Sarix® Value Series
IR Environmental Cameras
Operations Manual

Bullet IBV

Dome IMV and IJV

Turret IFV and ITV

Document number: C6701M-A

Publication date: 06/21

Table of Contents

Accessing the Network Camera

Access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, or the VideoXpert System.

Access the Network Camera Via a Web Browser

Use VxToolbox to access the Network Cameras on LAN.

If your network environment is not a LAN, follow these steps to access the Network Camera:

1. Launch your web browser (for example: Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field, and then press Enter.

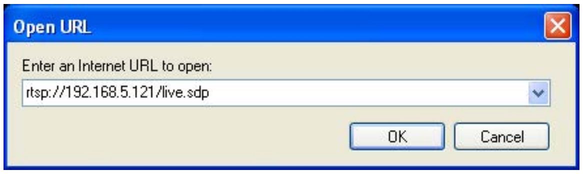
   Live video will be displayed in your web browser.
3. If it is the first time installing the network camera, an information bar might prompt you to install any necessary plugins. Follow the instructions to install the plugins on your computer.
4. By default, the Network Camera is not password-protected. To prevent unauthorized access, set a password for the Network Camera.

Viewing Streaming Media Using an RTSP Player

To view the streaming media using an RTSP player, use VLC media player.

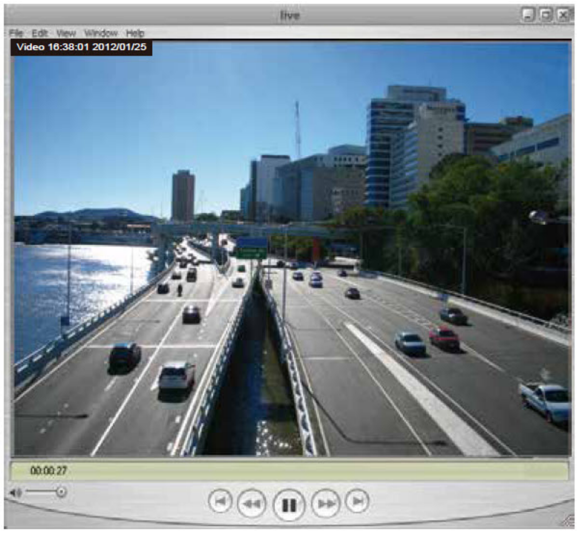
1. Launch the RTSP player.
2. Click **File > Open URL**.

   A URL dialog box will open.

   Enter an Internet URL to open:
   rtsp://192.168.5.121/live.sdp
3. Enter the Internet URL in the appropriate format: rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>
4. Because most ISPs and players only allow RTSP streaming through port number 554, set the RTSP port to 554.

The live video will be displayed in your player.



For more information on how to configure the RTSP access name, see the section titled *Viewing Streaming Media Using an RTSP Player*.

Viewing Streaming Media Using a 3GPP-compatible Mobile Device

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, see the current version of the product Installation Manual.

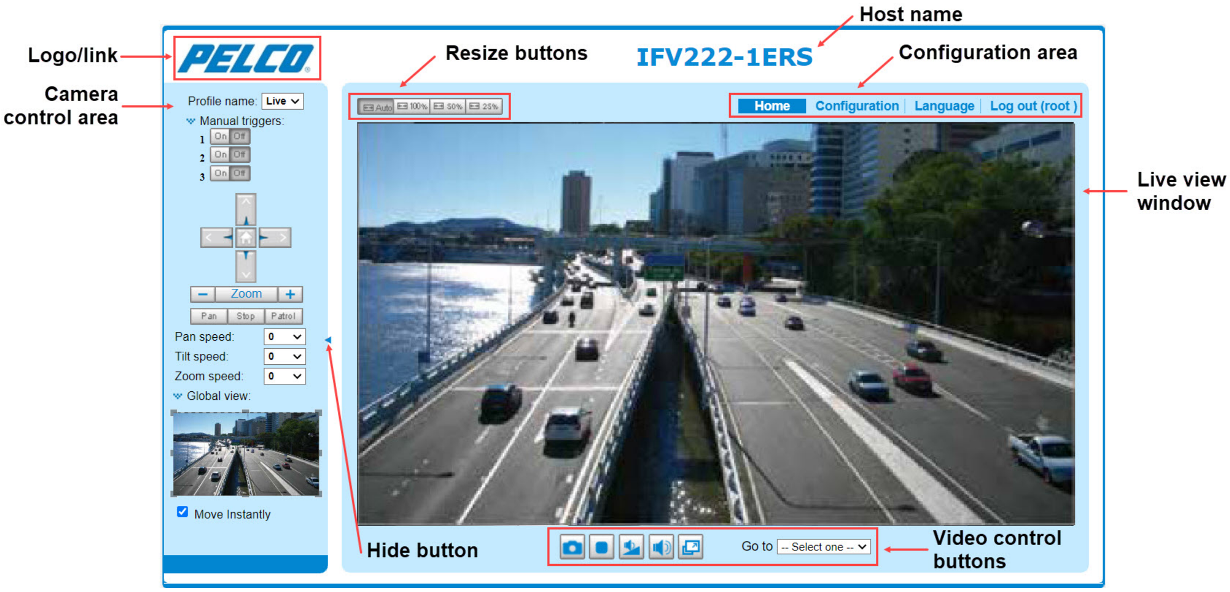
To use this feature, check the following settings on your Network Camera:

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, see the section titled *Viewing Streaming Media Using an RTSP Player*.
2. Because the bandwidth on 3G networks is limited, you will not be able to use a large video size. Set the video streaming parameters as listed below. For more information, see the section titled *Configuring Media > Video*.
   - Video Mode—H.264
   - Frame size—176 x 144
   - Maximum frame rate—5 fps
   - Intra frame period—1S
   - Video quality (constant bit rate)—40kbps
3. Because most ISPs and players only allow RTSP streaming through port number 554, set the RTSP port to 554. For more information,see the section titled *Viewing Streaming Media Using an RTSP Player*.
4. Launch the player on the 3GPP-compatible mobile devices (for example: QuickTime).
5. Type the following URL command into the player.

   rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream # with small frame size and frame rate>.

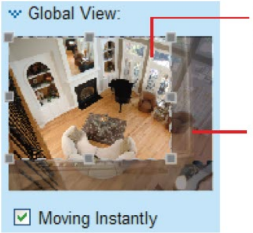
Using the Home Page

This chapter explains the layout of the *Home* page.



- Pelco logo—Click the logo to visit the Pelco web site.
- Host name—The host name can be customized to fit your needs. The name can be changed especially if there are many cameras in your surveillance deployment. For more information, see the section titled *Configuring System > General Settings*.
- Camera control area (available to Administrators only)
  - *Profile name*—Choose from **Max View**, **Recording**, and **Live view**. The choice you make here determines what else you see in the Camera control area.
  - *Manual triggers*—This Network Camera supports multiple streams (streams 1, 2, and 3) simultaneously. You can select any of them for live viewing. For more information about multiple streams, see the section titled *Configuring Media > Video*.

    Click to enable/disable an event trigger manually. Configure an event setting on the *Application* page before you enable this function. See the section titled *Configuring Event > Event*. There can be a total of three event configurations. If you want to hide this item on the homepage, go to **Configuration> System > Homepage Layout > General settings > Customized** button to deselect the *show manual trigger button* checkbox.
  - **Global View**—Click to display the *Global View* window and the *Move Instantly* checkbox. The *Global View* window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation or how to set up the viewing region of the current video stream, see the section titled *Configuring Digital PTZ > Digital PTZ Settings*.



The viewing region of the curruent video stream

The largest frame size

Note: The PTZ buttons on the panel are not operational unless you are showing only a portion of the full image. If the live view window is displaying the full view, the PTZ buttons are not functional.

- Hide Button—You can click the hide button to hide or display the Camera control area.
- Resize Buttons

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

- Configuration area
  - **Home**—Click to access the home page.
  - **Configuration**—Click to access the configuration page of the Network Camera. Pelco recommends that you set a password to the Network Camera so that only the administrator can configure the Network Camera. For more information, see the section titled *Configuring the Network Camera*.
  - **Language**—Click to choose a language for the user interface. You can also change a language on the *Configuration* page; see the section titled *Configuring the Network Camera*.
  - **Log out (root)**—Click to log out and return to the login screen.

- Live view window—View live or recorded video here.
- Video Control Buttons—Depending on the Network Camera model and Network Camera configuration, some buttons might 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.
  - *Stop* (■)—Stop the transmission of the streaming media. Click the Resume (▶) button to continue transmission.
  - *Volume* (🔉)—When the Mute function is not activated (🔊), move the slider bar to adjust the volume on the local computer.
  - *Mute* (🔊)—Turn off the volume on the local computer. The button becomes the *Audio on* (🔇) button after clicking the *Mute* button.

- *Full Screen* (⧉)—Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.
- *Go to*—Click to select a preset from the drop-down menu.

Note: For a megapixel camera, it is recommended to use monitors of the 24" size or larger, and are capable of 1600 x 1200 or better resolutions.

Note: For cameras with built-in microphone, the default audio setting is *Audio on*; for cameras without built-in microphone, the default is audio setting is *Muted*.

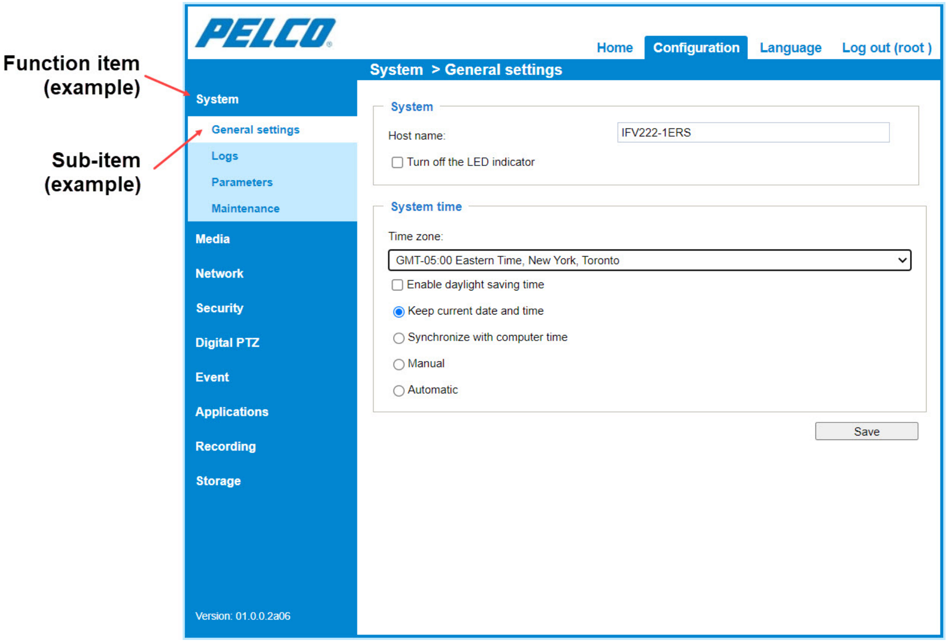
Note: To receive audio input from an external microphone, you might need to enable the audio input from. See the section titled *Configuring Media > Audio*.

Configuring the Network Camera

Click **Configuration** in the Configuration area to enter the camera setting pages. Only Administrators can access the configuration page.

Pelco provides an easy-to-use user interface that helps you set up your network camera with minimal effort. In order to simplify the user interface, 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 in the right panel; 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 interface of the camera settings page:



System

Host name: IFV222-1ERS

□ Turn off the LED indicator

System time

Time zone: GMT-05:00 Eastern Time, New York, Toronto

□ Enable daylight saving time

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

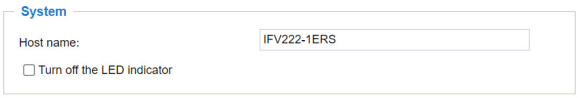
Version: 01.0.0.2a06

Each function item and sub-item in the left panel is explained in the following sections.

Configuring System > General Settings

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

Configuring the System Settings



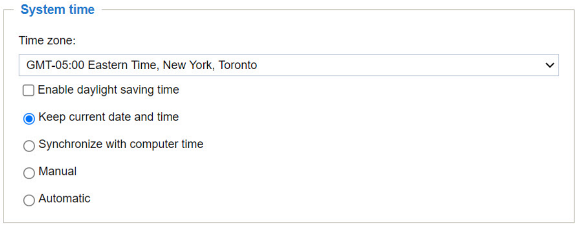
System

Host name: IFV222-1ERS

□ Turn off the LED indicator

- *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 cells of the 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.

Configuring the System Time Settings



System time

Time zone:

GMT-05:00 Eastern Time, New York, Toronto

□ Enable daylight saving time

● Keep current date and time

○ Synchronize with computer time

○ Manual

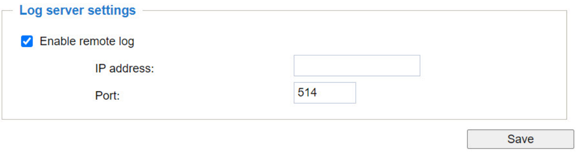
○ Automatic

- *Time Zone*—Select from the drop-down menu, and click to select or deselect the checkbox for *Enable daylight saving time*. If prompted and appropriate, to upload Daylight Savings Time rules, see the section titled *Configuring System > Maintenance*.
- *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. The precondition is that the camera must have the access to the Internet.
  - Update interval—Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Configuring System > Logs

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

Configuring Log Server Settings



Log server settings

☑ Enable remote log

IP address:

Port: 514

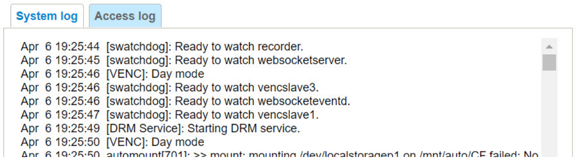
Follow the steps below to set up the remote log:

1. Select *Enable remote log*.
2. In the *IP address* text box, enter the IP address of the remote server.
3. In the *Port* text box, enter the port number of the remote server.
4. 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 using this feature, install a log-recording tool to receive system log messages from the Network

Camera. An example is Kiwi Syslog Daemon. See http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

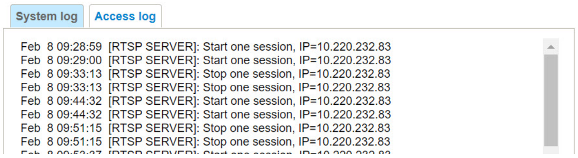
Viewing the System Log



```
Apr  6 19:25:44  [swatchdog]: Ready to watch recorder.
Apr  6 19:25:45  [swatchdog]: Ready to watch websocketserver.
Apr  6 19:25:46  [VENC]: Day mode
Apr  6 19:25:46  [swatchdog]: Ready to watch vencslave3.
Apr  6 19:25:46  [swatchdog]: Ready to watch websocketeventd.
Apr  6 19:25:47  [swatchdog]: Ready to watch vencslave1.
Apr  6 19:25:49  [DRM Service]: Starting DRM service.
Apr  6 19:25:50  [VENC]: Day mode
Apr  6 19:25:50  automount[701]: >> mount: mounting /dev/localstoragep1 on /mnt/auto/CF failed: No
```

This page displays the system log in chronological order. The *System log* is stored in the Network Camera's buffer area and will be overwritten when it reaches a certain limit.

Viewing the Access Log

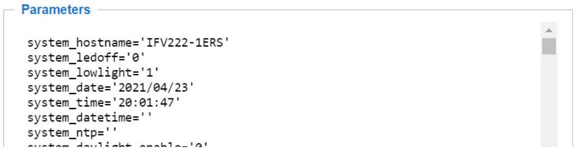


```
Feb  8 09:28:59  [RTSP SERVER]: Start one session, IP=10.220.232.83
Feb  8 09:29:00  [RTSP SERVER]: Start one session, IP=10.220.232.83
Feb  8 09:33:13  [RTSP SERVER]: Stop one session, IP=10.220.232.83
Feb  8 09:33:13  [RTSP SERVER]: Stop one session, IP=10.220.232.83
Feb  8 09:44:32  [RTSP SERVER]: Start one session, IP=10.220.232.83
Feb  8 09:44:32  [RTSP SERVER]: Start one session, IP=10.220.232.83
Feb  8 09:51:15  [RTSP SERVER]: Stop one session, IP=10.220.232.83
Feb  8 09:51:15  [RTSP SERVER]: Stop one session, IP=10.220.232.83
Feb  8 09:53:27  [RTSP SERVER]: Start one session, IP=10.220.232.83
```

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

Configuring System > Parameters

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



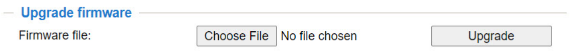
```
system_hostname='IFV222-1ERS'
system_ledoff='0'
system_lowlight='1'
system_date='2021/04/23'
system_time='20:01:47'
system_datetime=''
system_ntp=''
system_daylight_enable='0'
```

Configuring System > Maintenance

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

Configuring the General Settings Tab

Upgrading Firmware



The *Upgrade firmware* area allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.

⚠ **Caution**: Do not power off the Network Camera during the upgrade.

Follow the steps below to upgrade the firmware:

1. Download the latest firmware file using Pelco VxToolbox and/or CCT. The file is in .pkg file format.
2. Click **Choose File**, and then browse to 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”. When this message is displayed, re-access the Network Camera.

