=<value>*

[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://*<servername>*/cgi-bin/admin/setparam.cgi? *<parameter>=<value>*

[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>_<name>.*
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be

		placed at the end of the parameter list

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>

where <parameter pair> is

=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

7. Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[64]	SC8131	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	\<boolean\>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	\<YYYY/MM/DD\>, keep, auto	\<current date\>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	\<hh:mm:ss\>, keep, auto	\<current time\>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	\<MMDDhhmmYYYY.ss\>	\<blank\>	7/6	Another current time format of the system.
ntp	string[40]	au.pool.ntp.org	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America,

				Central Time, Mexico City, Saskatchewan
				-200: GMT-05:00 Eastern Time, New York, Toronto
				-201: GMT-05:00 Bogota, Lima, Quito, Indiana
				-180: GMT-04:30 Caracas
				-160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago
				-140: GMT-03:30 Newfoundland
				-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland
				-80: GMT-02:00 Mid-Atlantic
				-40: GMT-01:00 Azores, Cape_Verde_IS.
				0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
				40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris
				41: GMT 01:00 Warsaw, Budapest, Bern
				80: GMT 02:00 Athens, Helsinki, Istanbul, Riga
				81: GMT 02:00 Cairo
				82: GMT 02:00 Lebanon, Minsk
				83: GMT 02:00 Israel
				120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi
				121: GMT 03:00 Iraq
				140: GMT 03:30 Tehran
				160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan
				180: GMT 04:30 Kabul
				200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent

				220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	1~4 <positive integer>	1	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120, -80,-40,0, 40,41,80, 81,82,83, 120,140,	6/6	List time zone index which support daylight saving time.

		380,400,48 0		
updateinterval	0, 3600, 86400, 604800, 2592000	86400	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	<Any Value>	N/A	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

restoreexceptvadp	<Any Value>	N/A	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	SC8131	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	SC8131	0/7	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<product dependent>	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	<product dependent>	0/7	Available language lists.
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	<blank>	0/6	Custom language name.

7.1.2 system.location

Subgroup of **system**: **location**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
groupid	string[256]	0	1/6	Location information: Group id of this camera
deviceid	string[256]	0	1/6	Location information: Device id of this camera

7.1.3 system.mvaas

Subgroup of **system**: **mvaas**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
registerserver_address	string[256]	127.0.0.1	1/6	Remote management register server address
registerserver_port	443,1025~ 65535	443	1/6	Remote management register server port
logserver_address	string[256]	127.0.0.1	1/6	Remote management log server address
logserver_port	443,1025~ 65535	8833	1/6	Remote management log server port

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)> <product dependent>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)> <product dependent>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
onlinenum_rtsp	integer	0	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP push server connections.
eth_i0	<string>	<product dependent>	1/7	Get network information from mii-tool.
vi_i<0~(nvi-1)> <product dependent>	<boolean>	0	1/7	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: security

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do <product dependent>	view, operator, admin	operator	1/6	Indicate which privileges and above can control digital output (capability.ndo > 0)
privilege_camctrl <product dependent>	view, operator, admin	view	1/6	Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i1_name	string[64]	vivotekmvaas	6/7	User name of remote management server
user_i<2~20>_name	string[64]	<blank>	6/7	User name
user_i0_pass	password[64]	<blank>	6/6	Root password
user_i1_pass	password[64]	<blank>	6/6	Remote management server password
user_i<2~20>_pass	password[64]	<blank>	7/6	User password
user_i0_privilege	view, operator, admin	admin	6/7	Root privilege
user_i1_privilege	view, operator, admin	admin	6/7	Remote management server privilege
user_i<2~20>_ privilege	view, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	<blank>	6/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556& network_rtp_videoport=20480"
type	lan, pppoe <product dependent>	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	<product dependent>	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.

dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	eap-peap	6/6	Selected EAP method
identity_peap	String[64]	<blank>	6/6	PEAP identity
identity_tls	String[64]	<blank>	6/6	TLS identity
password	String[253]	<blank>	6/6	Password for TLS
privatekeypassword	String[253]	<blank>	6/6	Password for PEAP
ca_exist	<boolean>	0	6/6	CA installed flag
ca_time	String[20]	0	6/7	CA installed time. Represented in EPOCH
ca_size	String[20]	0	6/7	CA file size (in bytes)
certificate_exist	<boolean>	0	6/6	Certificate installed flag (for TLS)
certificate_time	String[20]	0	6/7	Certificate installed time. Represented in EPOCH
certificate_size	String[20]	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	0	6/6	Private key installed flag (for TLS)
privatekey_time	0~20	0	6/7	Private key installed time. Represented in EPOCH
privatekey_size	0~20	0	6/7	Private key file size (in bytes)

7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio <product dependent>	0~7	0	6/6	Audio channel for CoS (capability.naudio > 0)
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP (capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address>	<blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address>	<blank>	6/6	IPv6 router address.
addondns	<ip address>	<blank>	6/6	IPv6 DNS address.
allowoptional	<boolean>	0	6/6	Allow manually setup of IP address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	1/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
s0_accessname	string[32]	video.mjpg	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname <product dependent>	string[32]	video2.mjpg	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
s2_accessname <product dependent>	string[32]	video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2)
anonymousviewing	<boolean>	0	1/6	Enable anonymous streaming viewing.

7.6.6 HTTPS

Subgroup of **network**: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	443	1/6	HTTPS port.

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	\<boolean\>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)
s2_accessname	string[32]	live3.sdp	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2)

7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	\<boolean\>	0	4/4	Enable always multicast.
ipaddress	\<ip address\>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address.
videoport	1025 ~ 65535	s0:5560 s1:5564 s2:5568	4/4	Multicast video port.
audioport	1025 ~ 65535	S0:5562	4/4	Multicast audio port.

<product dependent>		S1:5566 S2:5570		(capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name.
pass	password[64]	<blank>	6/6	PPPoE account password.

7.6.11 WebSocket port

Subgroup of **network**: **websocket**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65534	777	1/6	Server port for WebSocket. (capability.protocol.websocket =1)

7.7 IP Filter

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[43]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	0~31 (Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>)	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[43]	<blank>	6/6	IPv6 address list.

