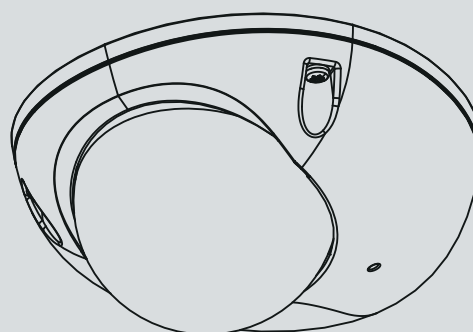




FD9366-HV Fixed Dome Network Camera

# User's Manual

2MP • Outdoor • IP67 • IK10 • NEMA 4x • Day & Night  
WDR Pro • Smart Stream III • 20M Smart IR



Rev. 1.0

## **Table of Contents**

Overview .....	3
Revision History .....	4
Read Before Use .....	4
Package Contents .....	5
Symbols and Statements in this Document .....	5
Physical Description .....	6
Hardware Installation .....	8
Software Installation .....	16
Network Deployment .....	25
Ready to Use .....	26
Accessing the Network Camera .....	29
Using Web Browsers .....	29
Using RTSP Players .....	32
Using 3GPP-compatible Mobile Devices .....	33
Using VIVOTEK Recording Software .....	34
Main Page .....	35
Client Settings .....	40
Configuration .....	45
System > General settings .....	46
System > Homepage layout .....	48
System > Logs .....	51
System > Parameters .....	53
System > Maintenance .....	54
Media > Image .....	58
Media > Video .....	70
Media > Video .....	71
Media > Audio .....	80
Network > General settings .....	81
Network > Streaming protocols .....	88
Network > SNMP (Simple Network Management Protocol) .....	97
Network > FTP .....	98
Bonjour .....	99
Security > User accounts .....	100
Security > HTTPS (Hypertext Transfer Protocol over SSL) .....	102
Security > Access List .....	109
PTZ > PTZ settings .....	115
Event > Event settings .....	119
Applications > Motion detection .....	133
Applications > DI and DO .....	136
Applications > Tampering detection .....	137
Applications > Audio detection .....	138
Applications > Package management - a.k.a., VADP (VIVOTEK Application Development Platform) .....	140
Recording > Recording settings .....	143
Storage > SD card management .....	148

Local storage > Content management .....	151
<b>Appendix .....</b>	<b>154</b>
URL Commands for the Network Camera.....	154
Technology License Notice.....	408
Electromagnetic Compatibility (EMC).....	409

## Overview

The FD93666 is an outdoor fixed dome network camera capable of 1920 x 1080 at 30 fps. With the most updated VIVOTEK WDR Pro technology, the camera series is capable of capturing the highest quality images in both low light and high contrast environments.

The onboard IR can provide illumination in total darkness. With the Smart IR feature, the firmware automatically adjusts the IR intensity for objects that came too close, in order to avoid over-exposure.

The camera supports WDR function at the effectiveness of up to 120dB. These models support local video storage on the MicroSD cards if network service should be interrupted. The cameras also come with configurable motion detection and tampering detection with up to 5 privacy mask areas.

## Revision History

- Rev. 1.0: Initial release.

## Read Before Use

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

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

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



### **IMPORTANT:**

1. The product must be installed and protected in a location that is not easily accessible, and is away from impacts or heavy vibration. For example, at the location where the surveillance cameras are looking down or installed at high positions such as on a wall, or at least 3 meters above the ground.
  2. Maintenance and repair work must always be carried out by qualified technical personnel. Disconnect power from the unit when performing a maintenance task.
-


## Package Contents

- FD9366-HV
- Screw pack anchors.
- Alignment sticker and desiccant bag.
- Quick Installation Guide, DI/DO terminal blocks, T10 star driver.
- Waterproof cable gland.