If a firmware upgrade is disrupted (for example: by a power outage), you can still restore normal operations.

Applicable scenario:

- Power is disconnected during a firmware upgrade.
- The LED indicates abnormal status for unknown reasons, and a Restore cannot recover normal working conditions.

To activate the camera with its backup firmware:

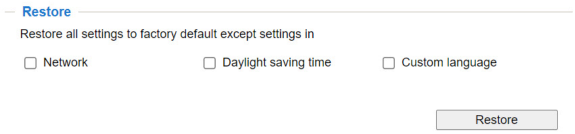
1. Press and hold down the reset button for at least one minute.
2. Power on the camera until the Red LED blinks rapidly.
3. After boot up, the firmware will return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When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

Rebooting the System

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 "The device is rebooting now..." message and status bar are displayed during the reboot process.

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

Restoring the System Settings



Restore all settings to factory default except settings in

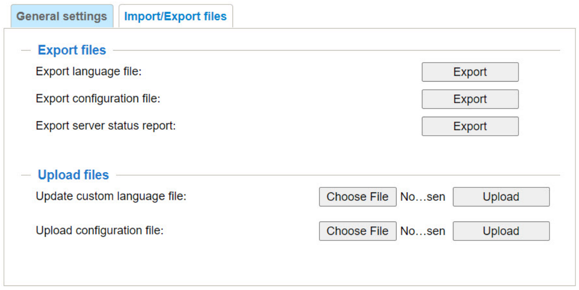
□ Network □ Daylight saving time □ Custom language

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

- *Network*—Select this option to retain the network type settings. See the section titled *Configuring Network > General Settings*.
- *Daylight saving time*—Select this option to retain the daylight saving time settings. See the section titled *Configuring the Import/Export Files Tab*, below.
- *Custom language*—Select this option to retain the custom language settings.

If none of the options is selected, all settings will be restored to factory default. The "The device is rebooting now..." message and status bar are displayed during the restore process.

Configuring the Import/Export Files Tab



Export files

Export language file: Export

Export configuration file: Export

Export server status report: Export

Upload files

Update custom language file: Choose File No...sen Upload

Upload configuration file: Choose File No...sen Upload

In the *Export files* area:

- *Export language file*—Click to export language strings. Pelco provides the following languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.
- *Export configuration file*—Click to export all parameters for the device and user-defined scripts.
- *Export server staus report*—Click to export the current server status report, including: time, logs, parameters, process status, memory status, file system status, network status, and kernel message.

In the *Upload files* area:

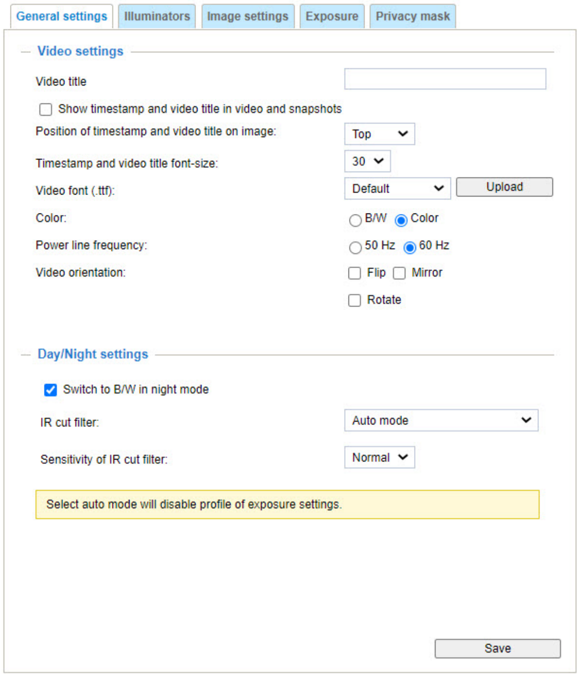
- *Update custom language file*—Click **Choose File**, select the custom language file to upload, and then click **Upload**.
- *Upload configuration file*—Click **Choose File**, select the configuration file to upload, and then click **Upload**..

Note: The model and firmware version of the device must be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, do not update a configuration file.

Configuring Media > Image Settings

This section explains how to configure the image settings of the Network Camera.

Configuring the General Settings Tab



General settings | Illuminators | Image settings | Exposure | Privacy mask

Video settings

Video title:

□ Show timestamp and video title in video and snapshots

Position of timestamp and video title on image: Top

Timestamp and video title font-size: 30

Video font (.ttf): Default | Upload

Color: ○ B/W ● Color

Power line frequency: ○ 50 Hz ● 60 Hz

Video orientation: □ Flip □ Mirror

□ Rotate

Day/Night settings

☑ Switch to B/W in night mode

IR cut filter: Auto mode

Sensitivity of IR cut filter: Normal

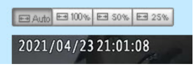
Select auto mode will disable profile of exposure settings.

Save

Configuring Video Settings

In the *Video settings* area:

- *Video title*—Enter a name that will be displayed on the title bar of the live video.
- *Show timestamp and video title in video and snapshots*— The date and time stamp is displayed on the Home page at the location selected in the next field. In the example below, the stamp is displayed at the *Top* left corner of the live view window

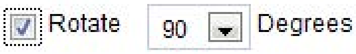


Auto | 100% | 50% | 25%

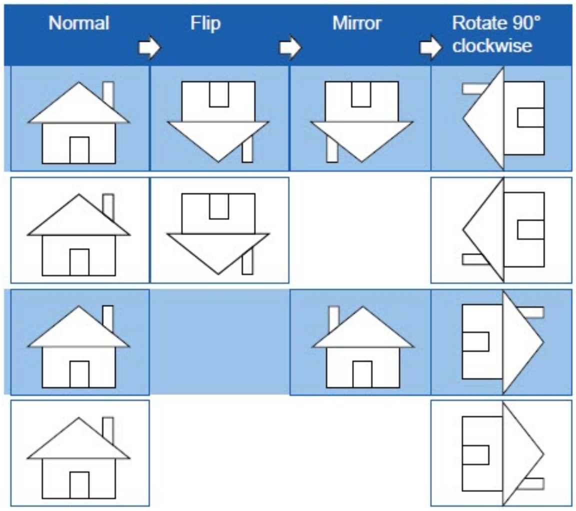
2021/04/23 21:01:08

- *Position of timestamp and video title on image*—Select to display time stamp and video title at 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.
- *Video font (.ttf)*—You can select a True Type font file for the display of text on video.
- *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. 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.
- *Video orientation*:
  - *Flip*—Vertically reflect the display of the live video
  - *Mirror*—Horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (for example: on the ceiling) to correct the image orientation.

- *Rotate*—Rotate the live video clockwise. Rotation can be applied with flip, mirror, and physical lens rotation (see below) settings to adapt to different mounting locations. The figures in the illustration are shown in a consecutive order.



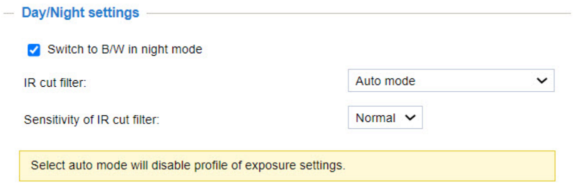
☑ Rotate 90 Degrees



The camera may be installed on a vertical, side-facing, or tilted surface in order to accommodate the interior or exterior design of a building. The interior of a building can be shaped as a narrow rectangular space, such as a corridor. The conventional HD image, such as that of a 16:9 aspect ratio, will be incongruous with its wide horizontal view. With video rotation, the camera can more readily cover the field of view on a tall and narrow scene.

Configuring Day/Night Settings

In the *Day/Night settings* area:



Day/Night settings

☑ Switch to B/W in night mode

IR cut filter: Auto mode

Sensitivity of IR cut filter: Normal

Select auto mode will disable profile of exposure settings.

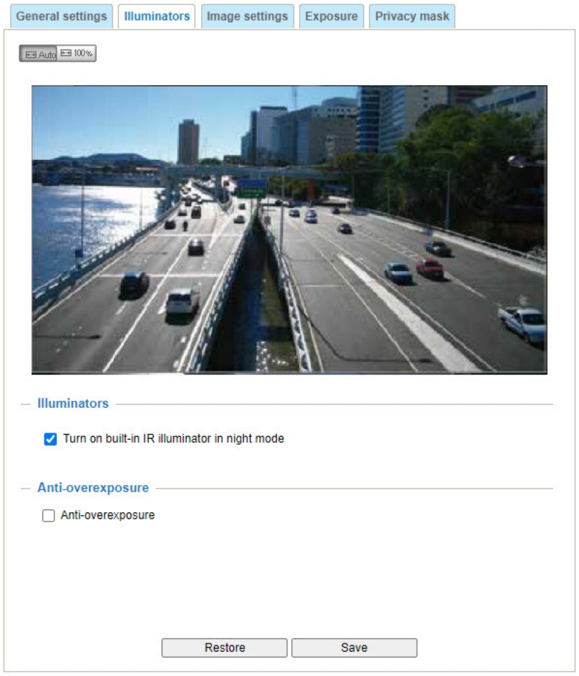
- *Switch to B/W in night mode*—Select this to enable the Network Camera to automatically switch to Black/White during night mode.
- *IR cut filter*—With a removable IR-cut filter, this Network Camera can automatically remove the filter to let Infrared light pass into the sensor during low light conditions.
  - **Auto mode**—(The Day/Night Exposure Profile will not be available if Auto mode is selected) The Network Camera automatically removes the filter by judging the level of ambient light.
  - **Day mode**—In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.
  - **Night mode**—In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

- **Schedule mode**—In Schedule mode, you can select a time range to which *Day mode* settings are enforced. Click to select **Schedule mode**, and then enter the *From* and *To* time range.

- *Sensitivity of IR cut filter*—Tune the responsiveness of the IR filter to lighting conditions as **Low**, **Normal**, or **High**.

When completed with the settings on this page, click **Save** to enable the settings.

Configuring the Illuminators Tab



Illuminators

☑ Turn on built-in IR illuminator in night mode

Anti-overexposure

□ Anti-overexposure

Above the live view area, click the resize buttons to select the display size.

Configuring the Illuminators Settings

In the *Illuminators* area:

- *Turn on built-in IR illuminator in night mode*—Select this to turn on the camera's onboard IR illuminator when the camera detects low light condition and enters the night mode.

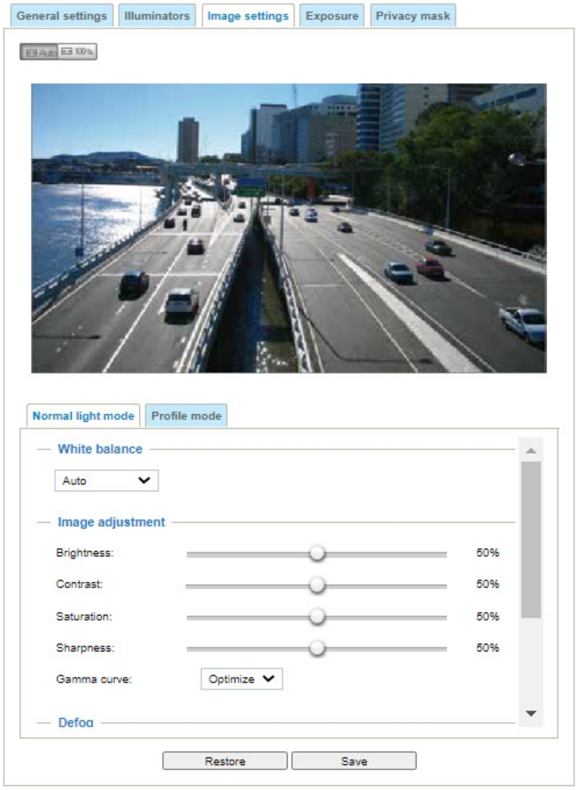
Configuring Anti-overexposure Settings

In the Anti-overexposure area:

- Anti-overexposure—Enable this if you want the camera to automatically adjust the IR projection to adjacent objects, in order to avoid over-exposure in the night mode.

Configuring the Image Settings Tab

Use the *Image settings* page to tune the *Normal light mode* and *Profile mode*.



White balance: Auto

Brightness: 50%

Contrast: 50%

Saturation: 50%

Sharpness: 50%

Gamma curve: Optimize

Configuring the Image Settings > Normal Light Mode

- *White balance*—Adjust the value for 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.
  3. If you chose *Manual*, tune the color temperature by pulling the *RGain* and *BGain* slider 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*—You can let the camera **Optimize** your display or select the **Manual** mode to adjust the image sharpness level, which ranges from 0.45 to 1, from *Detailed* to *Contrast*. For manual mode, use the slider bar 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.

  This option is disabled when the WDR feature is enabled.

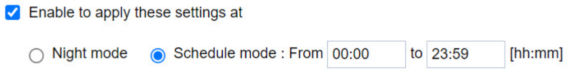
- *Defog*—Defog helps improve the visibility of the captured image in poor weather conditions such as smog, fog, or smoke. If you select *Defog*, adjust the *Strength*.
- *Noise reduction*—Check to enable noise reduction in order to reduce noises and flickers in image. This applies to the onboard 3D Noise Reduction feature. Use the slider bar to adjust the reduction strength.

  Note: Applying this function to the video channel will consume system computing power.

  3D Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of motion can occur. You may then select a lower strength level or disable the function.
- When all settings are correct, click **Save**.

Configuring the Image Settings > Profile Mode

- *Enable to apply these settings at*—Select the mode for this profile: *Night mode* or *Schedule mode*. If you chose the *Schedule mode*, manually enter a range of time.



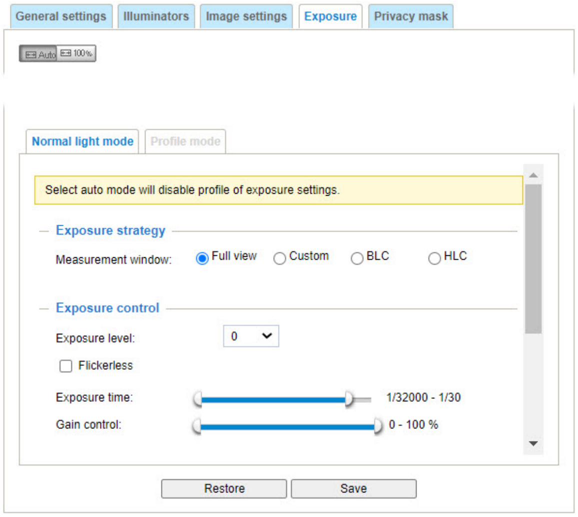
☑ Enable to apply these settings at

○ Night mode ● Schedule mode : From 00:00 to 23:59 [hh:mm]

- Verify settings or change them using the same process as for *Configuring the Image Settings > Normal Light Mode*.
- When all settings are correct, click **Save**.

Configuring the Exposure Tab

On this page, you can configure exposure for two sets of settings: one for normal situations, the other for special situations, such as the night/schedule mode.



Select auto mode will disable profile of exposure settings.

Exposure strategy

Measurement window: ● Full view ○ Custom ○ BLC ○ HLC

Exposure control

Exposure level: 0

□ Flickerless

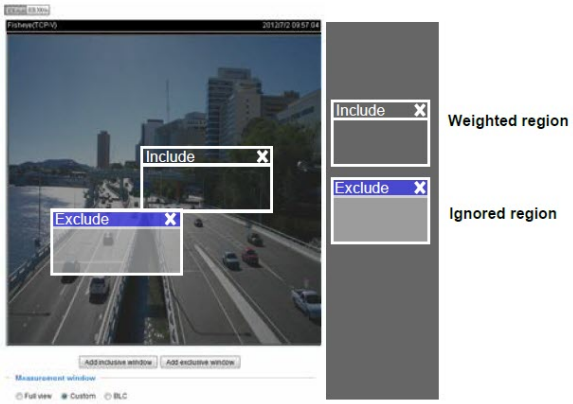
Exposure time: 1/32000 - 1/30

Gain control: 0 - 100 %

Configuring Exposure > Normal Light Mode

- *Exposure strategy*—This function allows users to set *Measurement window*(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background, exclude the bright sunlight shining through a building corridor.
  - Full view—Calculate the full range of view and offer appropriate light compensation.
  - Custom—This option allows you to manually add customized windows as included or excluded regions. A total of 10 windows can be configured. See the detailed illustration, below.

    The included window refers to the “weighted window“; the excluded window refers to “ignored window“. It adopts the weighted averages method to calculate the value. The included windows have a higher priority. You can overlap these windows, and, if you place an excluded window within a larger included window, the excluded part of the overlapped windows will be deducted from the included window. An exposure value will then be calculated out of the remaining of the included window.



Measurement window

○ Full view ● Custom ○ BLC

  - BLC (Back Light Compensation)—This option will automatically add a “weighted region“ in the middle of the window and give the necessary light compensation.
  - HLC (Highlight Compensation)—Firmware detects strong light sources and compensates affected spots to enhance the overall image quality. For example, the HLC helps reduce the glare produced by spotlights or headlights. Using HLC will disable Smart IR; click **OK** in the warning pop-up window.
- *Exposure control*
  - *Exposure level*—You can manually set the *Exposure level*, which ranges from -2.0 to +2.0 (dark to bright).
  - *Flickerless*—Under some circumstances when there is a difference between the video capture frequency and local AC power frequency (NTSC or PAL), the mismatch causes color shifts or flickering images. If the above mismatch occurs, select the *Flickerless* checkbox. When selected, the range of *Exposure time* (the shutter time) will be limited to a range in order to match the AC power frequency; the exposure time will be forced to stay longer than 1/120 second.