7.8 Video input

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	4/4	CMOS frequency. (capability.videoin.type=2)
whitebalance	auto, manual, rbgain <product dependent>	auto	1/4	"auto" indicates auto white balance. "manual" indicates keep current value. "rbgain" indicates using rgain and gbain.
exposurelevel	0~12	6	4/4	Exposure level
autoiris	<boolean>	1	1/4	Enable auto Iris.
enableblc	<boolean>	0	1/4	Enable backlight compensation.
color	0, 1	1	1/4	0 =>monochrome 1 => color
flip	<boolean>	0	1/4	Flip the image.
mirror	<boolean>	0	1/4	Mirror the image.
ptzstatus	<integer>	0	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[64]	<blank>	4/4	Enclose caption.
imprinttimestamp	<boolean>	0	1/4	Overlay time stamp on video.
maxexposure	1, 15, 30,	30	1/4	Maximum exposure time.

	60, 120, 240, 480 <product dependent>			

7.8.1 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	0	0	1/4	Set video mode.
cmosfreq	50, 60	60	1/4	CMOS frequency. (capability.videoin.type=2)
whitebalance	auto, manual, rbgain <product dependent>	auto	1/4	"auto" indicates auto white balance. "manual" indicates keep current value. "rbgain" indicates using rgain and gbain.
rgain	0~100	30	1/4	Manual set rgain value of gain control setting.
bgain	0~100	30	1/4	Manual set bgain value of gain control setting.
exposurelevel	0~12	6	1/4	Exposure level
autoiris	0~1	1	1/4	set 1 to enable auto iris, set 0 to disable auto iris.
piris_mode	manual, indoor, outdoor	manual	1/4	PIris mode manual = 0 indoor=1 outdoor=2
piris_position	1~100	1	1/4	Position of piris
enableblc	0~1	0	1/4	Enable backlight compensation
maxgain	0~100	100	1/4	Manual set maximum gain value.
color	0, 1	1	1/4	0 =>monochrome

				1 => color
flip	<boolean>	0	1/4	Flip the image.
mirror	<boolean>	0	1/4	Mirror the image.
ptzstatus	<integer>	0	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[64]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	1/4	Overlay time stamp on video.
textonvideo_position	top, bottom	top	1/4	Text on video string position
textonvideo_size	15, 25, 30	15	1/4	Text on video font size
exposuremode	auto,fixed	auto	1/4	Exposure mode
maxexposure	50~32000	60	1/4	Maximum exposure time.
minexposure	1~32000	32000	1/4	Minimum exposure time.
enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
s<0~(m-1)>_codectype	mjpeg, h264 <product dependent>	h264	1/4	Video codec type.
s<0~(m-1)>_streamtype	0~3	2	1/4	Video stream type. 0: rectified 1: side by side 2: single eye 3: depth

s<0~(m-1)>_resolution	Reference capability_videoin_resolution	s0: 1280x784 s1: 1280x784 s2: 640x392	1/4	Video resolution in pixels.	
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	1/4	Intra frame period in milliseconds.	
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	cbr	1/4	cbr, constant bitrate vbr, fix quality smart , smart stream	
s<0~(m-1)>_h264_quant	1~5, 99, 100	3	1/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.	
s<0~(m-1)>_h264_qvalue	0~51	30	1/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)	
s<0~(m-1)>_h264_qpercent	1~100	50	1/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 100)	
s<0~(m-1)>_h264_bitrate	20000~40000000	s0: 2000000 s1: 2000000 s2: 512000	1/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".	
s<0~(m-1)>_h264_maxvbrbitrate	20000~40000000	40000000	1/4	Set bit rate in bps when choosing vbr in "ratecontrolmode".	
s<0~(m-1)>_h264_maxframe	1~15	s0:10 s1:15 s2:10	1/4	Set maximum frame rate in fps (for h264).	
s<0~(m-1)>_h264_profile <product dependent>	0~2	1	1/4	Indicate H264 profiles 0: baseline	

				1: main profile 2: high profile
s<0~(m-1)>_h264_prioritypolicy	framerate,imagequality	framerate	1/4	Set prioritypolicy
s<0~(m-2)>_h264_smartstream_mode	autotracking,manual,hybrid	autotracking	7/7	Set Smart stream mode autotracking:Auto (Motion detection for ROI) manual:Manual (set manual window for ROI) hybrid:Auto and Manual (mix both motion detection and Manual window for ROI)
s<0~(m-2)>_h264_smartstream_foreground_qvalue	0~51	20	7/7	Manual video quality level input. (s<0~(m-1)>_h264_smartstream_foreground_quant = 99)
s<0~(m-2)>_h264_smartstream_foreground_quant	0~5, 99, 100	3	7/7	Quality of foreground quality 1 = worst quality, 5 = best quality.
s<0~(m-2)>_h264_smartstream_background_qvalue	0~51	40	7/7	Manual video quality level input. (s<0~(m-1)>_h264_smartstream_background_quant = 99)
s<0~(m-2)>_h264_smartstream_background_quant	0~5, 99, 100	1	7/7	Quality of background quality 1 = worst quality, 5 = best quality.
s<0~(m-2)>_h264_smartstream_maxbitrate	20000~40000000	40000000	7/7	Maximum bitrate
s<0~(m-2)>_h264_smartstream_win_i<0~2>_enable	0~1	0	7/7	Enable or disable the window.
s<0~(m-2)>_h264_smartstream_win_i<0~2>_home	0~368, 0~288	(150,110)	7/7	Left-top corner coordinate of the window.
s<0~(m-2)>_h264_smartstream_win_i<0~2>_size	0~400, 0~320	(100x75)	7/7	Width and height of the window.
s<0~(m-1)>_mjpeg_ratecontrolmode <product dependent>	cbr, vbr	vbr	1/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mjpeg_quant	1~5, 99, 100	3	1/4	Quality of JPEG video. 99 is the customized manual input setting. 1 = worst quality, 5 = best quality.