### **WARNING:**

1. IR lights emit from this product.
2. Use appropriate shielding or eye protection.

## Symbols and Statements in this Document

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



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



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



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



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

### **IMPORTANT:**

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

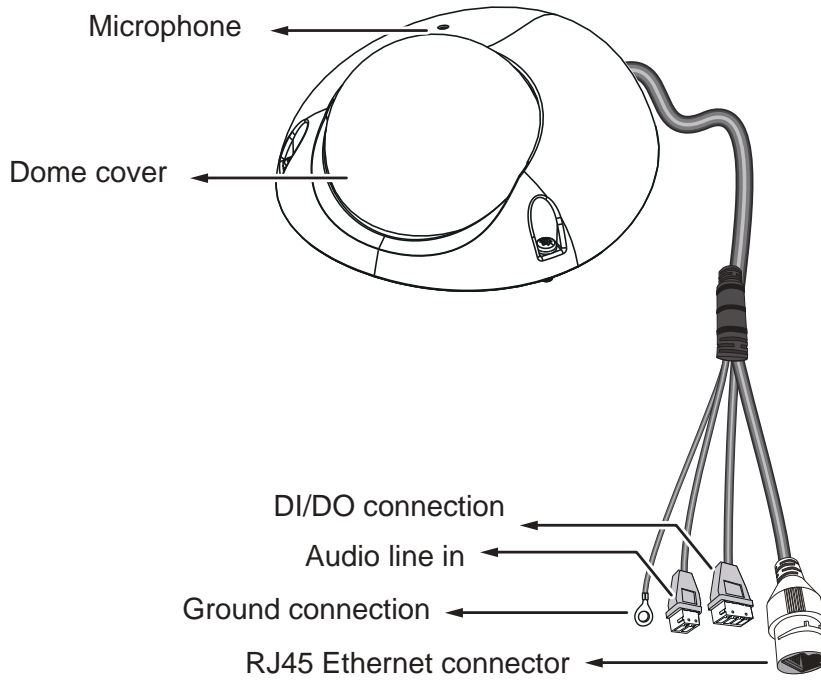
1. La caméra ne doit être raccordée qu'à des réseaux PoE, sans routage vers des installations extérieures.
2. Pour les raccordements PoE, utilisez uniquement un équipement de TI homologué UL, avec une sortie PoE.

Use the camera only with a DC power supply that is UL listed, and limited power source (LPS) certified. The power supply should bear the UL listed and LPS marks. The power supply should also meet any safety and compliance requirements for the country of use.

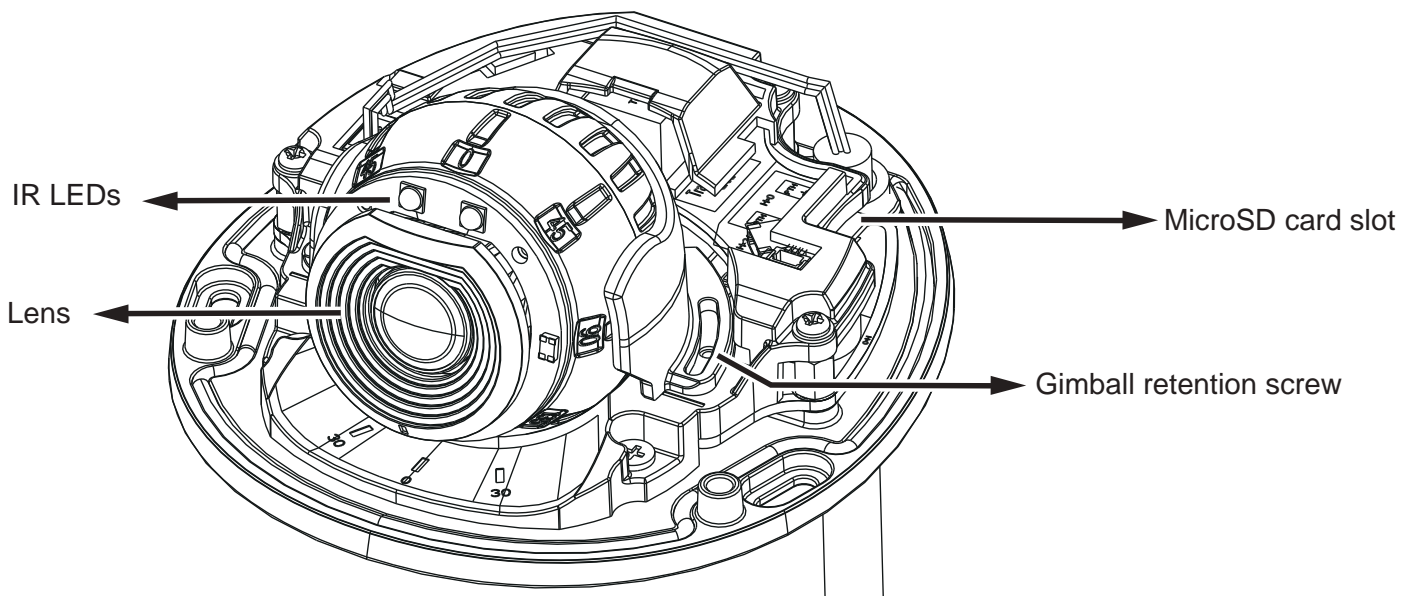
n'utilisez la caméra qu'avec un bloc d'alimentation CC homologué UL, ainsi qu'avec une alimentation limitée (LPS) certifiée. Le bloc d'alimentation doit porter les indications d'homologation UL et LPS. Il doit également répondre aux exigences en matière de sécurité et de conformité relatives au pays d'utilisation.