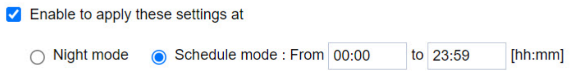
    Note: Setting the exposure time to longer than 1/120 second might introduce too much light into the lens.

  - *Exposure time*—Click and drag the semi-circular pointer on the *Exposure time* slider bar to specify a range of shutter time within which the camera can automatically tune to an optimal imaging result.
  - *Gain control*—Click and drag the semi-circular pointer on the *Gain control* slider bar to specify a range of *Gain control* within which the camera can automatically tune to an optimal imaging result.
- *AE Speed Adjustment*
  - *Enable AE speed adjustment*—Enable this setting to monitor fast changing lighting conditions. For example, use this if the camera monitors a highway lane or entrance of a parking area at night, where cars passing by with their lights on can bring fast changes in light levels.
- *WDR*—This refers to the Wide Dynamic Range function that enables the camera to capture details in a high contrast environment.
  - *Enable True WDR*—Use the checkbox to enable the function and the *Enable WDR Enhancements* function. You can deselect the *Enable WDR Enhancements* function.
  - *Enable WDR enhanced*—This function allows users to identify more image details with greater contrast from an object of interest in scenes with very bright and dark areas, for example: an entrance. Select the *Enable WDR enhanced* checkbox, and then adjust the strength (low, medium, high) to the best image.
- Click **Restore** to recall the original settings without incorporating the changes.
- Click **Save** to enable the settings.

Follow the steps below to set up a profile:

Note: *Profile mode* is not available when the IR cut filter is set to HLC.

- *Enable to apply these settings at*—Select the mode for this profile: *Night mode* or *Schedule mode*. If you chose the *Schedule mode*, manually enter a range of time.



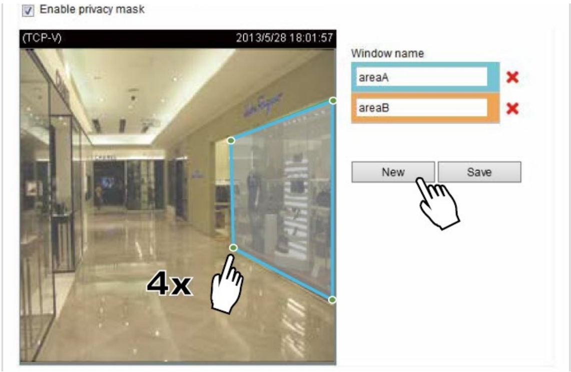
☑ Enable to apply these settings at

○ Night mode ● Schedule mode : From 00:00 to 23:59 [hh:mm]

- Verify settings or change them using the same process as for *Configuring Exposure > Normal Light Mode*.
- To recall the original settings without incorporating the changes, click **Restore**. When completed with the settings on this page.
- Click **Save** to enable the settings.

Configuring the Privacy Mask

Click **Privacy mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.



☑ Enable privacy mask

(TCP-V) 2013/5/28 18:01:57

Window name

areaA

areaB

To configure privacy mask windows:

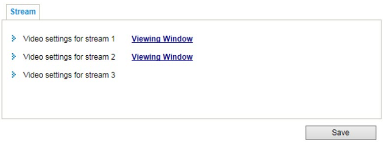
1. Click to select the *Enable privacy mask* checkbox to enable this function.
2. Click **New** to add a new window.
3. You can use 4 mouse clicks to create a new masking window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
4. Enter a *Window name* and click **Save** to enable the setting.

Note: Up to 5 privacy mask windows can be configured on the same screen.

To delete a privacy mask window, click the red x (✖) to the right of the window name.

Configuring Media > Video

Configuring Streams



Stream

Video settings for stream 1 Viewing Window

Video settings for stream 2 Viewing Window

Video settings for stream 3

This Network Camera supports real-time H.265, H.264 and MJPEG compression standards for real-time viewing. If the H.265 or H.264 mode is selected, the video is streamed via RTSP protocol. There are several parameters with which you can adjust the video performance.

This Network Camera supports multiple streams with frame sizes ranging from 480 x 352 to 2560 x 1920 pixels, depending on the model.

- Stream 1—Users can define the "Region of Interest" (viewing region) and the "Output Frame Size" (size of the live view window).
- Stream 2—The default frame size for Stream 2 is set to the 640 x 480.
- Stream 3—The default frame size for Stream 3 is set to the 1920 x 1080.

Click **Viewing Window** to open the viewing region settings page. On this page, you can configure the *Region of interest* for a video stream. That is, you can crop only a portion of the image that is of your interest, and thus save the bandwidth needed to transmit the video stream. For example: The area of your interest in a parking lot should be the vehicles; sky or lawn in an image is of little value.

To view or set up these settings for a stream:

1. Click **Viewing Window** to the right of a stream for which you want to view or set up the viewing region.
2. Select a *Region of interest* from the drop-down menu. The floating frame, the same as the one in the *Global view* window on the home page, will resize accordingly. You can also resize and drag the floating frame to a desired position with your mouse.
3. Choose a proper *Output Frame Size* from the drop-down menu according to the size of your monitoring device.

   Note: All of the items in the *Region of Interest* must not be larger than the *Output Frame Size* (current maximum resolution).

Stream	Region of Interest	Output Frame Size
1	2560 x 1920 ~ 480 x 352 (Selectable)	2560 x 1920 ~ 480 x 352 (Selectable)
2	2560 x 1920 ~ 480 x 352 (Selectable)	2560 x 1920 ~ 480 x 352 (Selectable)
3	Fixed	Fixed

4. Click **Save** to enable the settings, or **Close** to exit the window without saving the settings.
5. Click the stream item to display the detailed information.

Configuring the Frame Size

You can set up different video resolutions for different viewing devices. For example, you can configure 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, or recording the stream to an NVR. Note that a larger frame size takes up more bandwidth.

Configuring the Maximum Frame Rate

This limits the maximum frame rates per second. Set the frame rate higher for smoother video quality and for capturing detail on moving objects in the field of view.

If the power line frequency is set to 50 Hz , the selectable frame rates are 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, 12 fps, 15 fps, and up to 25 fps. If the power line frequency is set to 60 Hz, the selectable frame rates are 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, 12 fps, 15 fps, and up to 30 fps. You can also select **Customize** and manually enter a value. The available frame rates will decrease if you select a higher resolution.

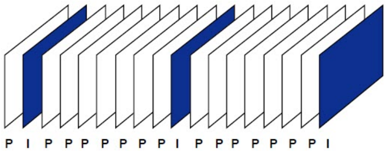
Configuring the Intra Frame Period

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

Configuring Smart Compression—Dynamic Intra Frame Period

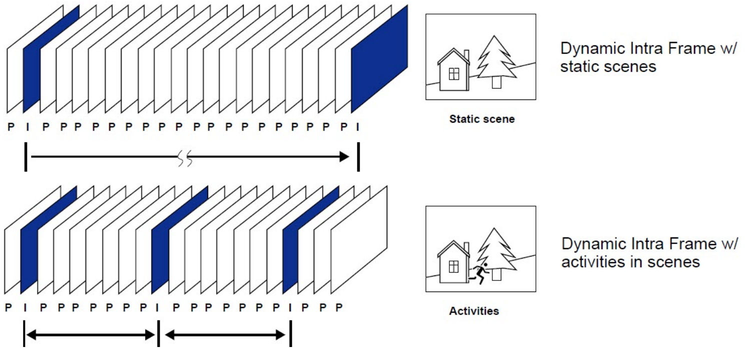
High quality motion codecs, such as H.265, utilize the redundancies between video frames to deliver video streams optimized between image quality and bit rate.

The encoding parameters are summarized and illustrated below. The I-frames are completely self-referential and they are largest in size. The P-frames are predicted frames. The encoder refers to the previous I- or P-frames for redundant image information.



By dynamically prolonging the intervals for I-frames insertion to up to 10 seconds, the bit rates required for streaming a video can be tremendously reduced. When streaming a video of a static scene, the Dynamic Intra frame feature can save up to 53% of bandwidth. The amount of bandwidth thus saved is also determined by the extent of motion in the field of view. If motion occurs in the scene, firmware automatically shortens the I-frame intervals in order to maintain image quality. In low light or at night , the sizes of P-frames tend to be larger due to noise, resulting in lower bandwidth.

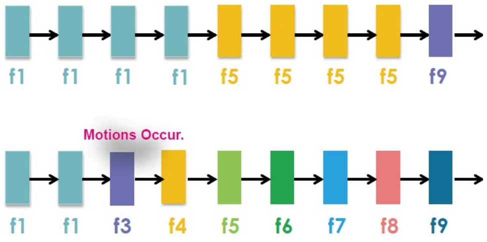
Streaming a typical scene with an average level of motion at 2 MP normally requires 3~4 Mb/s of bandwidth. With the Dynamic Intra frame function, the bandwidth can be reduced to 2~3 Mb/s, and during times when there is no motion, down to 500 kb/s.


P I P P P P P P P P P P P P P P P P P P P I
Static scene
Dynamic Intra Frame w/ static scenes
P I P P P P P P I P P P P P P I P P P
Activities
Dynamic Intra Frame w/ activities in scenes

With the H.265 codec in an optimal scenario and when Dynamic Intra frame is combined with the Smart Stream function, 80% of bandwidth saving can be achieved compared to using H.264 without these bandwidth-saving features.

Configuring Smart FPS

In a static scene, the algorithm puts old frames in queue when no motion occurs in the scene. When motion occurs, the encoding returns to normal to deliver real-time streaming.



This reduces both the computing efforts and the size of P-frames, while maintaining the frame rate.

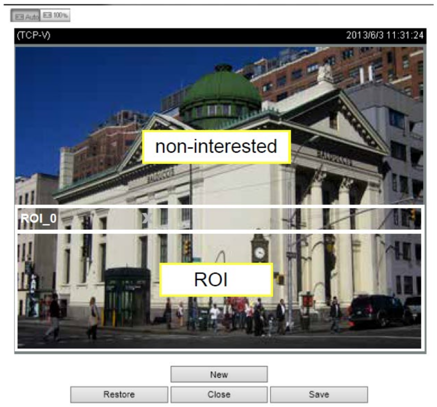
Configuring the Region of Interest

The Region of Interest effectively reduces the quality of areas in the scene that are not critical, and therefore reduces the bandwidth consumed. You can manually specify the video quality for the foreground and the background areas.

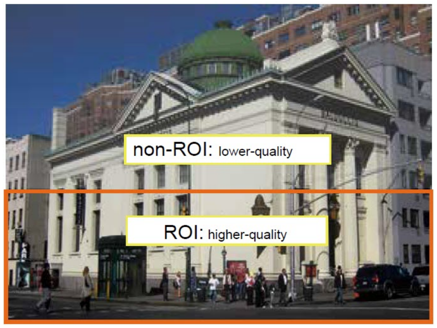
Select an operation mode if the Region of Interest is preferred.

- *Hybrid*—The major difference between the Manual mode and the Hybrid mode is that in the Hybrid mode, any objects entering the areas of less interest will restore the video quality of the moving objects and the area around them. In the Manual mode, the areas of less interest are always transmitted using a low-quality format regardless of the motion in that part of the scene.
- *Quality priority*—Use the slider to set the difference in image quality levels between the ROI and areas of less interest. The farther the slider is to the right, the higher the image quality of the ROI areas. The farther the slider is to the left, the higher the image quality of the areas.

  You should also select the *Maximum bit rate* from the pull-down menu as the threshold for bandwidth consumption for both the high- and low-quality areas in a smart stream.
- *Auto tracking*—The Auto mode configures the whole field of view as the area over which to optimize for bandwidth. The video quality of part of the screen returns to normal when one or more objects move in that area. The remainder of the screen where there are no moving objects will be transmitted at lower image quality for bandwidth savings.
- *Manual*—The Manual mode allows you to configure 3 ROI windows (Region of Interest, with Foreground quality) on the screen. Areas not included in any ROI windows will be considered areas that can be optimized for lower bandwidth and lower image quality. The details in the ROI areas will be transmitted at higher image quality. As illustrated below, the area in the upper part of the screen is of less interest, while the sidewalk on the lower part of the screen is included in a Region of Interest window.



As a result, the lower screen is constantly transmitted in high detail, while the upper half is transmitted with lower image quality. You still have awareness of what is happening across the whole screen.



Configuring Bit Rate Control

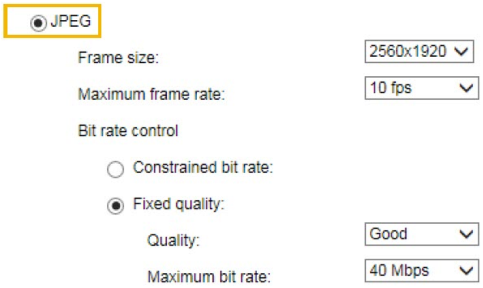
Constrained bit rate—A complex scene generally produces a larger file size, requiring a higher bandwidth for data transmission. The bandwidth utilization is configurable to not exceed a selectable cap. The constrained values are selectable at the following rates: 20 Kbps, 30 Kbps, 40 Kbps, 50 Kbps, 64 Kbps, 128 Kbps, 256 Kbps, 512 Kbps, 768 Kbps, 1 Mbps, 2 Mbps, 3 Mbps, 4 Mbps, 6 Mbps, 8 Mbps, 10 Mbps, 12 Mbps, 14 Mbps, ~ to 40 Mbps. You can also select *Customize* and manually enter a value up to 40 Mbps.

- *Target quality*—Select a desired image quality ranging from *Medium* to *Excellent*.
- *Maximum bit rate*— select a bit rate from the pull-down menu. The bit rate ranges from 20 kbps to a maximum of 40 Mbps. The bit rate then becomes the Upper bound bit rate number. The Network Camera will strive to deliver video streams 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 the image quality will be compromised. If Image quality priority is selected, the Network Camera might drop some video frames in order to maintain image quality level.
- *Smart Q*—Select **ON** or **OFF** to enable or disable the feature. Smart Q is scene-aware. It reduces frame size and bit rate consumption by:
  - Dynamically adjusting the image quality for scenes in different luminosities in low light frames. Lower-noise scenes consume less bandwidth.
  - Setting different image qualities for the I-frames and P-frames, therefore reducing the frame size.
  - Dividing a single frame into different sections, and giving these sections different qualities. For a highly complex area, such as an area with dense vegetation, screen windows, or repeated patterns (complex textiles patterns like wall paper), having a lower quality value is not noticeable to the human eye.

  Smart Q streaming can save up to 80% of bandwidth in different illumination conditions while keeping the same perceived imaging quality.
- *Fixed Quality*:
  - If *Fixed quality* is selected, all frames are transmitted with the same quality; bandwidth utilization can vary unpredictably. The video quality can be set to: *Medium*, *Standard*, *Good*, *Detailed*, and *Excellent*. You can also select *Customize* and manually enter a value.
  - With a fixed image quality, you might still want to place a bit rate constraint to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1 Mbps to 40 Mbps. The *Maximum bit rate* setting in the *Fixed quality* configuration can ensure a reasonable and bounded use of network bandwidth. For example, in low light conditions where a *Fixed quality* setting is applied, video packet sizes can vary tremendously if they are not capped by bit rate constraint. You may also manually enter a bit rate number by selecting the **Customized** option.

Selecting and Configuring JPEG Mode

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.



● JPEG

Frame size: 2560x1920

Maximum frame rate: 10 fps

Bit rate control

○ Constrained bit rate:

● Fixed quality:

Quality: Good

Maximum bit rate: 40 Mbps

There are three parameters provided in MJPEG mode to control the video performance:

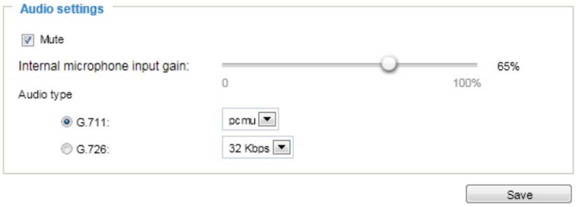
- *Frame size*—You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more 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 50 Hz (at the 5MP resolution), the frame rates are selectable at 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, and 15 fps. If the power line frequency is set to 60 Hz, the frame rates are selectable at 1 fps, 2 fps, 3 fps, 5 fps, 8 fps, 10 fps, and 15 fps. For 2 MP models, there are three additional frame rates: 12.5 fps, 25 fps, and 30 fps. 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 H.264.

For *Constant Bit Rate* and other settings, see the section titled *Configuring Bit Rate Control*.

Note: Video quality and fixed quality refer to the compression level, so a lower value will produce higher quality. High-quality video can significantly increase the CPU load, and you might encounter streaming disconnection or video loss while capturing a complicated scene. If this occurs, reduce the video resolution and/or frame rate to obtain smooth video.