				100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	2~97	50	1/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 99)
s<0~(m-1)>_mjpeg_qpercent	1~100	50	1/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_mjpeg_bitrate	20000~40000 000	s0: 20000000 s1: 1000000 s2: 20000000	1/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mjpeg_maxvb rbitrate	20000~40000 000	40000000	1/4	Set bit rate in bps when choosing vbr in "ratecontrolmode".
s<0~(m-1)>_mjpeg_maxfra me	1~15	s0:10 s1:15 s2:10	1/4	Set maximum frame rate in fps (for JPEG).
s<0~(m-1)>_mjpeg_priority policy	framerate,imag equality	s0: framerate s1: framerate s2: imagequali ty	1/4	Set priority policy
wdrc_mode	0~3	0	0/7	WDR enhanced. 0: off 1: auto 2: always on 3: keep current value
wdrc_strength	0~2	1	0/7	WDR enhanced. 0: low 1: medium 2: high

7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: **videoin_c0_profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	1/4	Enable/disable this profile setting
policy	schedule	schedule	1/4	The mode which the profile is applied to.
begintime	hh:mm	18:00	1/4	Begin time of schedule mode.
endtime	hh:mm	06:00	1/4	End time of schedule mode.
exposuremode	auto,fixed	auto	1/4	Exposure Mode
maxexposure	1~32000	30	1/4	Maximum exposure time.
minexposure	1~32000	32000	1/4	Minimum exposure time.
enableblc	<boolean>	0	1/4	Enable backlight compensation.
exposurelevel	0~12	6	1/4	Exposure level
maxgain	0~100	100	1/4	Manual set maximum gain value.
mingain	0~100	0	1/4	Manual set minimum gain value.
autoiris	<boolean>	0	1/4	Enable auto Iris.
whitebalance	auto, manual, rbgain	auto	1/4	"auto" indicates auto white balance. "manual" indicates keep current value.
rgain	0~100	30	1/4	Manual set rgain value of gain control setting.
bgain	0~100	30	1/4	Manual set bgain value of gain control setting.
irismode	fixed, indoor, outdoor	outdoor	1/4	Video Iris mode.
wdrc_mode	0~3	0	0/7	WDR enhanced. 0: off 1: auto 2: always on 3: keep current value
wdrc_strength	0~2	1	0/7	WDR enhanced. 0: low 1: medium

				2: high

7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
exposuremode	auto,fixed	auto	4/4	Exposure Mode
maxexposure	1~32000	30	4/4	Maximum exposure time.
minexposure	1~32000	32000	1/4	Minimum exposure time.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	<boolean>	0	4/4	Enable backlight compensation.
irismode	fixed, indoor, outdoor	outdoor	4/4	Video Iris mode.
wdrc_mode	0~3	0	0/7	WDR enhanced. 0: off 1: auto 2: always on 3: keep current value
wdrc_strength	0~2	0	0/7	WDR enhanced. 0: low 1: medium 2: high
maxgain	0~100	100	4/4	Manual set maximum gain value.
autoiris	<boolean>	0	4/4	Enable auto Iris.

7.10 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightnesspercent	0~100	0	4/4	Adjust brightnesspercent of image
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation=100
contrastpercent	0~100	50	4/4	Adjust contrastpercent of image
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
dnr_mode	0~1	0	4/4	0:disable 1:enable
dnr_strength	1~100	50	4/4	Strength of DNR
profile_i0_enable	<boolean>	0	4/4	Enable/disable this profile setting
profile_i0_policy	schedule	schedule	4/4	The mode which the profile is applied to.
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_brightnesspercent	0~100	0	4/4	Adjust brightnesspercent of image
profile_i0_contrastpercent	0~100	50	4/4	Adjust contrastpercent of image
profile_i0_saturationpercent	0~100	50	4/4	Adjust saturationpercent of image
profile_i0_sharpnesspercent	0~100	50	4/4	Adjust sharpnesspercent value of image
profile_i0_dnr_mode	0~1	0	4/4	0:disable 1:enable
profile_i0_dnr_strength	1~100	50	4/4	Strength of DNR

7.11 Image setting for preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5,100	100	4/4	Adjust brightness of image according to mode settings.
saturation	-5~5,100	100	4/4	Adjust saturation of image according to mode settings. 100 for saturation percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation=100
contrast	-5 ~ 5,100	100	4/4	Adjust contrast of image according to mode settings.
sharpness	-5~5,100	100	4/4	Adjust sharpness of image according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
dnr_mode	0~1	0	4/4	0:disable 1:enable
dnr_strength	1~100	50	4/4	Strength of DNR

Group: imagepreview

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual, rbgain	auto	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	1~	0	4/4	Restore of adjusting white balance of image according to mode settings
videoin_rgain	0~100	0	4/4	Manual set rgain value of gain control setting.
videoin_bgain	0~100	0	4/4	Manual set bgain value of gain control setting.

7.12 Exposure window setting per channel

Group: **exposurewin_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	auto, custom, blc	auto	4/4	The mode indicates how to decide the exposure. auto: Use full view as the only one exposure window. custom: Use inclusive and exclusive window. blc: Use BLC.
win_i<0~9>_enable	<boolean>	0	4/4	Enable or disable the window.
win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive. 1: Indicate inclusive.
win_i<0~9>_home	(0~368, 0~288)	(150,110)	4/4	Left-top corner coordinate of the window.
win_i<0~9>_size	(0~400, 0~320)	(100x75)	4/4	Width and height of the window.

Group: **exposurewin_c<0~(n-1)>_profile** for m profile and n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
i<0~(m-1)>_mode	auto, custom, blc	auto	4/4	The mode indicates how to decide the exposure. auto: Use full view as the only one exposure window. custom: Use inclusive and exclusive window. blc: Use BLC.
i<0~(m-1)>_win_i<0~9>_enable	<boolean>	0	4/4	Enable or disable the window.
i<0~(m-1)>_win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive. 1: Indicate inclusive.
i<0~(m-1)>_win_i<0~9>_home	(0~368, 0~288)	(150,110)	4/4	Left-top corner coordinate of the window.
i<0~(m-1)>_win_i<0~9>_size	(0~400, 0~320)	(100x75)	4/4	Width and height of the window.

7.13 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	CustomSafe100, DyndnsDynamic, DyndnsCustom, Safe100,	DyndnsDynamic	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org CustomSafe100 => Custom server using safe100 method PeanutHull => PeanutHull
<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

7.14 Express link

Group: expresslink

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	badnetwork	6/6	Camera will check the status of network environment and express link URL
url	string[64]	NULL	6/6	The url user define to link to camera

7.15 UPnP presentation

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPnP presentation service.