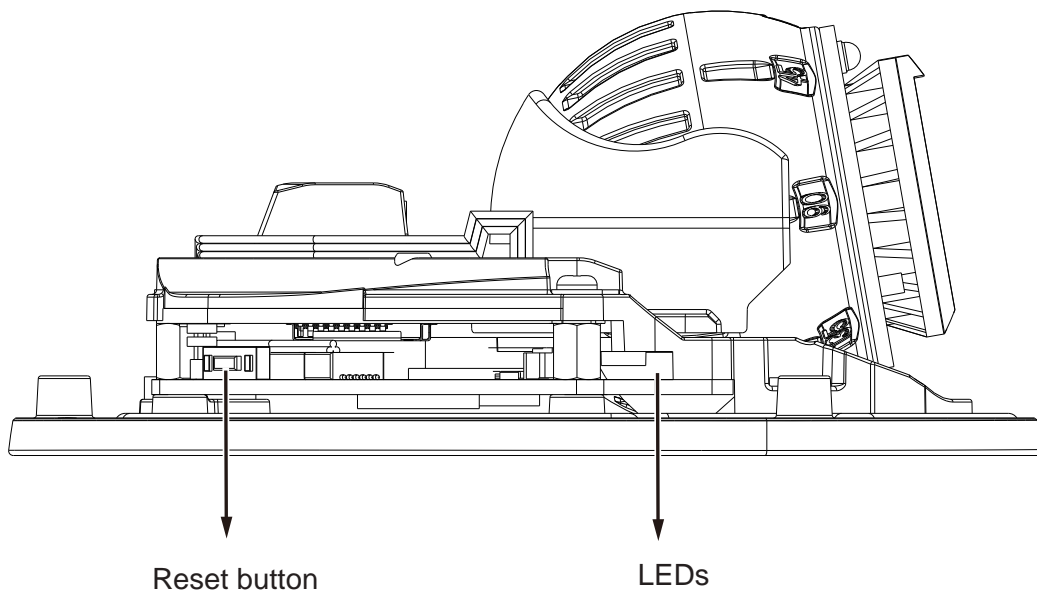
## Physical Description

### Outer View

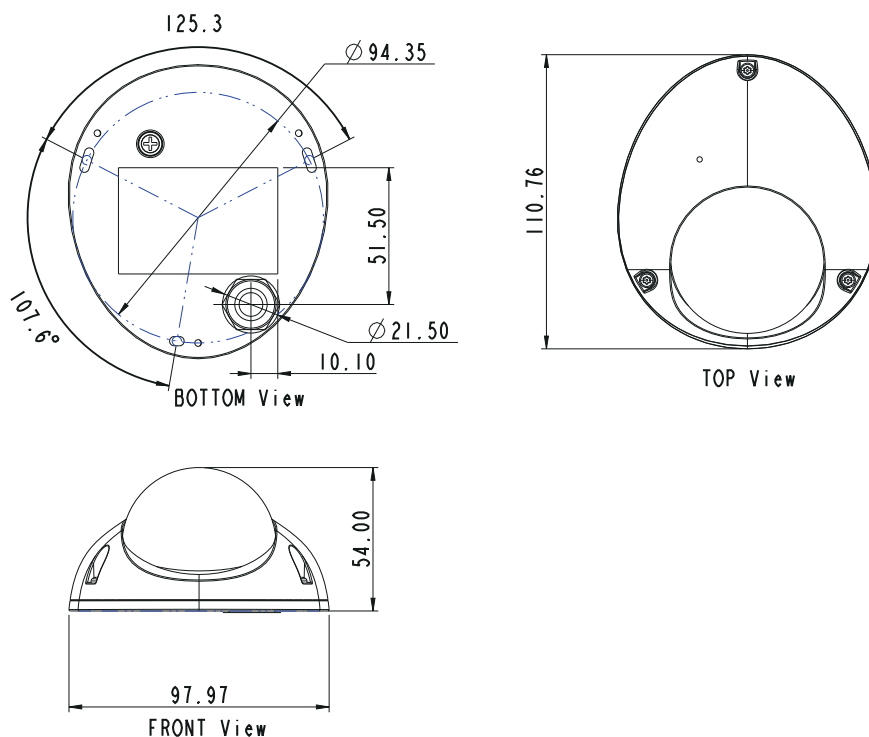


### Inner View





**Dimension Drawing**



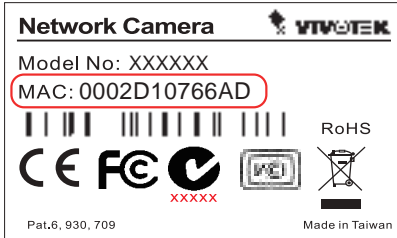