Configuring Media > Audio



Audio settings

☑ Mute

Internal microphone input gain: 65%

Audio type

● G.711: pcmu

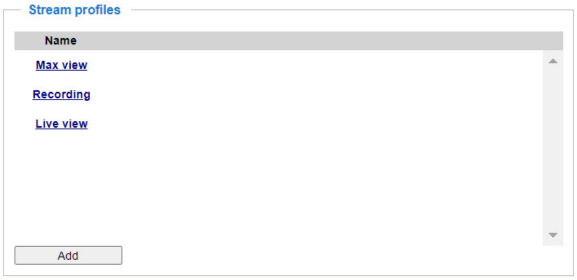
○ G.726: 32 Kbps

- *Mute*—Select this option to disable audio transmission from the Network Camera to all clients.
- *Internal microphone input gain*—Select the gain of the external audio input according to ambient conditions. Adjust the gain from 0% to 100%.
- *Audio type*—Select audio codec and the sampling bit rate.

- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

- Click **Save** to enable the settings.

Configuring Media > Media Profiles



Media profiles, called *Stream profiles*, are selected on the **Home** page, at the top of the Camera configuration panel. They are configured on the **Configuration > Media > Media profiles** page.

The three default profiles are *Max view*, *Recording*, and *Live view*. You can change the existing profile names and settings, and add new profiles. The profiles are associated with streams that were configured in the sections titled *Configuring Media > Audio*, *Configuring Media > Video*, and *Configuring Network > Streaming Protocols*

1. Click the profile name to select an existing profile to edit, or click **Add** to create a new one.
2. In the *Profile name* field:
   - To change an existing profile name or to create a name for a new profile, type the name.
   - To retain an existing profile name, do nothing.
3. Click to select or deselect the checkbox for *Always multicast for this stream profile*.
4. In the *Video configuration* area:
   a. For a new profile, if appropriate, click to select the checkbox for *Setup a video configuration*.
   b. For an existing profile, click to select or deselect the checkbox for *Setup a video configuration*.
   c. If you selected the checkbox, select the *Stream No* from the drop-down menu.
5. In the *Audio configuration* area:
   a. For a new profile, if appropriate, click to select the checkbox for *Setup an audio configuration*.
   b. For an existing profile, click to select or deselect the checkbox for *Setup an audio configuration*.
6. In the *Metadata configuration* area:
   a. For a new profile, if appropriate, click to select the checkbox for *Setup a metadata configuration*.

   b. For an existing profile, click to select or deselect the checkbox for *Setup a metadata configuration*.

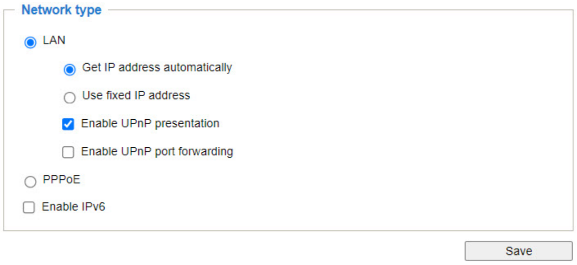
7. Click **Save** to enable the settings, or click **Close** to exit the window without saving.
8. Click **Close** to exit this window.
9. To delete a profile, click **Delete** to the right of the profile name.

   You can only delete an added profile; you cannot delete a default profile.

Configuring Network > General Settings

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

You can use LAN or PPPoE settings. You can also enable the use of IPv6.



Network type

● LAN

● Get IP address automatically

○ Use fixed IP address

☑ Enable UPnP presentation

☐ Enable UPnP port forwarding

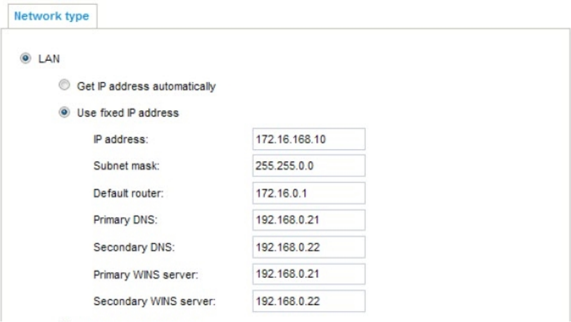
○ PPPoE

☐ Enable IPv6

Configuring LAN Settings

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.

- *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.



Network type

● LAN

○ Get IP address automatically

● Use fixed IP address

IP address:	172.16.168.10
Subnet mask:	255.255.0.0
Default router:	172.16.0.1
Primary DNS:	192.168.0.21
Secondary DNS:	192.168.0.22
Primary WINS server:	192.168.0.21
Secondary WINS server:	192.168.0.22

– Enter the values, provided by your ISP or network administrator, in each field.

- 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 hostnames 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.

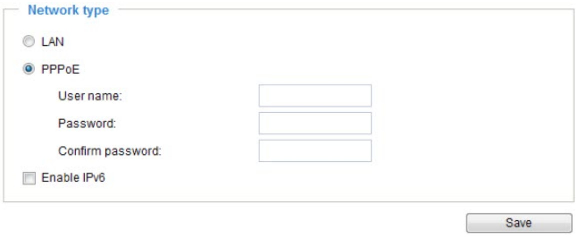
- *Enable UPnP presentation*—Select this option to enable UPnPTM presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, the shortcuts to connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnPTM is supported by Windows XP or later. Ensure that the UPnPTM component is installed on your computer.
- *Enable UPnP port forwarding*—To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnPTM and it is activated.

Configuring 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. This feature 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 Configuration > Event > Event settings > Add server (see the section titled *Configuring Event > Event*) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (see the section titled *Configuring Event > Event*) to add media.
4. 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.
5. Go to Configuration > Network > General settings > Network type.
6. Select *PPPoE* and enter the user name and password provided by your ISP.



Network type

○ LAN

● PPPoE

User name:

Password:

Confirm password:

□ Enable IPv6

7. Click **Save** to enable the setting.
8. When the Network Camera reboots, disconnect the power to the Network Camera and 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.

If UPnPTM is not supported by your router, you will see the message "Error: Router does not support UPnP port forwarding." To enable the UPnPTM user interface on your computer:

1. Log on to the computer as a system administrator to install the UPnPTM components.
2. Go to Start, click Control Panel, then click Add or Remove Programs.
3. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components Wizard dialog box, select Networking Services and click Details.
5. In the Networking Services dialog box, select Universal Plug and Play and click OK.
6. Click Next.
7. Click Finish.

UPnPTM 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.

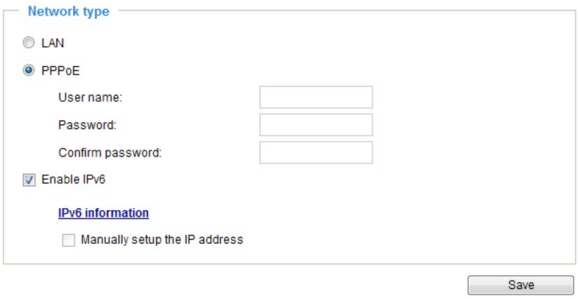
- From the Internet, use http://203.67.124.123:8080.
- In LAN, use either http://192.168.4.160 or http://192.168.4.160:8080.

If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default. See the section titled *Configuring System > Maintenance*. After the Network Camera is reset to factory default, it will be accessible on the LAN.

Enabling IPv6

Note: This section only applies to network environments and hardware equipment that support IPv6. Supported browsers are Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

1. Click to select the checkbox for *Enable IPv6*.



Network type

○ LAN

● PPPoE

User name:

Password:

Confirm password:

☑ Enable IPv6

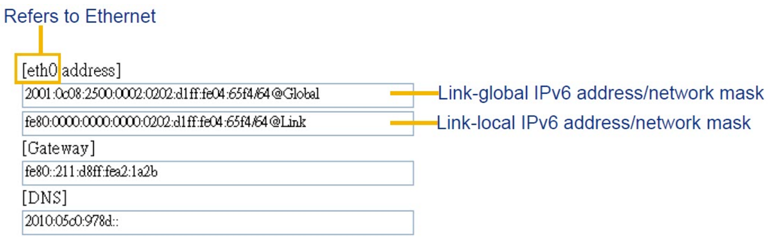
IPv6 information

□ Manually setup the IP address

Save

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

2. Click **IPv6 information**. 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 shown in the image below.


Refers to Ethernet
Link-global IPv6 address/network mask
Link-local IPv6 address/network mask

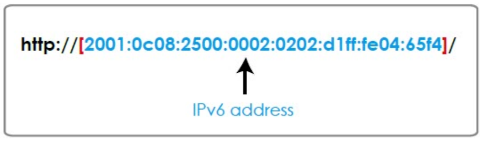
[eth0 address]
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link
[Gateway]
fe80::211:d8ff:fea2:1a2b
[DNS]
2010:05c0:978d::

3. To link to an IPv6 address:

   a. Open your web browser.

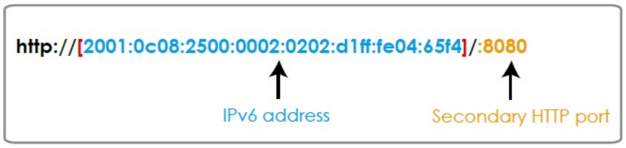
   b. Enter the link-global or link-local IPv6 address in the address bar of your web browser. Use one of the formats shown below.

      - Primary port.



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

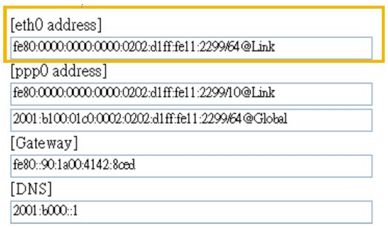
      - Secondary HTTP port (default value 8080)



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

   c. Press Enter on the keyboard or click **Refresh** to refresh the webpage.

   If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information area 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

4. Select *Manually setup the IP address* 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, enter the information in the following fields:

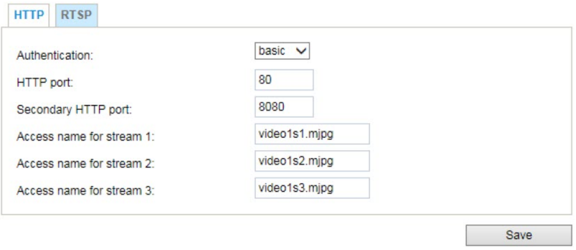
   - *Optional IP address / Prefix length*
   - *Optional Default router*
   - *Optional primary DNS*

When you have configured this page, click **Save**.

Configuring Network > Streaming Protocols

Configuring HTTP Streaming

To use HTTP authentication, ensure that your have set a password for the Network Camera first. See the section titled *Configuring Security > User Accounts*.



Authentication: basic

HTTP port: 80

Secondary HTTP port: 8080

Access name for stream 1: video1s1.mjpg

Access name for stream 2: video1s2.mjpg

Access name for stream 3: video1s3.mjpg

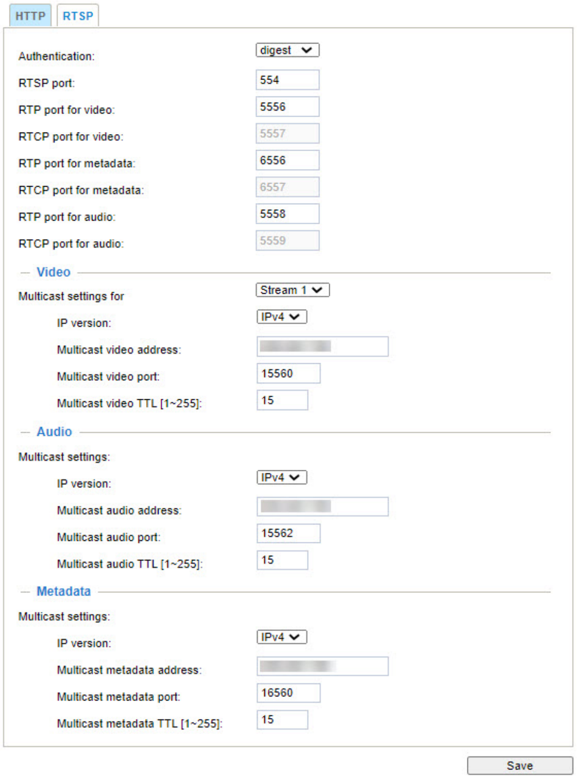
- *Authentication*—Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. 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, a warning dialog box is 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, the LAN is at http://192.168.4.160 or http://192.168.4.160:8080.
- *Access name for stream 1 ~ 3*
  - This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. 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, see the section titled *Configuring Media > Video*.
  - 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.
  - Use the URL command "http://<ip address>:<http port>/<access name for stream 1, 2, 3>". For example, when the Access name for stream 2 is set to video1s2.mjpg:

    1. Launch Mozilla Firefox.
    2. Type the above URL command in the address bar.
    3. Press Enter.

    The JPEG images will be displayed in your web browser.

Configuring RTSP Streaming

To use RTSP streaming authentication, ensure that you have set a password for controlling the access to video stream first. See the section titled *Configuring Security > User Accounts*.



Authentication:	digest
RTSP port:	554
RTP port for video:	5556
RTCP port for video:	5557
RTP port for metadata:	6556
RTCP port for metadata:	6557
RTP port for audio:	5558
RTCP port for audio:	5559
Video	
Multicast settings for	Stream 1
IP version:	IPv4
Multicast video address:	[redacted]
Multicast video port:	15560
Multicast video TTL [1~255]:	15
Audio	
Multicast settings:	
IP version:	IPv4
Multicast audio address:	[redacted]
Multicast audio port:	15562
Multicast audio TTL [1~255]:	15
Metadata	
Multicast settings:	
IP version:	IPv4
Multicast metadata address:	[redacted]
Multicast metadata port:	16560
Multicast metadata TTL [1~255]:	15

- *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 via VLC for the three authentication modes is listed below.
  - Disable mode: Yes
  - Basic mode: Yes
  - Digest: No
- Real-Time Streaming Protocol (RTSP), Real-time Transport Protocol (RTP), and Real-time Transport Control Protocol (RTCP) ports:
  - *RTSP port* controls the delivery of streaming media. By default, the port number is set to 554.
  - *RTP port for video*, *RTP port for metadata*, and *RTP fort for audio* are used to deliver data to the clients. By default, the *RTP port for video* is set to 5556, for metadata is set to 6556, and for audio is set to 5558.
  - *RTCP port for video*, *RTCP port for metadata*, and *RTCP port for audio* allow the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the *RTCP port for video* is set to 5557, for metadata is set to 6557, and 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, a warning dialog box is displayed.

When the RTP port changes, the RTCP port will change accordingly.

- In the *Video* area:
  - *Multicast settings for*—Select a stream from the drop-down menu.
  - *IP version*—Select **IPv4** or **IPv6** from the drop-down menu.
  - *Multicast video address*—Type in the correct URL.
  - *Multicast video port*—Type in the correct port number, following the guidelines above.
  - *Multicast video 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
225	Unrestricted in scope

- In the *Audio* area:
  - *Multicast settings for*—Select a stream from the drop-down menu.
  - *IP version*—Select **IPv4** or **IPv6** from the drop-down menu.
  - *Multicast audio address*—Type in the correct URL.
  - *Multicast audio port*—Type in the correct port number, following the guidelines above.
  - *Multicast audio TTL [1~255]*—The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded. See the table above for Initial TTL and Scope correspondences.
- In the *Metadata* area:
  - *Multicast settings for*—Select a stream from the drop-down menu.
  - *IP version*—Select **IPv4** or **IPv6** from the drop-down menu.
  - *Multicast metadata address*—Type in the correct URL.
  - *Multicast metadata port*—Type in the correct port number, following the guidelines above.

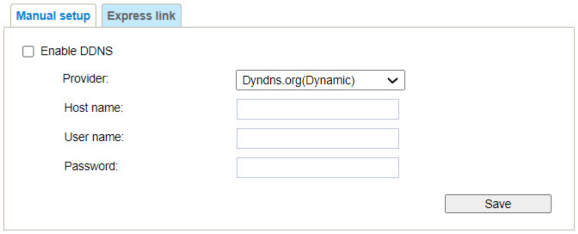
    ⚠ **Caution**: The Multicast metadata port is to transfer video analytics results, PTZ stream, textual data, and event messages between the camera and the client side running and observing the video analysis. If your client side computer is located outside the local network, you might need to open the associated TCP port on routers and firewall.
  - *Multicast metadata TTL [1~255]*—The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded. See the table above for Initial TTL and Scope correspondences.
- Click **Save**.

Configuring Network > DDNS

This section explains how to configure the dynamic domain name service (DDNS) 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.

Configuring Network > DDNS Manually

1. Click **Manual setup**.



□ Enable DDNS

Provider: Dyndns.org(Dynamic)

Host name:

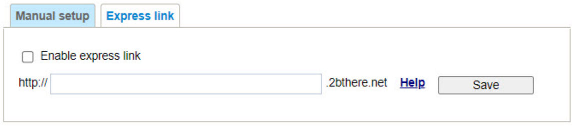
User name:

Password:

2. Click to select the checkbox for *Enable DDNS*.
3. To apply for a dynamic domain account, access Dyndns.org(Dynamic) / Dyndns.org(Custom) at http://www.dyndns.com/.
4. Select a DDNS *Provider* from the provider drop-down menu. The options are:
   - Dyndns.org(Dynamic)
   - Dyndns.org(Custom)
5. Type a *Host name*, *User name*, and *Password* in the appropriate fields.
6. Click **Save**.