7.16 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

7.17 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

| setparamlevel | 0~2 | 0 | 6/6 | Show log of parameter setting. 0: disable 1: Show log of parameter setting set from external. 2. Show log of parameter setting set from external and internal. |

7.18 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password
authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write passwrd
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	DES	6/6	Read/write encryption type
encrypttypero	DES	DES	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Read only community
syslocation	string[128]	<blank>	6/6	System location
syscontact	string[128]	<blank>	6/6	System contact

7.19 Layout configuration

Group: **layout** (New version)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[128]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
custombutton_manualtrigger_show <product dependent>	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#565656	1/6	Background color of control area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color

7.20 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	7/7	Enable privacy mask.
win_i<0~4>_enable	<boolean>	0	7/7	Enable privacy mask window.
win_i<0~4>_name	string[40]	<blank>	7/7	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320	0	7/7	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240	0	7/7	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320	0	7/7	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240	0	7/7	Height of privacy mask window.

7.21 Capability

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string>	0300a	0/7	The HTTP API version.
bootuptime	<positive integer>	60	0/7	Server bootup time.
nir	0, <positive integer>	1	0/7	Number of IR interfaces.
ir	<boolean>	1	0/7	Indicate whether to support built-in IR led
extir	<boolean>	0	0/7	Indicate whether to support external IR led
npir	0, <positive integer>	Outdoor:0 Indoor:1	0/7	Number of PIRs.
ndi	0, <positive integer>	1	0/7	Number of digital inputs.
nvi	0, <positive integer>	3	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer>	1	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0	0/7	Number of audio outputs.
nvideoin	<positive integer>	1	0/7	Number of video inputs.
nvideoinprofile	0, <positive integer>	1	0/7	Number of video input profiles.
nmediastream	<positive	3	0/7	Number of media stream per

	integer>			channels.
nmotion	<positive integer>	0	0/7	Number of motions
nvideosetting	<positive integer>	3	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	1	0/7	Number of video input profiles.
nmotionprofile	0, <positive integer>	0	0/7	Number of motion profiles.
ptzenabled	0, <positive integer>	0	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support) Bit 7 => External or built-in PT; 0(built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris.

				0(fields are valid), 1(fields are invalid)
evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0	0/7	Indicate whether to support joystick control.
remotefocus	<boolean>	0	0/7	Indicate whether to support remote focus function.
storage_dbenabled	<boolean>	1	0/7	Media files are indexed in database.
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	1	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive integer>	10	0/7	The maximum general streaming connections .
protocol_rtp_multicast_scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_backchannel	<boolean>	0	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
protocol_pppoe	<boolean>	1	0/7	Indicate whether to support PPPoE.
protocol_ieee8021x	<boolean>	1	0/7	Indicate whether to support IEEE802.1x.
protocol_qos_cos	<boolean>	1	0/7	Indicate whether to support CoS.
protocol_qos_dscp	<boolean>	1	0/7	Indicate whether to support QoS/DSCP.

protocol_ddns	<boolean>	1	0/7	Indicate whether to support DDNS.
videoin_type	0, 1, 2	2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_c0_nmode	<Integer>	1	0/7	Indicate how many video modes supported by this channel.
videoin_c0_mode	<Integer>	0	0/7	Indicate current video mode.
videoin_c0_streamcodec	<A list of positive integer separated by commas>	6,6,6	0/7	Represent supported codec types of each stream. This contains a list of positive integers, split by comma. Each one stands for a stream, and the definition is as following: Bit 0: Support MPEG4. Bit 1: Support MJPEG Bit 2: Support H.264
videoin_c0_lens_type	motor	motor	0/7	The lens type of this channel. fisheye: Fisheye lens fixed: Build-in lens. The lens may be fixed focal, vari-focal, etc, but not be changeable. changeable: changeable lens. Like box-type camera, users can install any C-Mount or CS-Mount lens as they wish. motor: Lens with motor to support zoom, focus, etc. -: N/A
videoin_c0_lens_modelname	-	-	0/7	Optional model name for lens.
videoin_c0_mode<0~1>_binning	0	0	0/7	Indicate binning is used or not in this video mode. 0: No binning 1: 2x2 binning 3: 3x3 binning
videoin_c0_mode<0~1>_description	<string>	Mode0: 960P (4:3) (MAX 30fps)	0/7	Description about this mode.

videoin_c0_mode<0~1>_ effectivepixel	<WxH>	Mode0: 2560x960	0/7	The visible area of full scene in this video mode. The unit is pixel.
videoin_c0_mode<0~1>_outputsize	<WxH>	Mode0: 2560x960	0/7	The output size of source, equal to the captured size by device, in this video mode. The unit is pixel.
videoin_c0_mode<0~1>_maxframerate	<A list of positive integer separated by commas>	Mode0: 30,30,15	0/7	Indicate maximum frame rate available for the corresponding resolution. Those values are one-to-one mapping to the "resolution" parameter in this video mode.
videoin_codec	<string>	mjpeg,h264	0/7	Available codec list.
videoin_c0_nresolution	<positive integer>	3	0/7	Number of videoin resolution.
videoin_c0_resolution	<a list of available resolution separated by commas><product dependent>	640x240 1280x480 2560x960	0/7	Available resolutions list.
Videoin_c0_maxsize	<WxH>	2560x960	0/7	The maximum resolution of this channel, the unit is pixel.
videoin_c0_mode0_nresolution	<positive integer>	3	0/7	Available resolutions list.
videoin_c0_mode0_resolution	<a list of available resolution separated by commas><product dependent>	640x240 1280x480 2560x960	0/7	Available resolutions list.
videoin_c0_mode0_maxfps_mjpeg	<Integer>	30,30,15	0/7	Maximum fps that the device can encode
videoin_c0_mode0_maxfps_h264	<Integer>	30,30,15	0/7	Maximum fps that the device can encode