**NOTE:**

Some of the suffix syntax used in model naming are listed below:

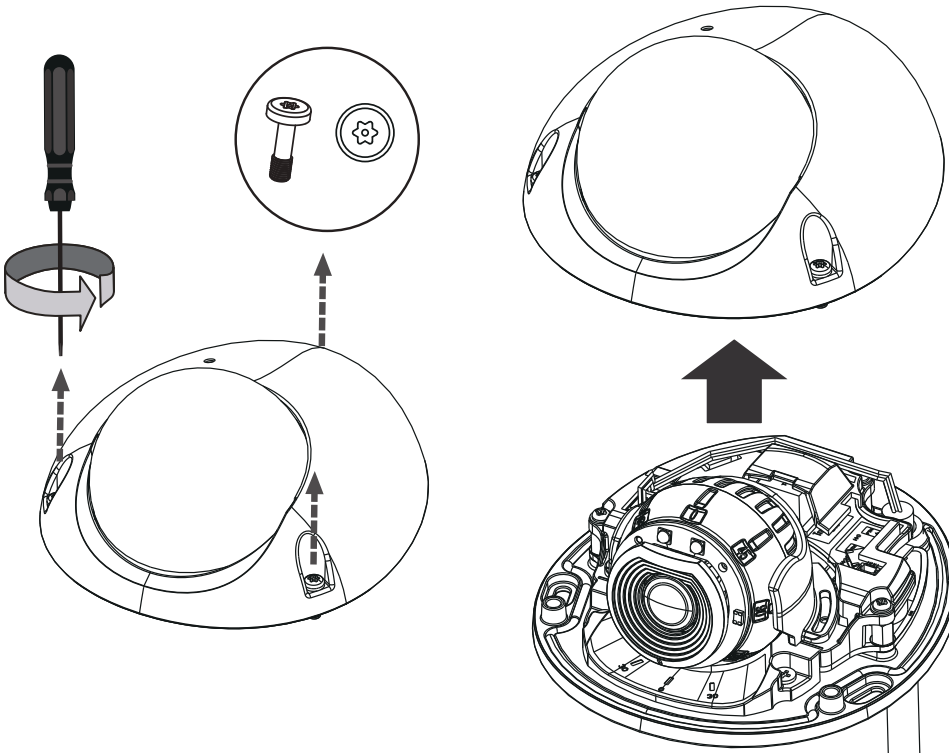
E	w/ heater for extreme weather
Fx	Focal length w/ number
T	w/ Remote focus lens
R	w/ PoE repeater
H	w/ High Dynamic Range functionality