Configuring Network > DDNS Using Express Link

Express link is a free service 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.



□ Enable express link

http:// .2bthere.net

To enable **Express link**:

1. Verify that your router supports UPnP port forwarding and that 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 stating "The camera can now be accessed at [URL]".

Configuring Network > QoS

Quality of Service (QoS) 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.

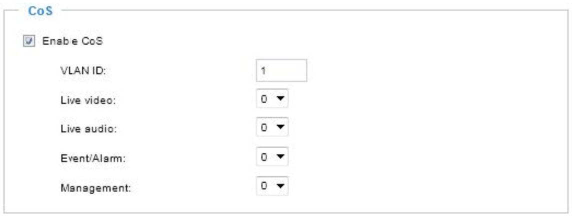
To use QoS in a network environment, the following requirements must be met:

- 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.

Using 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 area for CoS. Click to select the checkbox for *Enable CoS*, enter the *VLAN ID* of your switch (0~4095), and choose the priority for each application (0~7). When you have completed these settings, click **Save**.



CoS

☑ Enable CoS

VLAN ID:	1
Live video:	0
Live audio:	0
Event/Alarm:	0
Management:	0

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

Note: A VLAN Switch (802.1p) is required. Web browsing might fail if the CoS setting is incorrect.

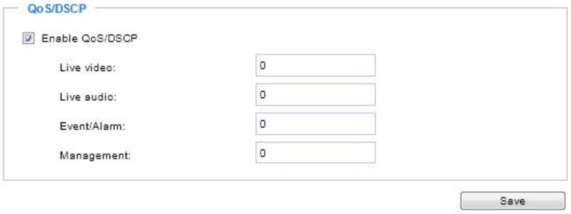
Note: The Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.

Note: Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees because it is based on L2 protocol.

Using 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). Click to select the checkbox for *Enable QoS/DSCP*, and specify the DSCP value for each application (0~63). When you have completed these settings, click **Save**.



QoS/DSCP

☑ Enable QoS/DSCP

Live video: 0

Live audio: 0

Event/Alarm: 0

Management: 0

Note: Different vendors of network devices might have different methodologies and unique implementations. You should enter a DSCP tag value according to the information provided by the network devices.

Below are the QoS Baseline/Technical Marketing Classification and Marking Recommendations.

Application	Layer 3 Classification			Layer 2 Classification	
	IPP	PHB	DSCP	CoS	MPLS EXP
IP Routing	6	CS6	48	6	—
Voice	5	EF	46	5	—
Interactive Video	4	AF41	34	4	QoS B
Streaming-Video	4	CS4	32	4	—
Locally-defined Mission- Critical Data	3	—	25	3	—
Call-signaling	3	AF31/CS3	26/24	3	—
Transactional Data	2	AF21	18	2	—
Network Management	2	CS2	16	2	—
Bulk Data	1	AF11	10	1	—

Configuring Network > SNMP

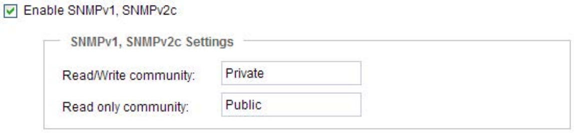
This section explains how to use the Simple Network Management Protocol (SNMP) on the network camera. The SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find,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

The SNMP consists of the following three key components:

- Manager—Network-management station (NMS), a server which executes applications that monitor and control managed devices.
- Agent—A network-management software module on a managed device which transfers the status of managed devices to the NMS.
- 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.

Caution: Before configuring SNMP settings on the this page, enable your NMS.

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



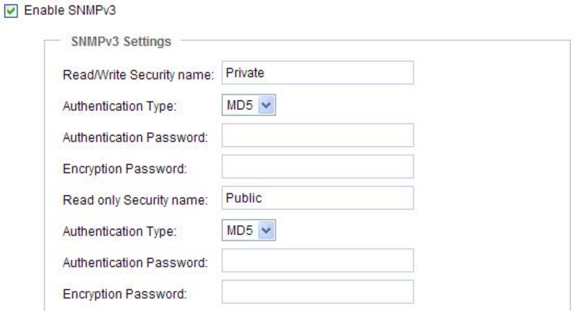
☑ Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community: Private

Read only community: Public

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



☑ Enable SNMPv3

SNMPv3 Settings

Read/Write Security name: Private

Authentication Type: MD5

Authentication Password:

Encryption Password:

Read only Security name: Public

Authentication Type: MD5

Authentication Password:

Encryption Password:

  - *Read/Write security name*—Type in 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).
  - *Read only security name*—Type in 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).

- Click **Save**.

Configuring Network > Bonjour

Click to select the checkbox for *Enable Bonjour*, enter the appropriate value in the *Service name* field, and then click **Save**.

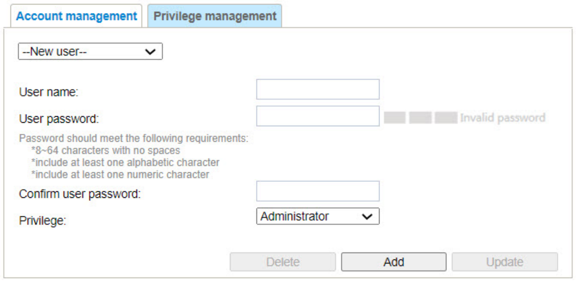
Bonjour is Apple's implementation of zero-configuration networking. Bonjour uses multicast Domain Name System (mDNS) service records to discover devices and services on a LAN, assign IP addresses, and resolve hostnames.

- Bonjour will be useful if you have a PC together with an iPhone or Apple TV.
- If Apple devices such as MacBooks or iPhones are not in use in your environment, you most likely do not need Bonjour.

Configuring Security > User Accounts

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

Configuring Account Management



--New user--

User name:

User password:

Password should meet the following requirements:
*8~64 characters with no spaces
*include at least one alphabetic character
*include at least one numeric character

Confirm user password:

Privilege: Administrator

Caution: The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the *Account management* window, apply the password for the “root” account first.

The administrator can create up to 20 user accounts.

To create a new user:

1. Click to select **New user** from the drop-down menu.
2. Type in the new *User name* and *User password*, and then retype the password in the *Confirm user password* field.

   Some, but not all special ASCII characters are supported: !, $, %, -, ., @, ^, _, and ~. You can use them in the password combination.

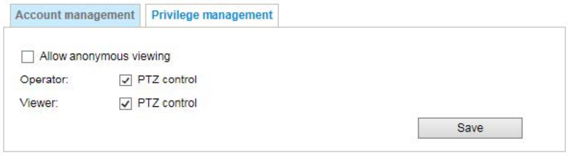
   The strength of your password combination is shown on the right, use the combination of alphabetic, numeric, upper case, and lower case characters until the password strength is good enough.
3. Select the privilege level for the new user account. The privilege levels are:
   - **Administrator**—Full control
   - **Operator**—View live video, listen and talk through the camera interface, take snapshots, and use the URL Commands to get and set the value of parameters; unable to enter the camera Configuration page.
   - **Viewer**—View live video, listen and talk through the camera interface, and take snapshots; unable to enter the camera Configuration page.

   Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the **Configuration** page. Viewers can only access the main page for live viewing.
4. Click **Add** to enable the setting.
5. To change a user’s access rights or delete user accounts:

   a. Select an existing account to modify.

   b. Make necessary changes and click **Update** or **Delete** to enable the setting.

Configuring Privilege Management



□ Allow anonymous viewing

Operator: ☑ PTZ control

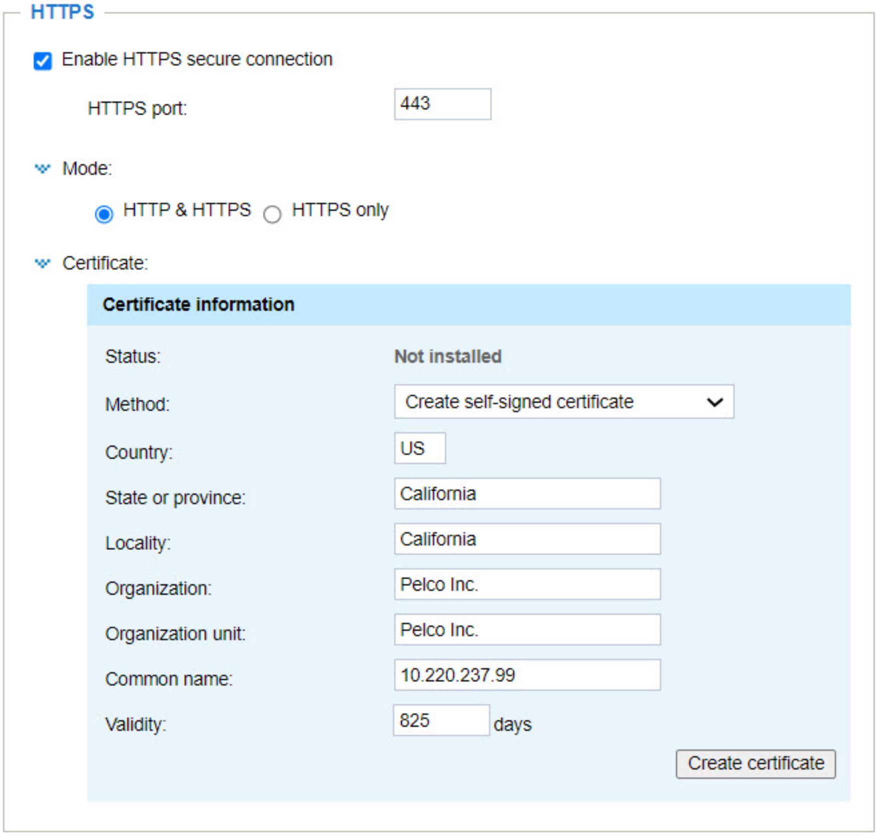
Viewer: ☑ PTZ control

In the *Previlege management* tab:

1. Click to select or deselect the checkbox for *Operator PTZ control*, and for *Viewer PTZ Control*.
2. Click **Save**.

Configuring Security > HTTPS

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.



☑ Enable HTTPS secure connection

HTTPS port: 443

Mode:

● HTTP & HTTPS ○ HTTPS only

Certificate:

Certificate information

Status:	Not installed
Method:	Create self-signed certificate
Country:	US
State or province:	California
Locality:	California
Organization:	Pelco Inc.
Organization unit:	Pelco Inc.
Common name:	10.220.237.99
Validity:	825 days

To configuring HTTPS:

1. Click to select the checkbox for *Enable HTTPS secure connection*.
2. Type in the *HTTPS port*.
3. Click to select the radio button for the appropriate *Mode*: *HTTP & HTTPS* or *HTTPS only*.
4. Create and install a certificate using one of the following methods, described in the sections below.

- Create self-signed certificate (See the section titled *Creating a Self-Signed Certificate*.)
- Create certificate request and install (See the section titled *Creating and Installing a Certificate Request*.)

Creating a Self-Signed Certificate

1. Select this option from the *Method* pull-down menu.
2. Enter the appropriate value in the *Country*, *State or province*, *Locality*, *Organization*, and *Organization unit* fields.
3. Enter a string in the *Common name* field (for example: the URL).
4. Enter a number of days in the *Validity* field.
5. Click **Create certificate** to generate a certificate.

   The Certificate Information will automatically be displayed.
6. Click **Certificate properties** to view detailed information about the certificate.
7. (Optional) To remove the certificate, click **Remove certificate**.
8. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
9. If your web session does not automatically change to an encrypted HTTPS session:
   a. Click **Home** to return to the home page.
   b. Change the URL address from “http://” to “https://“ in the address bar and press Enter on your keyboard.
   c. In the *Security Alert* and *Security Information* dialog boxes, click **OK** or **Yes** to enable HTTPS.

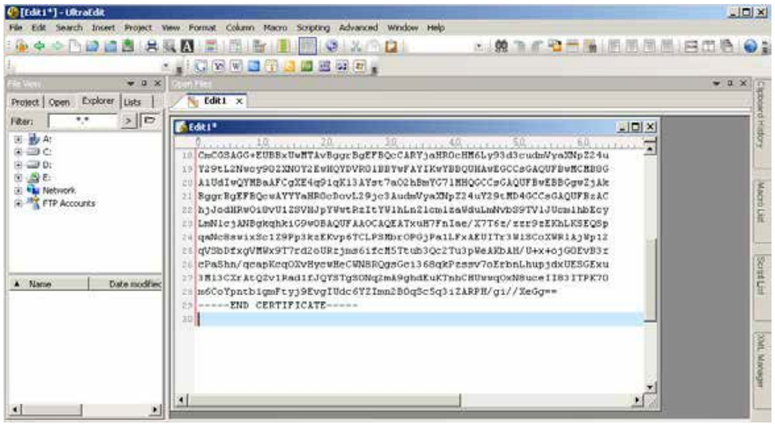
Creating and Installing a Certificate Request

1. Select the option from the *Method* pull-down menu.
2. Enter the appropriate value in the *Country*, *State or province*, *Locality*, *Organization*, and *Organization unit* fields.
3. Enter a string in the *Common name* field (for example: the URL).
4. Enter a number of days in the *Validity* field.
5. Click **Create certificate** to generate a certificate.

   The Certificate Information will automatically be displayed.
6. The "Please wait..." status box will appear. When the certificate has been generated, click **Save**. The *Certificate request* window is displayed.
7. If you see an Information bar at the top of the window, click **OK**, and then click on the Information bar at the top of the page to allow pop-ups.
8. 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 Certificate Authority's (CA’s) signing request window. Proceed with the rest of the CA's process as instructed on their webpage.

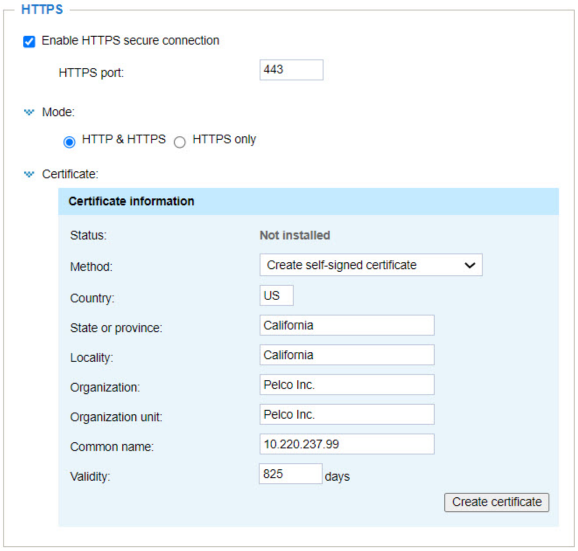
   When this is complete, your SSL certificate will be delivered to you via an email or other means.

9. 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.
10. Open a new file, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.


[Edit1*] - UltraEdit
File Edit Search Insert Project View Format Column Macro Scripting Advanced Window Help
Project Open Explorer Lists
Filter: *.*
A:
C:
D:
E:
Network
FTP Accounts
Name
Date modified
Edit1
Edit1*

```
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy9O2XNOY2EwHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBOG
A1UdIwQYMBaAFCgXE4q91qKi3AYst7aO2hBmYG71MHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU1ZSVHJpYWwtRzItYW1hLn2icmlzaWduLmNvbS9TV1JUcmlhbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp
qaMc8swixSc1Z9Pp3kzEKvp6TCLPSMbrOPGjPa1LFxAKUITr3W1SCoXWR1AjWp1Z
qVSbDfxgVMWx9T7rd2oURzjms6ifcM5Ttub3Qc2Tu3pWeAKbAM/U+x+ojGOEvB3r
cPaShn/qcapKcqOXvHycwHeCWNBRQgsGc1368qkPzssv7oErbnLhupjdxUESGExu
3M13CXrAtQ2v1Rad1fJQYSTgSONq2mA9ghdKuKTnbCHUwwqOxN8uceII831TPK70
m6CoYpntbigmFtyj9EvgIUdc6YZImn2BOqSc5q3iZARPH/gi//XeGg==
-----END CERTIFICATE-----
```

11. Convert the file format from DOS to UNIX. To do so, select **Open File menu > Conversions > DOS to Unix**.
12. Save the file using the ".crt" extension. For example: save the file as "CAcert.crt."
13. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.



☑ Enable HTTPS secure connection

HTTPS port: 443

Mode:

● HTTP & HTTPS ○ HTTPS only

Certificate:

Certificate information

Status:	Not installed
Method:	Create self-signed certificate
Country:	US
State or province:	California
Locality:	California
Organization:	Pelco Inc.
Organization unit:	Pelco Inc.
Common name:	10.220.237.99
Validity:	825 days

14. When the certificate file is successfully loaded, its status will be *Active*.

Note: A certificate must have been created and installed before you can click on the "Save" button for the configuration to take effect.

15. To open an encrypted HTTPS session:

a. Click Home to return to the main page.

b. Change the URL address from “http://” to “https://“ in the address bar and press Enter on your keyboard.

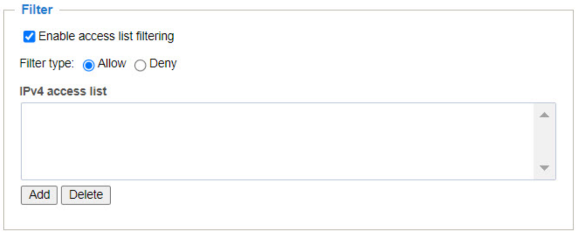
c. In the *Security Alert* and *Security Information* dialog boxes, click **OK** or **Yes** to enable HTTPS.