videoin_flexiblebitrate	<boolean>	1	0/7	Indicate whether to support flexible bit rate control.
videoout_codec	<a list of the available codec types separated by commas) <product dependent>	ntsc	0/7	Available codec list.
videoin_flexiblebitrate	<boolean>	1	0/7	Indicate whether to support flexible bitrate.
audio_aec	<boolean>	0	0/7	Indicate whether to support acoustic echo cancellation.
audio_mic	<boolean>	0	0/7	Indicate whether to support built-in microphone input.
audio_extmic	<boolean>	1	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	1	0/7	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	1	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0	0/7	Indicate whether to support headphone output.
audioin_codec	aac4, g711, g726 <product dependent>	aac4, g711, g726	0/7	Available codec list for audio input.
audioout_codec	g711 <product dependent>	<blank>	0/7	Available codec list for SIP.
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support "Manage Privilege" of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi

uart_httptunnel	<boolean>	0	0/7	Indicate whether to support HTTP tunnel for UART transfer.
nprivacymask	<positive integer>	0	0/7	Number of privacy masks.
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0	0/7	Indicate whether to support wireless 802.11g.
wireless_s802dot11n	<boolean>	0	0/7	Indicate whether to support wireless 802.11n.
wireless_beginchannel	1 ~ 14	N/A	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	N/A	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0	0/7	Indicate whether to support wireless WPA2.
localstorage_manageable	<boolean>	1	0/7	Indicate whether manageable local storage is supported.
localstorage_seamless	<boolean>	1	0/7	Indicate whether seamless recording is supported.
localstorage_modnum	0, <positive integer>	4	0/7	The maximum MOD connection numbers.

localstorage_slconnum	0, <positive integer>	1	0/7	The maximum seamless connection number.
localstorage_modversion	<string>	1.0.3.3	0/7	Indicate MOD daemon version
adaptiverecording	<boolean>	1	0/7	Indicate whether to support adaptive recording.
adaptivestreaming	<boolean>	1	0/7	Indicate whether to support adaptive recording.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
npreset	0, <positive integer>	20	0/7	Number of preset locations
eptz	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
nanystream	0, <positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
tampering	<boolean>	0	0/7	Indicate whether to support tampering detection.
test_ac	<boolean>	1	0/7	Indicate whether to support test ac key.
windowless	<boolean>	1	0/7	Indicate whether to support windowless plug-in.
supportsd	<boolean>	1	0/7	Indicate whether to support local storage.
timeshift	<boolean>	1	0/7	Indicate whether to support time shift caching stream.
whitelight	<boolean>	0	0/7	Indicate whether to support white

				light led.
iris	<boolean>	0	0/7	Indicate whether to support iris control.
temperature	<boolean>	0	0/7	Indicate whether to support temperature detection.
fisheye	<boolean>	0	0/7	Indicate where fisheye camera.
vadp	<positive integer>	0	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => VADP interface Bit 1 => Capture video raw data Bit 2 => Support encode jpeg Bit 3 => Capture audio raw data Bit 4 => Support event trigger Bit 5 => Support license registration Bit 6 => Support shared memory API
remotecamctrl_master	0, <positive integer>	0	0/7	Indicate whether to support remote auxiliary camera (master side), this value means supporting max number of auxiliary camera.
remotecamctrl_slave	<boolean>	0	0/7	Indicate whether to support remote camera control (slave side).
media_totalspace	<positive integer>	35000	0/7	Available memory space (KB) for media.
media_snapshot_sizepersecond	<positive integer>	1250	0/7	Maximum size (KB) of one snapshot image.
media_snapshot_maxpreevent	<positive integer>	7	0/7	Maximum snapshot number before event occurred.
media_snapshot_maxpostevent	<positive integer>	7	0/7	Maximum snapshot number after event occurred.
media_videoclip_maxsize	<positive integer>	8192	0/7	Maximum size (KB) of a videoclip.
media_videoclip_maxlength	<positive integer>	20	0/7	Maximum length (second) of a videoclip.
media_videoclip_maxpreevent	<positive integer>	9	0/7	Maximum duration (second) after event occurred in a videoclip.
version_genetec	<string>	1.0.2.7	0/7	Indicate Genetec daemon version
version_onvifdaemon	<string>	1.12.0.2	0/7	Indicate ONVIF daemon version
image_ c0_wdrc	<boolean>	1	0/7	Indicate whether to support WDR

				enhanced.
image_c0_dnr	<boolean>	1	0/7	Indicate whether to support digital noise reduction.
image_ c0_iristype	<string>	piris	0/7	Indicate iris type.
image_ c0_backfocus	<boolean>	0	0/7	Indicate whether to support back focus.
image_ c0_focusassist	<boolean>	0	0/7	Indicate whether to support focus assist.
image_ c0_remotefocus	<boolean>	1	0/7	Indicate whether to support remote focus.

7.22 Customized event script

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Custom script identification of this entry.
date	string[4~20]	<blank>	6/6	Date of custom script.
time	string[4~20]	<blank>	6/6	Time of custom script.

7.23 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.
priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	10	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, seq, recnotify, vi, vadp	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "seq" = Periodic condition "recnotify" = Recording notification. "vi"= Virtual input (Manual trigger) "vadp"=VADP event
triggerstatus	String[40]	trigger	6/6	The status for event trigger.
exttriggerstatus	String[40]	<blank>	6/6	The status for event trigger.
exttriggerstatus1	String[40]	<blank>	6/6	The status for event trigger.
exttriggerstatus2	String[40]	<blank>	6/6	The status for event trigger.
exttriggerstatus3	String[40]	<blank>	6/6	The status for event trigger.
di	0~3	1	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.

mdwin	0~7	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	0~7	0	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
vi	0~7	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is "vi". One bit represents one digital input. The LSB indicates VI 0.
valevel	0,1	0	6/6	Select audio detection event. 0: not select 1: select
valevel0	0,1	0	6/6	Select audio detection profile event. 0: not select 1: select
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.

endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
lowlightcondition <product dependent>	0, 1	1	6/6	Switch on white light LED in low light condition 0 => Do action at all times 1 => Do action in low-light conditions
action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_goto_enable <product dependent>	<Boolean>	0	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name <product dependent>	string[40]	<blank>	6/6	Specify the preset name that ptz goto on event triggered.
action_cf_enable	<Boolean>	0	6/6	Enable or disable sending media to SD card.
action_cf_folder	string[128]	<blank>	6/6	Path to store media.
action_cf_media	0~4,101	<blank>	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.
action_cf_backup	<Boolean>	0	6/6	Enable or disable the function that send media to SD card for backup if network is disconnected.
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	0~4,101	<blank>	6/6	Index of the attached media. 101 means "Recording Notify"
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.