Configuring Security > Access List

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

Configuring the 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*, only those clients whose IP addresses are on the access list below can access the Network Camera, and the others cannot.
  - If you choose *Deny*, those clients whose IP addresses are on the access list will not be allowed to access the Network Camera, and the others can.



Filter

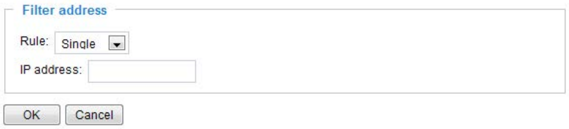
☑ Enable access list filtering

Filter type: ● Allow ○ Deny

IPv4 access list

The IPv4 field/list is always available; the IPv6 field/list will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, see the section titled *Configuring Network > General Settings*.

- Click **Add**, to add a rule to the access list.
  - *Single*—This rule allows the user to add an IP address to the allowed/denied list.



Filter address

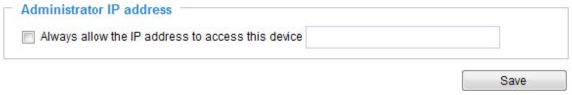
Rule: Single

IP address:

  - *Network*—This rule allows the user to assign a *Network address* and corresponding *Network mask* to the allow/deny list. The address and network mask are written in CIDR format.

    If the IPv6 filter is preferred, you will be prompted to enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.
  - *Range*—This rule only applies to IPv4 addresses and it allows the user to assign a range of IP addresses to the allow/deny list.

Configuring the Administrator IP Address



Administrator IP address

☐ Always allow the IP address to access this device

Save

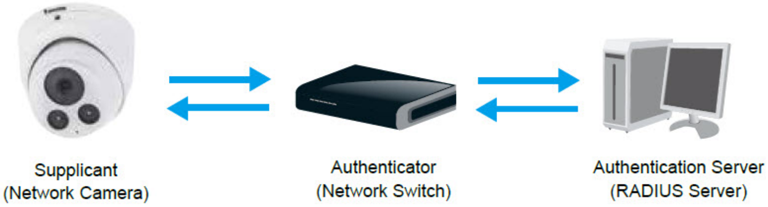
Always allow the IP address to access this device—You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Configuring Security > IEEE802-1X

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 are:

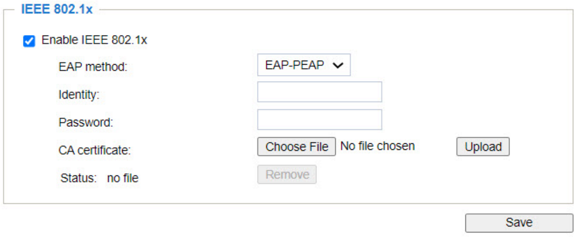


- Supplicant: A client end user (camera), which requests authentication.
- Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
- Authentication server (usually a RADIUS server): Checks the client certificate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

Sarix Value Network Cameras support two types of EAP methods to perform authentication—EAPPEAP and EAP-TLS.

To enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (for example: 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. Select **EAP-PEAP** or **EAP-TLS** as the *EAP method*.



IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-PEAP

Identity:

Password:

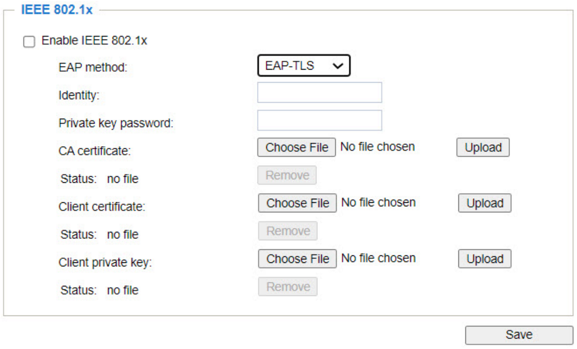
CA certificate: Choose File No file chosen Upload

Status: no file Remove

Save

3. In the remaining fields, enter all information including the *Identity* and *Password* issued by the CA.

4. Upload the related *CA certificate*. To do so, click **Choose File**, navigate to and select the file, and then click **Upload**.
5. If you chose **EAP-TLS** as the *EAP method*:



IEEE 802.1x

☐ Enable IEEE 802.1x

EAP method: EAP-TLS

Identity:

Private key password:

CA certificate: Choose File No file chosen Upload

Status: no file Remove

Client certificate: Choose File No file chosen Upload

Status: no file Remove

Client private key: Choose File No file chosen Upload

Status: no file Remove

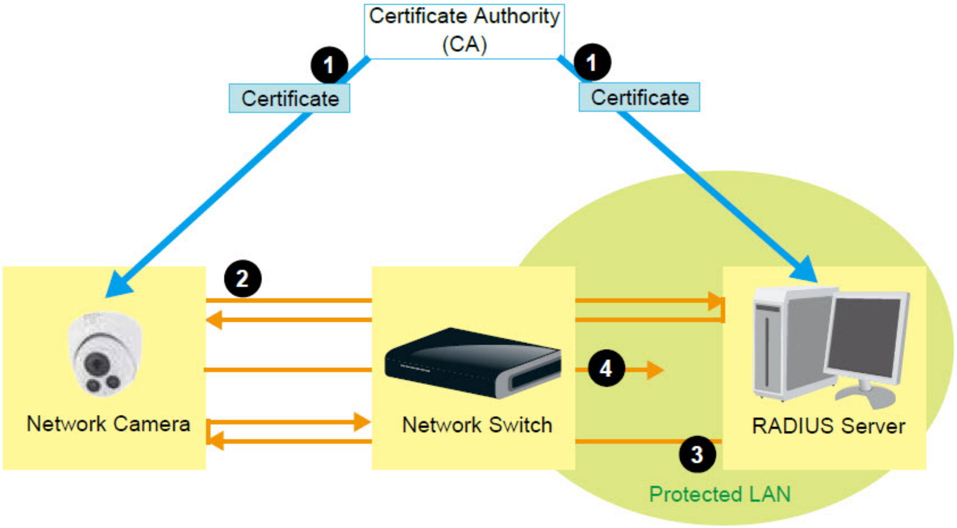
   a. Upload the related *Client certificate*. To do so, click **Choose File**, navigate to and select the file, and then click **Upload**.

   b. Upload the related *Client private key*. To do so, click **Choose File**, navigate to and select the file, and then click **Upload**.

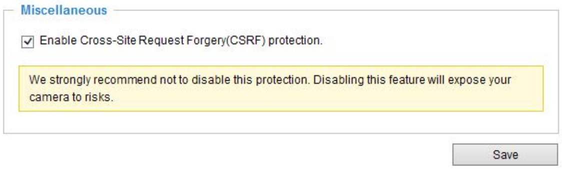
6. Click **Save**.
7. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x'enabled switch. The devices will then start the authentication automatically.

The authentication process for 802.1x is as follows:

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.



Configuring Security > Miscellaneous


Miscellaneous

☑ Enable Cross-Site Request Forgery(CSRF) protection.

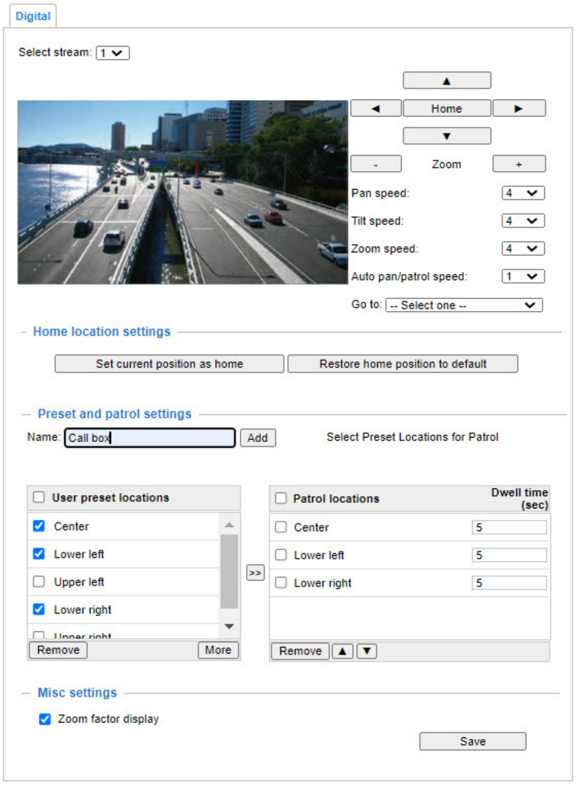
We strongly recommend not to disable this protection. Disabling this feature will expose your camera to risks.

- *Enable Cross-Site Request Forgery(CSRF) Protection*—TrendMicro utitlity provides the protection against Cross-Site Request Forgery. CSRF is also known as one-click attack or session riding. CSRF is a type of malicious exploit of a website, in this case, the camera. Unauthorized commands are transmitted from a user that the web application trusts, using the mechanism of forging a trusted user's own request with a request containing his own cookies, etc. Different ways can be used for a malicious website to transmit such commands. They can be specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests. The malicious attack can occur without users' interaction or even knowing it.

Configuring Digital PTZ > Digital PTZ Settings

This section explains how to control the Network Camera’s Pan/Tilt/Zoom operation.

The *Digital PTZ settings* page enables you to control PTZ operation. Within a field of view, it allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera.


Digital
▲
◄
Home
►
▼
-
Zoom
+
Home location settings
Set current position as home
Restore home position to default
Preset and patrol settings
Add
Select Preset Locations for Patrol
>>
Remove
More
Remove
▲
▼
Misc settings
Save

Select stream: 1

Pan speed: 4

Tilt speed: 4

Zoom speed: 4

Auto pan/patrol speed: 1

Go to: -- Select one --

Name: Call box

□ User preset locations
☑ Center
☑ Lower left
□ Upper left
☑ Lower right
□ Upper right

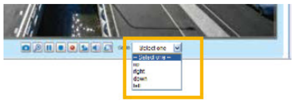
□ Patrol locations	Dwell time (sec)
□ Center	5
□ Lower left	5
□ Lower right	5

☑ Zoom factor display

- In the top area of the page:
  - *Select stream*—Select the stream from the drop-down menu.
  - Click **Home** and/or use the arrows, -, and + buttons to pan/tilt/zoom to a specific view.
  - *Pan speed*—Select from the drop-down menu from -5~5 (slow/fast).
  - *Tilt speed*—Select from the drop-down menu from -5~5 (slow/fast).
  - *Zoom speed*—Select from the drop-down menu from -5~5 (slow/fast).
  - *Auto pan/patrol speed*—Select from the drop-down menu from 1~5 (slow/fast).
  - *Go to*—Click to select camera presets from the drop-down menu.
- In the *Home location settings* area, click either *Set current position as home* or *Restore home position to default*.
- In the *Preset and patrol settings area*:
  1. If you are adding a new preset location, enter a string in the *Name* field, and then click *Add*.
  2. Select the preset locations in the *User preset locations* list, and click >> to add them to the *Patrol locations* list.
  3. To see the full list of *User preset locations*, click **More**; click **Less** to return to the default list length.
  4. For each preset location in the *Patrol locations* list, time a *Dwell time (sec)* to use during an auto patrol.

5. If you want to delete a preset location from the *Patrol locations* list, select it and click **Remove**.
6. Select a location and click ▲ ▼ to rearrange the patrol order.
7. To implement the patrol schedule, go to the **Home** page and click on the **Patrol** button. The Network Camera will patrol along the selected positions repeatedly.

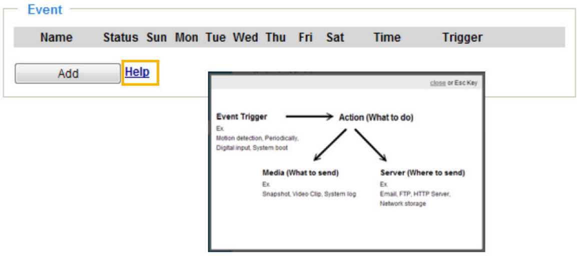
- In the *Misc settings* area, click to select or deselect the checkbox for *Zoom factor display*. If you check this item, the zoom indicator will be displayed on the *Home* page when you zoom in/out on the live viewing window.



- Click **Save** to enable the settings.

Configuring Event > Event

This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or email address as notifications. When you click **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.

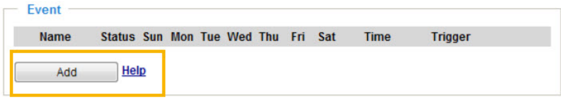

Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger

Add
Help
close or Esc Key
Event Trigger
Ex.
Motion detection, Periodically, Digital input, System boot
Action (What to do)
Media (What to send)
Ex.
Snapshot, Video Clip, System log
Server (Where to send)
Ex.
Email, FTP, HTTP Server, Network storage

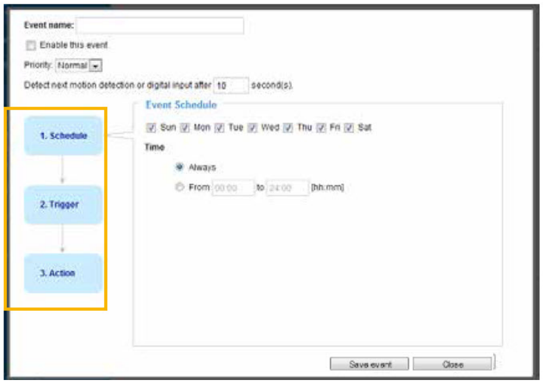
Configuring an Event

To configure an event with reactive measures such as recording 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. An event is an action initiated by a user-defined trigger source. In the Event area, click **Add** to open the event settings window. Here you can arrange three elements—Schedule, Trigger, and Action—to set an event. A total of three event settings can be configured.



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger



Event name:

□ Enable this event

Priority: Normal

Detect next motion detection or digital input after 10 second(s).

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

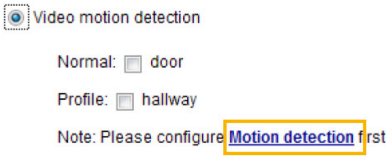
- *Event name*—Enter a name for the event setting.
- *Enable this event*—Select this checkbox to enable the event setting.
- *Priority*—Select the relative importance of this event (**High**, **Normal**, or **Low**). Events with a higher priority setting will be executed first.
- *Detect next motion detection or digital input after [#] seconds*—Enter the duration in seconds to pause motion detection after a motion is detected. This can prevent event-related actions from taking place too frequently.

To add an event:

1. Specify the **Schedule**. This is the period of time during which the event trigger will take effect. Select the days of the week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, trigger an event only during the off-office hours.
2. Specify the **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. Select the item to display the detailed configuration options.

   - *Video motion detection*—This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, see the section titled .

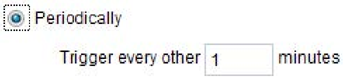
     ● Video motion detection

     Normal: □ door

     Profile: □ hallway

     Note: Please configure Motion detection first

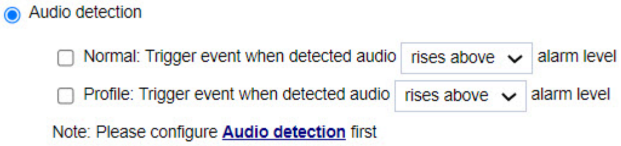
   - *Periodically*—This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

     ● Periodically

     Trigger every other 1 minutes

- *System boot*—This option triggers the Network Camera when the power to the Network Camera is disconnected and re-connected.
- *Recording notify*—This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite older data.
- *Audio detection*—A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera's view. See the section titled *Configuring Applications > Audio Detection*



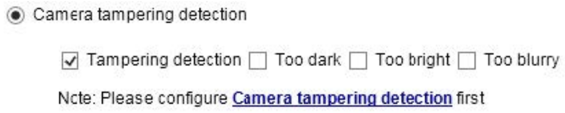
● Audio detection

□ Normal: Trigger event when detected audio rises above alarm level

□ Profile: Trigger event when detected audio rises above alarm level

Note: Please configure **Audio detection** first

- *Camera tampering detection*—This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. See the section titled *Configuring Applications > Tamper Detection*.

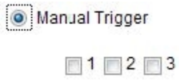


● Camera tampering detection

☑ Tampering detection □ Too dark □ Too bright □ Too blurry

Ncte: Please configure **Camera tampering detection** first

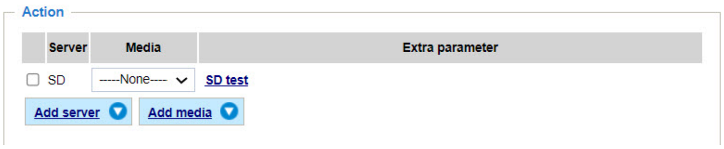
- *Manual Triggers*—This option allows users to enable event triggers manually by clicking the on/off button on the homepage. Configure 1 to 3 associated events before using this function.



● ManJal Trigger

□ 1 □ 2 □ 3

3. **SD Test**—Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, format it before use.
4. Define the actions to be performed by the Network Camera when a trigger is activated.