7.24 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[640]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.25 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	systemlog	6/6	Media type to send to the server or store on the server.
snapshot_source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	Snapshot[n]_	6/6	Indicate the prefix of the filename. media_i0=> Snapshot1_ media_i1=> Snapshot2_ media_i2=> Snapshot3_ media_i3=> Snapshot4_ media_i4=> Snapshot5_
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	VideoClip[n]_	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 8192	500	6/6	Maximum size of one video clip file in Kbytes.

7.26 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification
notifyserver	0~31	0	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.

weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	<blank>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	cf	6/6	The destination to store the recorded data. "cf" means local storage (CF or SD card). "0" means the index of the network storage.
cffolder	string[128]	NULL	6/6	Folder name.
maxsize <product dependent>	100~2000 <product dependent>	100 <product dependent>	6/6	Unit: Mega bytes. When this condition is reached, recording file is truncated.
maxduration <product dependent>	60~3600 <product dependent>	60 <product dependent>	6/6	Uuit: Second When this condition is reached, recording file is truncated.
adaptive_enable <product dependent>	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent <product dependent>	0~9	1	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)

| adaptive_postevent <product dependent> | 0~10 | 1 | 6/6 | Indicate when is the adaptive recording stopped after the event trigger point (seconds) |

7.27 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	auto	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	0	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.
organizationname	string[64]	VIVOTEK Inc.	6/6	Organization name in the certificate information.
unit	string[64]	VIVOTEK Inc.	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek.com	6/6	Common name in the certificate information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

7.28 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
cyclic_enabled	<boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	0	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	1~	7	6/6	To specify the expired days for automatic clean up.

7.29 Region of interest

Group: **roi_c<0~(n-1)>** for n channel product, and m is the number of streams which support ROI. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
s<0~(m-1)>_home	(0~1744,0~936)	(0,0)	7/7	ROI left-top corner coordinate.
s<0~(m-1)>_size	176~ x 144~	2560x1920	7/7	ROI width and height. The width value must be multiples of 16 and the height value must be multiples of 8

7.30 ePTZ setting

Group: **eptz_c<0~(n-1)>** for n channel product. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
osdzoom	<boolean>	1	7/7	Indicates multiple of zoom in is "on-screen display" or not
smooth	<boolean>	1	7/7	Enable the ePTZ "move smoothly" feature
tiltspeed	-5 ~ 5	0	7/7	Tilt speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

panspeed	-5 ~ 5	0	7/7	Pan speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	0	7/7	Zoom speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
autospeed	1 ~ 5	1	7/7	Auto pan/patrol speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

Group: **eptz_c<0~(n-1)>_s<0~(m-2)>** for n channel product and m is the number of streams which support ePTZ. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
patrolseq	string[120]	<blank>	1/4	The patrol sequence of ePTZ. All the patrol position indexes will be separated by ","
patroldwelling	string[160]	<blank>	1/4	The dwelling time (unit: second) of each patrol point, separated by ",".
preset_i<0~19>_name	string[40]	<blank>	1/7	Name of ePTZ preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)
preset_i<0~19>_pos	<coordinate>	<blank>	1/7	Left-top corner coordinate of the preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)
preset_i<0~19>_size	<window size>	<blank>	1/7	Width and height of the preset. (It should be set by ePreset.cgi rather than by setparam.cgi.)

7.31 VIVOTEK Application Development Platform setting

Group: **vadp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
version	0~.0~.0~.0~.0~	1.3.1.0	6/7	Indicate the VADP version.
resource_total_memory	0~	134996	6/7	Indicate total available memory size for VADP modules.
resource_total_storage	0~	155284	6/7	Indicate total size of the internal storage space for storing VADP modules.
resource_free_memory	0~	24576	6/7	Indicate free memory size for VADP modules.
resource_free_storage	0~	10240	6/7	Indicate current free storage size for uploading VADP modules.
module_number	0~	1	6/7	Record the total module number that already stored in the system.
module_order	string[40]	0	6/6	The execution order of the enabled modules.
module_save2sd	<boolean>	0	6/6	Indicate if the module should be saved to SD card when user want to upload it. If the value is false, save module to the internal storage space and it will occupy storage size.

Group: vadp_module_i<0~(n-1)>

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	module_i0: 1 module_i1~9: 0	6/6	Indicate if the module is enabled or not. If yes, also add the index of this module to the module_order.
name	string[40]	module_i0: Stereo Counting	6/6	Module name

		module_i1~9: <blank>		
url	string[120]	module_i0: Stereo-Counting/www/index.html module_i1~9: <blank>	6/6	Define the URL string after the IP address if the module provides it own web page.
vender	string[40]	module_i0: VIVOTEK module_i1~9: <blank>	6/6	The provider of the module.
vendorurl	string[120]	module_i0: http://www.vivotek.com module_i1~9: <blank>	6/6	URL of the vendor.
version	string[40]	module_i0: 1.0 module_i1~9: <blank>	6/6	Version of the module.
license	string[40]	module_i0: N/A module_i1~9: <blank>	6/6	Indicate the license status of the module.
path	string[40]	module_i0: /mnt/flash2/vadp-preload/0 module_i1~9: <blank>	6/6	Record the storage path of the module.
initscr	string[40]	module_i0: main.sh module_i1~9: <blank>	6/6	The script that will handle operation commands from the system.
status	string[40]	module_i0: on module_i1~9: off	6/6	Indicate the running status of the module.

7.32 Seamless recording setting

Group: **seamlessrecording** (capability.localstorage.seamless > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
diskmode	seamless, manageable	seamless	1/6	"seamless" indicates enable seamless recording. "manageable" indicates disable seamless recording.
maxconnection	3	3	1/6	Maximum number of connected seamless streaming.
stream	1~3	1	7/7	(Internal used, read only)
output	0~2	2	7/7	(Internal used, read only)
enable	<boolean>	0	1/6	Indicate whether seamless recording is recording to local storage or not at present. (Read only)
guid<0~2>_id	string[127]	<blank>	1/6	The connected seamless streaming ID. (Read only)
guid<0~2>_number	0~3	0	1/6	Number of connected seamless streaming with guid<0~2>_id. (Read only)

7.33 Genetec info

Group: genetec

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
image_ contrast	<integer>	50	7/7	Only for genetec omnicast
image_ brightness	<integer>	0	7/7	Only for genetec omnicast
motion_ i<0~4>	<integer>	0,0,0,0	7/7	Only for genetec omnicast

8. Useful Functions

Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/dido/setdo.cgi?do1=*<state>*[&do2=<state>] [&do3=<state>][&do4=<state>]

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all of the digital input statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: *<length>*\r\n \r\n [di0=<state>]\r\n [di1=<state>]\r\n [di2=<state>]\r\n [di3=<state>]\r\n

where *<state>* can be 0 or 1.