Action

Server	Media	Extra parameter
□ SD	-----None----	SD test

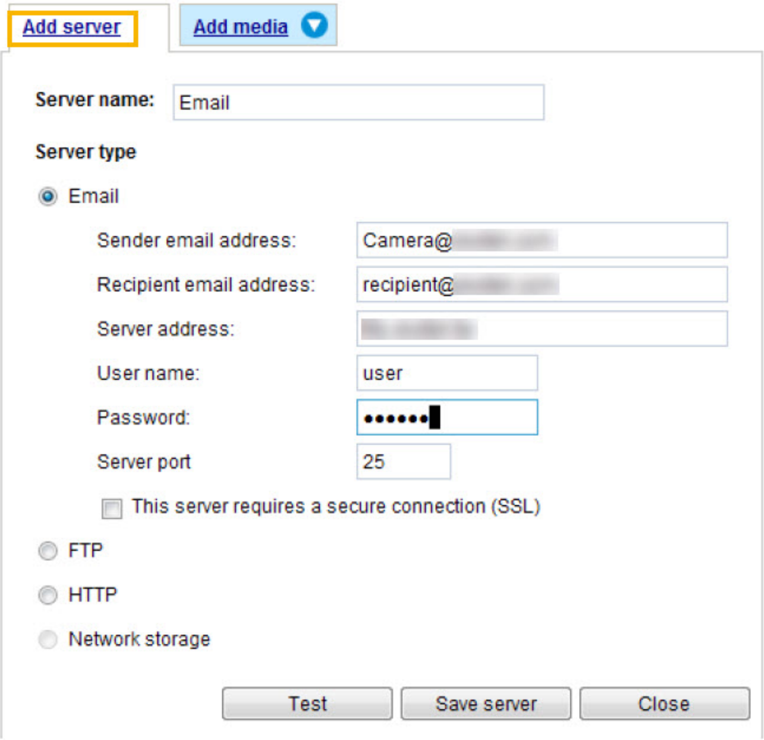
5. To do so, perform the procedures in the sections titled:
   - *Adding a Server*
   - *Adding Media*
6. Click **Save event**, or click **Close** to exit this window without saving.

Adding a Server

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. Click **Add**

server to open the server setting window. You can specify where the notification messages are sent to 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 one or all of them.



Server name: Email

Server type

● Email

Sender email address: Camera@[redacted]

Recipient email address: recipient@[redacted]

Server address: [redacted]

User name: user

Password: ••••••

Server port 25

□ This server requires a secure connection (SSL)

○ FTP

○ HTTP

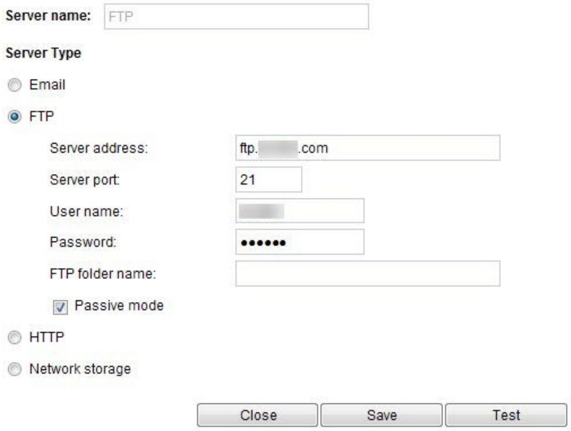
○ Network storage

- *Server name*—Enter a name for the server setting.
- *Server type > Email*

1. Select to send the media files via email when a trigger is activated.
   - *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.
2. If your SMTP server requires a secure connection (SSL), select *This server requires a secure connection* (SSL).
3. 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. Click **Save server** to enable the settings.
4. After you configure the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.

- *Server type > FTP*

1. Select to send the media files to an FTP server when a trigger is activated.



Server name: FTP

Server Type

○ Email

● FTP

Server address: ftp.[redacted].com

Server port: 21

User name: [redacted]

Password: ••••••

FTP folder name:

☑ Passive mode

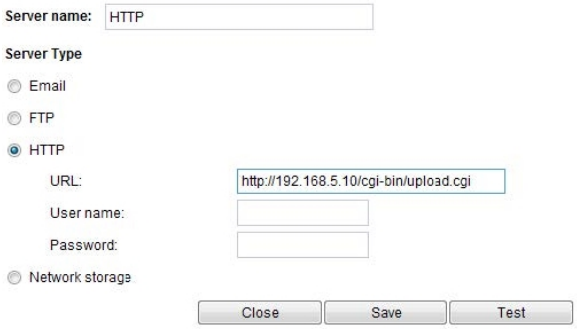
○ HTTP

○ Network storage

   - *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 files will be placed. If the folder name does not exist, the Network Camera will automatically 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. The firmware default has the *Passive mode* checkbox selected.

2. To verify that the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive a test.txt file on the FTP server.
3. Click **Save server** to enable the settings.

- *Server type > HTTP*



Server name: HTTP

Server Type

○ Email

○ FTP

● HTTP

URL: http://192.168.5.10/cgi-bin/upload.cgi

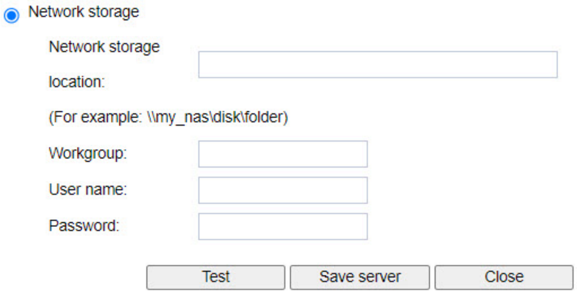
User name:

Password:

○ Network storage

1. Select to send the media files to an HTTP server when a trigger is activated.
   - *URL*—Enter the URL of the HTTP server.
   - *User name*—Enter the user name if necessary.
   - *Password*—Enter the password if necessary.
2. To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.
3. Click **Save server** to enable the settings.

- *Server type > Network storage*



● Network storage

Network storage location:

(For example: \\my_nas\disk\folder)

Workgroup:

User name:

Password:

1. Select to send the media files to a networked storage when a trigger is activated. See the section titled *Configuring Recording > Recording Settings*, information about NAS servers for details.

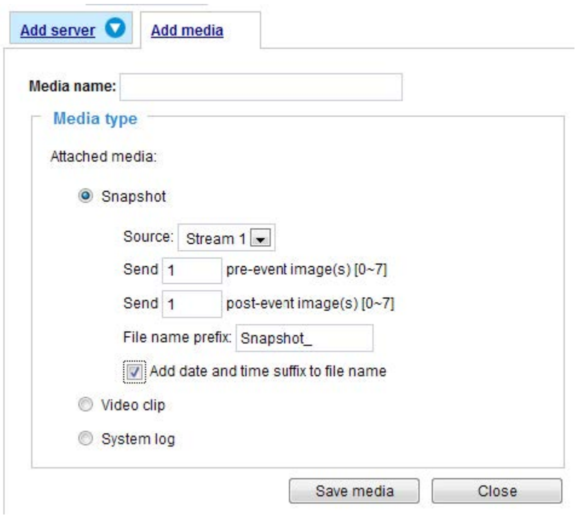
   Note: Only one NAS server can be configured.

   - *Network storage location*—Enter the path of the ntwork storage location.
   - *Workgroup*—Enter the name of the workgroup.
   - *User name*—Enter the user name if necessary.
   - *Password*—Enter the password if necessary.
2. To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.
3. Click **Save server** to enable the settings.

Adding Media

1. Click **Add media** to open the media setting window.

   You can specify the type of media that will be sent 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 one or all of them.



Media name:

Media type

Attached media:

● Snapshot

Source: Stream 1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

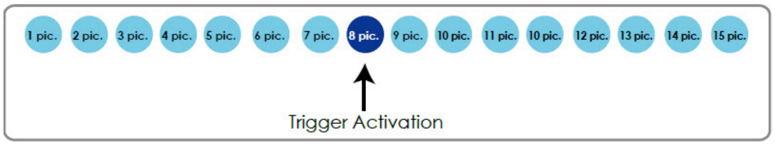
File name prefix: Snapshot_

☑ Add date and time suffix to file name

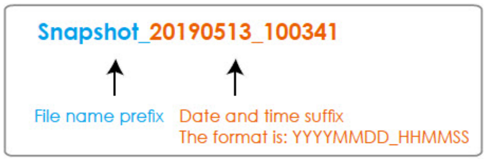
○ Video clip

○ System log

2. Type a string in the *Media name* field.
3. *Media type > Snapshot*—Select to send snapshots when a trigger is activated.
   - *Source*—Select the video stream from which to take snapshots.
   - *Send [#] pre-event images*—The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to seven 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 seven 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 can be generated after a trigger is activated.

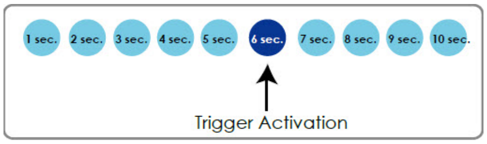


   - *File name prefix*—Enter the text that will be appended to the front of the file name.
   - *Add date and time suffix to the file name*—Select this option to add a date/time suffix to the file name.

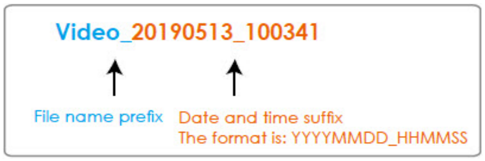


   - *Media type > Video clip*—Select to send video clips when a trigger is activated.
     - *Source*—Select a video stream as the source of video clip.
     - *Pre-event recording*—The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to nine seconds can be set.

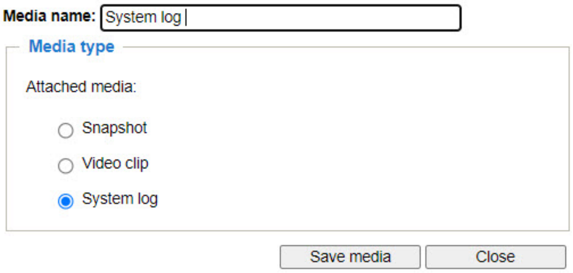
- *Maximum duration*—Specify the maximum recording duration in seconds. The duration can be up to ten seconds. For example, if *Pre-event recording* is set to five seconds and the *Maximum duration* is set to ten seconds, the Network Camera continues to record for another four seconds after a trigger is activated.



- *Maximum file size*—Specify the maximum file size allowed. Some users might need to stitch the video clips together when searching and packing up forensic evidence.
- *File name prefix*—Enter the text that will be appended to the front of the file name.



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



Media name: System log

Media type

Attached media:

○ Snapshot

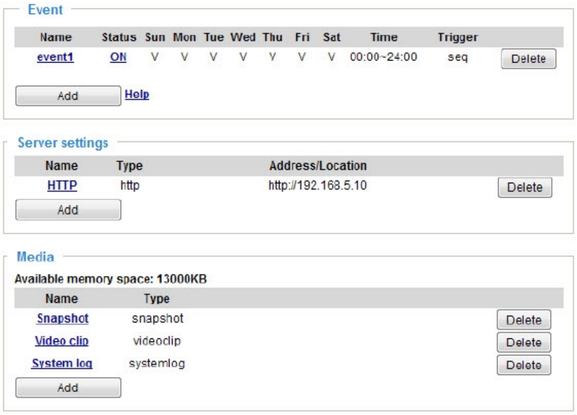
○ Video clip

● System log

4. Click **Save media** to enable the settings.

   Note: After you set up the first media server, a new media server will automatically display on the *Media* list. To add more media options, click **Add media**.

5. Click **Close** to exit the page.
6. When completed, click **Save event** to enable the settings and click **Close** to exit t window. The new event servers and media entries will appear in the event drop-down menu on the *Event setting* page. See the example of the Event setting page below.



Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
event1	ON	V	V	V	V	V	V	V	00:00~24:00	seq	Delete

Server settings

Name	Type	Address/Location	
HTTP	http	http://192.168.5.10	Delete

Media

Available memory space: 13000KB

Name	Type	
Snapshot	snapshot	Delete
Video clip	videoclip	Delete
System log	systemlog	Delete

When the Event Status is *ON*, the event configuration above is triggered by motion detection, the Network Camera will automatically send snapshots via email.

7. To stop the event trigger, you can click on the **ON** button to turn it to **OFF** status or click the **Delete** button to remove the event setting.
8. To remove a server setting from the list, select a server name and click **Delete**.

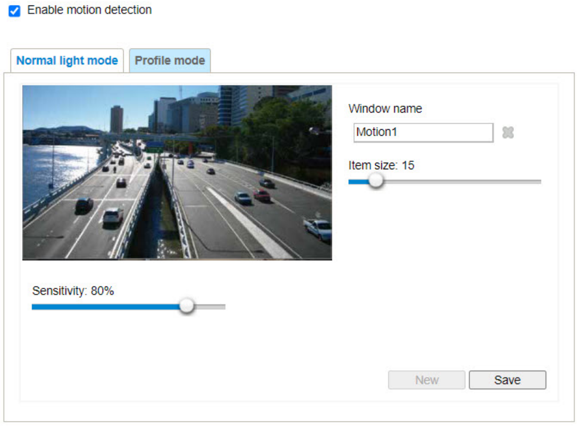
Note: You can only delete a server setting when it is not applied in an existing event setting.

9. To remove a media setting from the list, select a media name and click **Delete**.

Note: You can only delete a media setting when it is not applied in an existing event setting.

Configuring Applications > Motion Detection

This section explains how to configure the Network Camera to enable motion detection. A total of five motion detection windows can be configured.



☑ Enable motion detection

Window name: Motion1

Item size: 15

Sensitivity: 80%

To enable motion detection:

1. Click to select the checkbox for *Enable motion detection*.
2. Click **Normal light mode**.

a. Click **New** to add a new motion detection window.

b. In the *Window name* text box, enter a name for the motion detection window.

c. In the live view window, use four mouse clicks to designate a detection window. You can change the window shape by dragging the corner marks to a preferred location.

d. Drag the *Item size* slider bar to change the minimum size of item to trigger an alarm. An item size box will appear in the center of screen for your reference (in semi-transparent red). An intruding object must be larger than the *Item size* to trigger an alarm. Change the item size according to the live view.

e. Define the sensitivity to moving objects by moving the *Sensitivity* slider bar. A high sensitivity is prone to produce false alarms such as the fast changes of light (day/night mode switch, turning lights on/off). A movement must persist longer than 0.3 second for the motion to be detected.

f. To delete a window, click the X mark (✖) to the right of the window name.

g. Click **Save** to enable the settings.

h. Click **New** to add another motion detection window, or click **Close** to exit the page.

3. To configure other motion detection settings for night/schedule mode (that is, for a different lighting condition), click **Profile mode**. Another three motion detection windows can be configured on this page.

a. Click **New**.

b. In the *Window name* text box, enter a name for the motion detection window.

c. In the live view window, use four mouse clicks to designate a detection window. You can change the window shape by dragging the corner marks to a preferred location.

d. Drag the *Item size* slider bar to change the minimum size of item to trigger an alarm. An item size box will appear in the center of screen for your reference (in semi-transparent red). An intruding object must be larger than the *Item size* to trigger an alarm. Change the item size according to the live view.

e. Define the sensitivity to moving objects by moving the *Sensitivity* slider bar. A high sensitivity is prone to produce false alarms such as the fast changes of light (day/night mode switch, turning lights on/off). A movement must persist longer than 0.3 second for the motion to be detected.

f. Click to select the checkbox for *Enable to apply these settings at*.

g. Click to select the radio button for either *Night mode* or *Schedule mode*.

h. If you selected Schedule mode, enter appropriate times in the *From* and *To* fields.

i. To delete a window, click the X mark (✖) to the right of the window name.

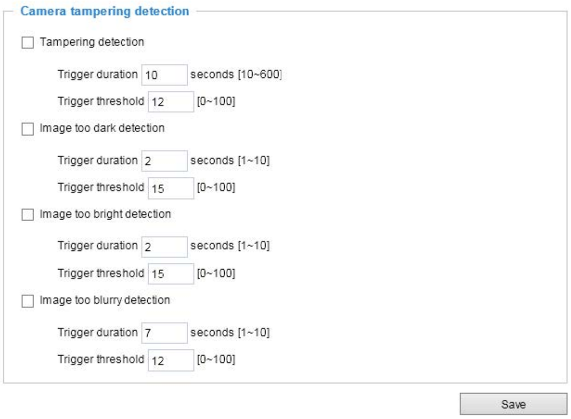
j. Click **Save** to enable the settings.

k. Click **New** to add another motion detection window, or click **Close** to exit the page.

This motion detection window will also be displayed on the *Event settings* page. You can go to **Event > Event settings > Trigger** to select it as a trigger source.

Configuring Applications > Tamper Detection

This section explains how to set up camera tamper detection. With tamper detection, the camera is capable of detecting incidents such as redirection, blocking or defocusing, or even spray paint.



Camera tampering detection

□ Tampering detection

Trigger duration 10 seconds [10~600]

Trigger threshold 12 [0~100]

□ Image too dark detection

Trigger duration 2 seconds [1~10]

Trigger threshold 15 [0~100]

□ Image too bright detection

Trigger duration 2 seconds [1~10]

Trigger threshold 15 [0~100]

□ Image too blurry detection

Trigger duration 7 seconds [1~10]

Trigger threshold 12 [0~100]

For each detection type selected, you must also set the trigger duration and trigger threshold.

- *Trigger duration [#] seconds [10-#]*—The duration specifies the set of time before the tampering is considered as a real alarm. This helps avoid false alarms by short-lived changes.
- *Trigger threshold [#] seconds [0-#]*—The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold. Conditions such as image too dark, too bright, or too blurry (defocused) can also be configured as tampering conditions. The Trigger threshold determines how sensitive your is tamper detection setting. Lower the threshold number, easier to trigger.

To set up the camera tamper detection function:

1. Click to select the checkbox for *Tampering detection*.
   a. Enter a value in the *Trigger duration [#] seconds [10-600]* field.
   b. Enter a value in the *Trigger threshold [#] seconds [0-100]* field.
2. Click to select the checkbox for *Image too dark detection*. This can occur when the object is covered or has been spray painted.
   a. Enter a value in the *Trigger duration [#] seconds [1-10]* field.
   b. Enter a value in the *Trigger threshold [#] seconds [0-100]* field.
3. Click to select the checkbox for *Image too bright detection*. This can occur when someone is shining a flash light at the camera. The average lighting level of the scene is taken into consideration.
   a. Enter a value in the *Trigger duration [#] seconds [1-10]* field.
   b. Enter a value in the *Trigger threshold [#] seconds [0-100]* field.
4. Click to select the checkbox for *Image too blurry detection*. This can occur when there is strong interference on the device, such as EMI interference.
   a. Enter a value in the *Trigger duration [#] seconds [1-10]* field.

b. Enter a value in the *Trigger threshold [#] seconds [0-100]* field.

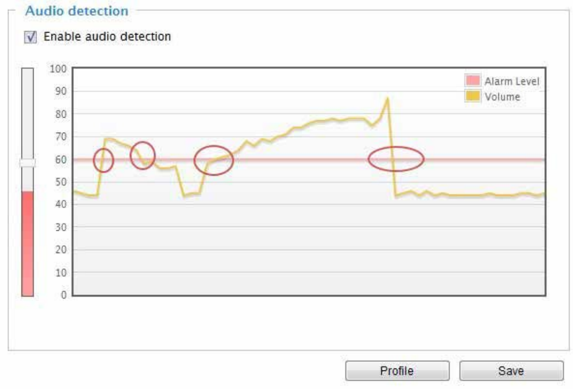
5. Click **Save**.

You can configure *Tampering detection* as a trigger element to the proactive event configurations in **Event > Event settings > Trigger**. For example, when the camera is tampered with, it will send the pre- and post-event video clips to a networked storage device. See the section titled *Configuring Event > Event*.

Configuring Applications > Audio Detection

Audio detection, along with video motion detection, is applicable in the following scenarios:

- Detection of activities not covered by camera view, for example: a loud input by gun shots or breaking a door/window.
- A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
- Dark environments where video motion detection might not function well.



Audio detection

☑ Enable audio detection

The red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

In the *Audio detection* window, the current sound input is interactively indicated by a fluctuating yellow wave diagram.

Note: The volume numbers (0~100) on the side of wave diagram do not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.

Note: To configure this feature, you must not mute the audio in **Configuration > Media > Audio**. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.

Use the *Profile* window to configure a different Audio detection setting. For example, a place can be noisy in the day time and become very quiet in the night.

1. Click on the *Enable audio detection* checkbox. The current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Click **Profile**.

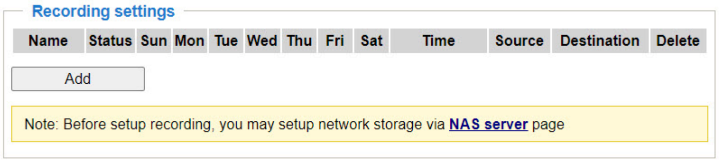
3. In the *Audio detection* area, click to drag the alarm level tab to a preferred location on the slider bar.
4. In the General settings area:
    a. Click to select *Enable this profile*.
    b. Click to select the radio button for either *Night mode* or *Schedule mode*.
    c. If you selected *Schedule mode*, enter values in the *From* and *to* fields.
5. Click **Save**, and then click **Close**.
6. Click **Save** again.

Note: If the alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. Pelco recommends that you set the alarm level farther from the detected sound level.

Note: To configure and enable this feature, you must not configure video stream #1 into Motion JPEG. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station along with stream #1.

Configuring Recording > Recording Settings

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



Recording settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete

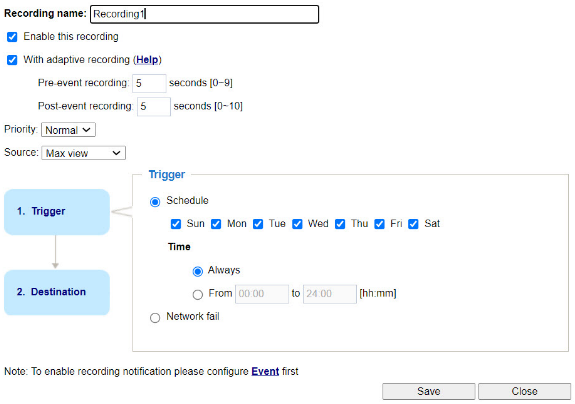
Add

Note: Before setup recording, you may setup network storage via **NAS server** page

- If the destination of recordings will be an SD card, format the SD card via the camera's web console (in the Local storage SD card management page) when using it for the first time. See the section titled *Configuring SD Card Management*.
- If the destination of recordings will be a NAS server, configure the server now. See the section titled *Configuring NAS Management*

To configure Recording settings:

1. Click **Add** to open the recording setting window. A total of two recording settings can be configured.



Recording name: Recording1

☑ Enable this recording

☑ With adaptive recording (**Help**)

Pre-event recording: 5 seconds [0~9]

Post-event recording: 5 seconds [0~10]

Priority: Normal

Source: Max view

Trigger

● Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

○ Network fail

Note: To enable recording notification please configure **Event** first

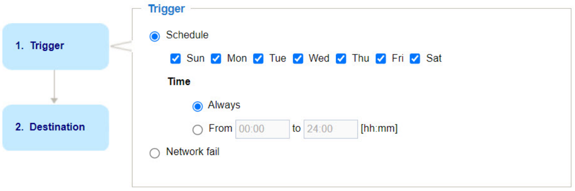
Note: To enable recording notification, configure *Event settings* first. See the section titled *Configuring Event > Event*.

- *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 to activate the frame rate control according to the 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. See the section titled *Configuring Media > Video*.
  - If you enable adaptive recording on a camera, 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 bandwidths and storage space.
  - To enable adaptive recording, 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 records 1 frame per second, H.264 mode records the I frame only.
  - When the I frame period is >1s on Video settings page, firmware will force down the I frame period to 1s when adaptive recording is enabled.
  - The alarm trigger includes motion detection and DI detection.

2. *Pre-event recording* and *Post-event recording*—The Network Camera has a buffer that temporarily holds data for a period of time. Therefore, when an event occurs, the camera can retrieve image frames taken several seconds ago. Enter a number to define the duration of recording before and after a trigger is activated.
3. *Priority*—Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
4. *Source*—Select a video stream as the recording source.

To set up the recording:

1. Click **Trigger** in the blue box in the left panel.



Trigger

● Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

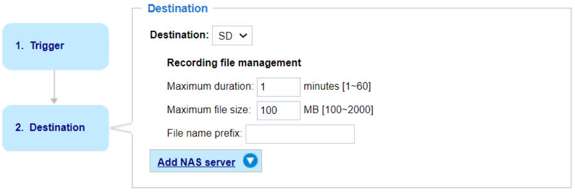
● Always

○ From 00:00 to 24:00 [hh:mm]

○ Network fail

2. Click to select one of these triggers.
   - *Schedule*—The server will start to record files on the local storage or network storage (NAS).
   - *Network fail*—If the network fails, the server will start to record files on the local storage (SD card).
3. If you selected *Schedule*, click to select a *Time*—either *Always* or *From [##:##] to [##:##]*.
4. If you selected *From [##:##] to [##:##]*, enter values in the *From* and *to* fields.

5. Click **Destination** in the blue box in the left panel.



Destination

Destination: SD

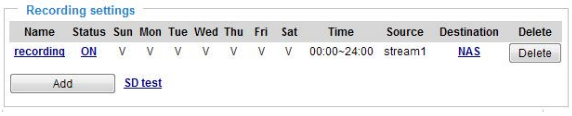
Recording file management

Maximum duration: 1 minutes [1~60]

Maximum file size: 100 MB [100~2000]

File name prefix:

6. Select the *Destination* for the recorded video file from the drop-down menu.
7. Under *Recording file management*:
   a. Enter a value in the *Maximum duration [#] minutes [1-60]* field.
   b. Enter a value in the *Maximum file size [#] MB [100-2000]* field.
   c. Enter a value in the *File name prefix* field—the text that will be appended to the front of the file name.
8. Click **Save**.
   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 menu on the recording page.
9. To remove a recording setting from the list, click **Delete** to the right of the setting.



Recording settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
recording	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	NAS	Delete

Configuring Storage > Storage Management

You can configure the system to store data on an SD card or on a NAS server.

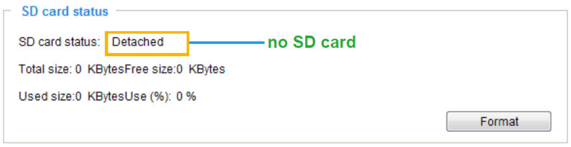
Configuring SD Card Management

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.

To use the camera SD card:

- 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 file system 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.
- Do not modify or change the folder names in the SD card. That might result in camera malfunctions.

In the *SD card status* section, SD card status shows the status and reserved space of your SD card. Format the SD card when using it for the first time.

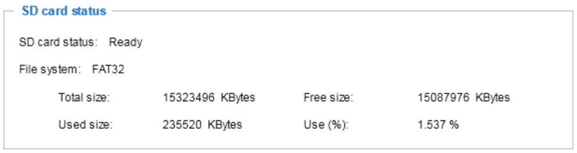


SD card status

SD card status: Detached — no SD card

Total size: 0 KBytesFree size:0 KBytes

Used size:0 KBytesUse (%): 0 %



SD card status

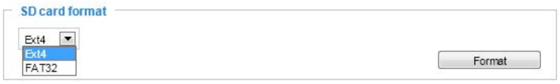
SD card status: Ready

File system: FAT32

Total size: 15323496 KBytes Free size: 15087976 KBytes

Used size: 235520 KBytes Use (%): 1.537 %

In the *SD card format* section, the Linux kernel EXT4 file system format applies to SD card larger than 32 GB. However, if EXT4 is applied, the computers running Windows will not be able to access the contents on the SD card unless using some 3rd-party software.



SD card format

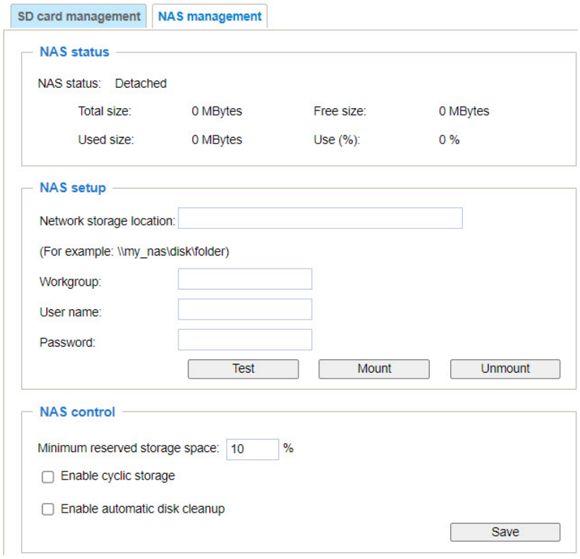
Ext4

1. Select the format from the drop-down menu.
2. Click **Format**.

In the *SD card control* section:

1. Enter a value for the *Minimum reserved storage space*. This is the percent of space allocated to storage.
2. If appropriate, click to select the checkbox for *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.
3. If appropriate, click to select the checkbox for *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.
4. Click **Save**.

Configuring NAS Management



NAS status

NAS status: Detached

Total size: 0 MBytes Free size: 0 MBytes

Used size: 0 MBytes Use (%): 0 %

NAS setup

Network storage location:

(For example: \\my_nas\disk\folder)

Workgroup:

User name:

Password:

NAS control

Minimum reserved storage space: 10 %

□ Enable cyclic storage

□ Enable automatic disk cleanup

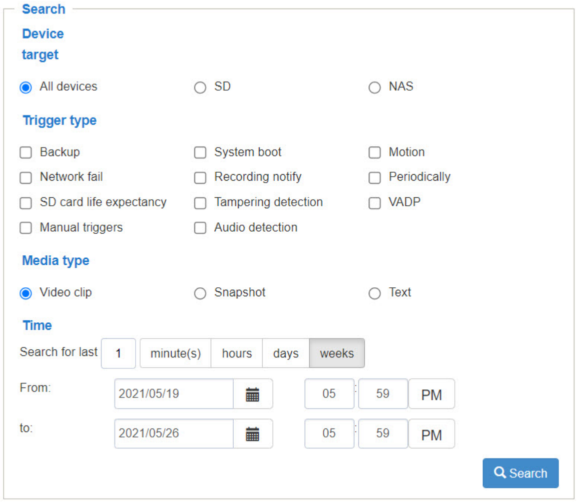
1. Click **NAS management**.
2. View information in the *NAS status* area of the window.
3. In the *NAS setup* area:
   a. Enter a string in the *Network storage location* field.
   b. Enter a string in the *Workgroup* field.
   c. Enter strings in the *User name* and *Password* fields.
   d. Click **Test** to test the setup.
   e. Click **Mount** to add the drive to a partition or folder.
   f. Click **Unmount** to remove the drive from a partition or folder.
4. In the NAS control area:
   1. Enter a value for the *Minimum reserved storage space*. This is the percent of space allocated to storage.
   2. If appropriate, click to select the checkbox for *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.
   3. If appropriate, click to select the checkbox for *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.
   4. Click **Save**.

Configuring Local > 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 the Records

This page allows the user to set up search criteria for recorded data. If you do not select any criteria and click the **Search** button, all recorded data will be listed in the Search results area.



Search

Device target

● All devices ○ SD ○ NAS

Trigger type

□ Backup □ System boot □ Motion
□ Network fail □ Recording notify □ Periodically
□ SD card life expectancy □ Tampering detection □ VADP
□ Manual triggers □ Audio detection

Media type

● Video clip ○ Snapshot ○ Text

Time

Search for last 1 minute(s) hours days [✓ weeks]

From: 2021/05/19 05 : 59 PM

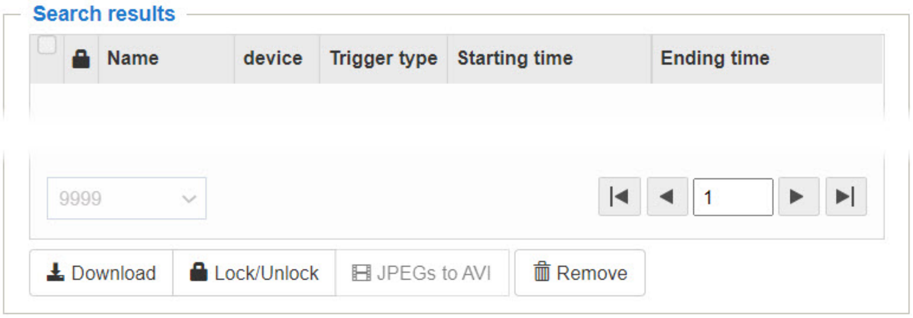
to: 2021/05/26 05 : 59 PM

1. In the *Search* area of the page, make the following selections:
   - *Device target*—Click to select the radio button for the device(s) on which to search.
   - *Trigger type*—Click to select the checkboxes for one or more trigger types on which to search.
   - *Media type*—Click to select the radio button for the type of media for which to search.
   - *Time*—Manually enter the time range you want to search for contents created at a specific point in time.
2. Click **Search**.

   The recorded data corresponding to the search criteria will be listed in the *Search results* area.

Viewing Search Results

The *Search results* window lists the results of the search. Column titles included in the table depend on the search criteria.



□	🔒	Name	device	Trigger type	Starting time	Ending time

- To sort the search results in either direction, click the up or down arrow in the field that displays the total number of results (lower left corner of the *Search results* area).
- To view another page of search results, click the right and left arrows (⏮ ◀ 1 ▶ ⏭) at the lower right corner of the *Search results* area.
- To play a video, click to highlight a search result, and then use the pop-up play window to view the selected file.
- To download a video, click to highlight a search result, click **Download**, and then use the pop-up download window to save the file.
- To lock and unlock recordings, click to select the checkboxes for appropriate search results, and then click **Lock/Unlock**. The selected items will become locked; they will not be deleted during cyclic recording. You can click again to unlock the selections.
- To convert JPEG format files, such as snapshots, into AVI files, click to select the checkboxes for the appropriate snapshots from the list, and then click **JPEGs to AVI**. Those snapshots will be converted into an AVI file.
- To delete search results, click to select the appropriate checkboxes, and then click **Remove**.

Pelco, Inc.
625 W. Alluvial Ave., Fresno, California 93711 United States
(800) 289-9100 Tel
(800) 289-9150 Fax
+1 (559) 292-1981 International Tel
+1 (559) 348-1120 International Fax
www.pelco.com