Example: Query the status of digital input 1 .

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di1=1\r\n

Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <*length*>\r\n

\r\n

[do0=<state>]\r\n

[do1=<state>]\r\n

[do2=<state>]\r\n

[do3=<state>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

do1=1\r\n

Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]

[&quality=<value>][&streamid=<value>]

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<product dependent>	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: image/jpeg\r\n

[Content-Length: <image size>\r\n]

<binary JPEG image data>

Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/admin/editaccount.cgi?

method=<value>&username=*<name>*[&userpass=*<value>*][&privilege=*<value>*]

[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Logs

Note: This request require Administrator privileges.
Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n

<system log information>\r\n

Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

fimage=<file name>[&return=<return page>]\r\n \r\n <multipart encoded form data>

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

ePTZ Camera Control (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value> [&move=<value>] – Move home, up, down, left, right [&auto=<value>] – Auto pan, patrol [&zoom=<value>] – Zoom in, out [&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick [&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick [&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image (Move the center of image to the coordination (x,y) based on resolution or videosize.) [[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>]] – Set speeds [&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2 http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100& videosize=640x400&resolution=640x400&stretch=0

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer>	The direction of movement, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.

return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

ePTZ Recall (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>& recall=<value>[&return=*<return page>*]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40 characters	One of the present positions to recall.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

ePTZ Preset Locations (capability.eptz > 0)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value> [&addpos=<value>][&delpos=<value>][&return=*<return page>*]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
addpos	<Text string less than 40 characters>	Add one preset location to the preset list.

delpos	<Text string less than 40 characters>	Delete preset location from the preset list.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path.

IP Filtering

Note: This request requires Administrator access privileges.
Method: GET/POST

Syntax: <product dependent>

http://*<servername>*/cgi-bin/admin/ipfilter.cgi?type[=<value>]		
http://*<servername>*/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=*<ipaddress>*[&index=<value>][&return=*<return page>*]		
http://*<servername>*/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=*<return page>*]		
PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

IP Filtering for ONVIF

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Get SDP of Streams

Note: This request requires Viewer access privileges.
Method: GET/POST

Syntax:

http://*<servername>*/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the

"subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://*<servername>*/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://*<servername>*/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

Senddata (capability.nuart > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/senddata.cgi?

[com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <system information length>\r\n

\r\n

<hex decimal data>\r\n

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

Storage managements (capability.storage.dbenabled > 0)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional.

		Indicate if the file is locked or not.
		0: file is not locked.
		1: file is locked.
		A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional.
		Indicate the event trigger time. (not the file created time)
		Format is "YYYY-MM-DD HH:MM:SS"
		Please embrace your input value with single quotes.
		Ex. triggerTime='2008-01-01 00:00:00'
		If you want to search for a time period, please apply "TO" operation.
		Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional.
		Limit the maximum number of returned search records.
offset	<positive integer>	Optional.
		Specifies how many rows to skip at the beginning of the matched records.
		Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations.
Moreover, to search for a specific time period, you can use "TO" connector.
Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required.
		Identify the designated record.
		Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION

label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript

Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state. Where "nstate" is next state after duration.	Ex: vi0=1 Setting virtual input 0 to trigger state
		Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state. Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	<return page>	Redirect to the page <return page> after the request is completely assigned. The <return page> can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. setvi.cgi?vi3=0 VI index is out of range. setvi.cgi?vi=1 No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: setvi.cgi?vi0=0(15000)1 setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

Open Timeshift Stream (capability.timeshift > 0,

timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]

"n" is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive integer>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)
reftime	mm:ss	The time camera receives the request.	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.) Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return "415 Unsupported Media Type".
minsft	<positive integer>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

Return Code	Description
400 Bad Request	Request is rejected because some parameter values are illegal.
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled.

Open Anystream (capability.nanystream > 0)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<servername>/videoany.mjpg?codectype=mjpeg[&resolution=<value>&mjpeg_quant=<value>&mjpeg_qvalue=<value>&mjpeg_maxframe=<value>]

For RTSP (H264), the user needs to input the URL below into an RTSP compatible player.

rtsp://<servername>/liveany.sdp?codectype=h264[&resolution=<value>&h264_intraperiod=<value>&h264_ratecontrolmode=<value>& h264_quant=<value>& h264_qvalue=<value>& h264_bitrate=<value>& h264_maxframe=<value>]

<product dependent>

PARAMETER	VALUE	DEFAULT	DESCRIPTION
codectype	mjpeg, h264	N/A	Set codec type for Anystream.
solution	capability_videoin_resolution	<product dependent>	Video resolution in pixels.
mjpeg_quant	99, 1~5	3	Quality of JPEG video. 0,99 is the customized manual input setting. 1 = worst quality, 5 = best quality.
mjpeg_qvalue	2~97	50	Manual video quality level input. (This must be present if mjpeg_quant is equal to 0, 99)
mjpeg_maxframe	1~25 (5M mode) 1~30 (2M mode)	30	Set maximum frame rate in fps (for JPEG).
h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	Intra frame period in milliseconds.

h264_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate vbr: fix quality
h264_quant	99, 1~5	3	Quality of video when choosing vbr in "h264_ratecontrolmode". 0,99 is the customized manual input setting. 1 = worst quality, 5 = best quality.
h264_qvalue	0~51	30	Manual video quality level input. (This must be present if h264_quant is equal to 0, 99)
h264_bitrate	20~40000000	8000000	Set bit rate in bps when choosing cbr in "h264_ratecontrolmode".
h264_maxframe	1~25 (5M mode) 1~30 (2M mode)	25 30	Set maximum frame rate in fps (for H264).

Remote Focus

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/admin/remotefocus.cgi?function=<value>[&direction=<value>] [&position=<value>][&steps=<value>][&iris]

PARAMETER	VALUE	DESCRIPTION

function	zoom, focus, auto, scan, stop, positioning getstatus	Function type
		zoom – Move zoom motor
		focus – Move focus motor
		auto – Perform auto focus
		scan – Perform focus scan
		stop – Stop current operation
		positioning – Position the motors
		getstatus – Information of motors, return value as below:
		    remote_focus_focus_motor_max: Maximum steps of focus motor
		    remote_focus_zoom_motor_max: Maximum steps of zoom motor
		    remote_focus_focus_motor_start: Start point of effective focal length
		    remote_focus_focus_motor_end: End point of effective focal length
		    remote_focus_focus_motor: Current position of focus motor
		    remote_focus_zoom_motor: Current position of zoom motor
		    remote_focus_focus_enable: Current function of focus motor
		    remote_focus_zoom_enable: Current function of zoom motor
		    remote_focus_value_mode: Source of focus value. 0: ISP, 1: Edge.

direction	direct, forward, backward	Motor's moving direction. It works only if function=zoom | focus.
position	0 ~ <motor_max>	Motor's position. It works only if function=zoom | focus and direction=direct. <motor_max> is refer to remote_focus_focus_motor_max or remote_focus_zoom_motor_max which replied from "function=getstatus"

steps	1 ~ <motor_max>	Motor's moving steps.
		It works only if function=zoom | focus and direction=forward | backward.
		<motor_max> is refer to remote_focus_focus_motor_max or remote_focus_zoom_motor_max which replied from "function=getstatus"
iris	N/A	Open iris or not.
		It works only if function=auto | scan.

Export Files

Note: This request requires Administrator privileges.

Method: GET

Syntax:

For daylight saving time configuration file:

http://<*servername*>/cgi-bin/admin/exportDst.cgi

For language file:

http://<*servername*>/cgi-bin/admin/export_language.cgi?currentlanguage=<value>

PARAMETER	VALUE	DESCRIPTION
currentlanguage	0~20	Available language lists.
		Please refer to:
		system_info_language_i0 ~ system_info_language_i19.

For setting backup file:

http://<*servername*>/cgi-bin/admin/export_backup.cgi?backup

Upload Files

Note: This request requires Administrator privileges.

Method: POST

Syntax:

For daylight saving time configuration file:

http://*<servername>*/cgi-bin/admin/upload_dst.cgi

Post data:

filename =<file name>\r\n

\r\n

<multipart encoded form data>

For language file:

http://*<servername>*/cgi-bin/admin/upload_lan.cgi

Post data:

filename =<file name>\r\n

\r\n

<multipart encoded form data>

For setting backup file:

http://*<servername>*/cgi-bin/admin/upload_backup.cgi

Post data:

filename =<file name>\r\n

\r\n

<multipart encoded form data>

Server will accept the file named <file name> to upload this one to camera.

Technical Specifications

Precision

· VIVOTEK's 3D Depth Technology
· Up to 98% counting accuracy rate
· Real-time data
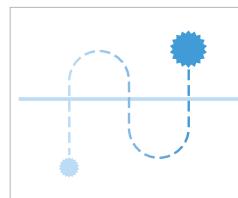 (system/counting/daily reports;
  time/region reports)

Efficiency

· Object tracking path
· Filter carts, children and strollers
· Bi-directional counting on definable flow
· Detection of U-turns to avoid double counting
· Not Influenced by shadows, reflections or glare conditions
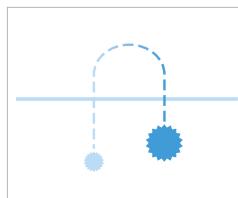
Counting: 0   Counting: 1

Video Security

· Video surveillance (viewing and recording)
· Multiple video streaming
· Remote management
· Seamless integration with VAST CMS

Easy Installation

· Discreet ceiling mount
· Compatible with 4"x2" electrical box

Technical Specifications

Model	SC8131(F2): f = 2 mm SC8131(F4): f = 4 mm SC8131(F6): f = 6 mm
System Information	
CPU	Multimedia SoC (System-on-Chip)
Flash	256 MB
RAM	512 MB
Camera Features	
Image Sensor	1/3" Progressive CMOS
Maximum Frame Rate	15 fps @ 2560x960
On-board Storage	MicroSD/SDHC/SDXC card slot
Video	
Compression	H.264 & MJPEG
Maximum Streams	3 simultaneous streams
Report Format	JSON/XML/CSV
General	
Connectors	RJ-45 for Network/PoE connection DI/DO USB 2.0 (Only as a power bank, not for data transmission) MicroSD Slot
LED Indicator	System power and status indicator
Power Input	IEEE 802.3af PoE Class 3
Power Consumption	PoE: Max.12.95W USB: Max. 300mA
Dimensions	160 (D) x 70 (W) x 38 (H) mm
Weight	396 g

Safety Certifications	CE, LVD, FCC Class B, VCCI, C-Tick, UL
Operating Temperature	Starting Temperature: 0˚C ~ 40˚C (32˚F ~ 104˚F) Working Temperature: -10˚C ~ 40˚C (14˚F ~ 104˚F)
Warranty	36 months
Installation	
Installation Height	SC8131(F2): 240~500 cm (7.9~16.4') SC8131(F4): 500~800 cm (16.4~26.2') SC8131(F6): 800~1000 cm (26.2~32.8')
System Requirements	
Operating System	Microsoft Windows 8/7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~43 (streaming only) Internet Explorer 9/10/11
Other Players	VLC: 1.1.11 or above QuickTime: 7 or above
Included Accessories	
Others	Quick installation guide, mounting bracket, screw pack
Dimensions	

38 mm   160 mm   70 mm
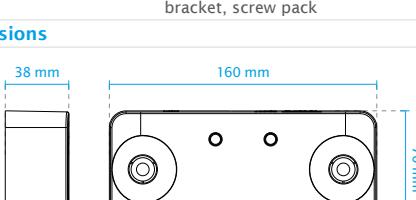
Technology License Notice

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

H.264

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

■ This device may not cause harmful interference, and

■ This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

■ Reorient or relocate the receiving antenna.

■ Increase the separation between the equipment and receiver.

■ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

■ Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準にづくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.