## Hardware Installation

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

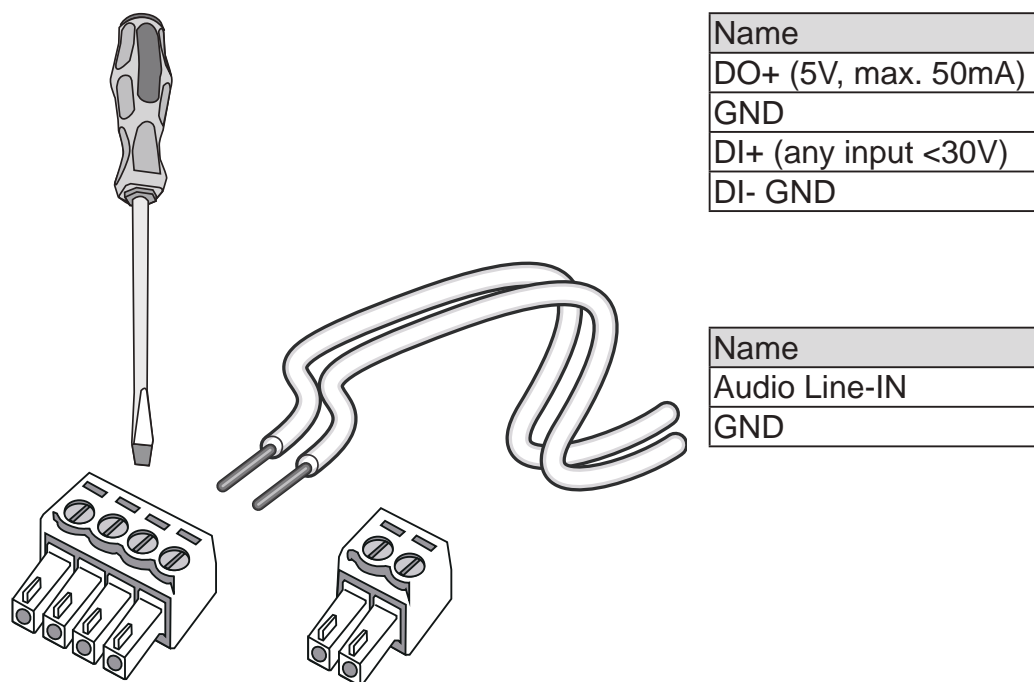


2. Open the top cover by loosening the T10 anti-tamper screws.

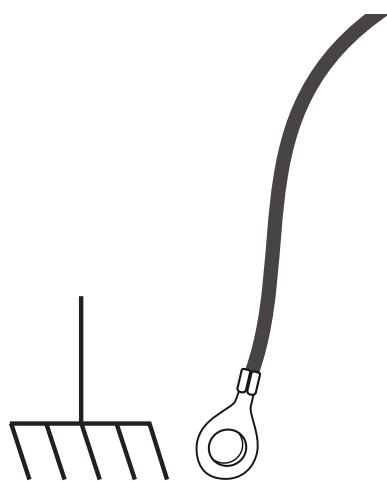




3. Connect the DI/DO and audio line in wires.

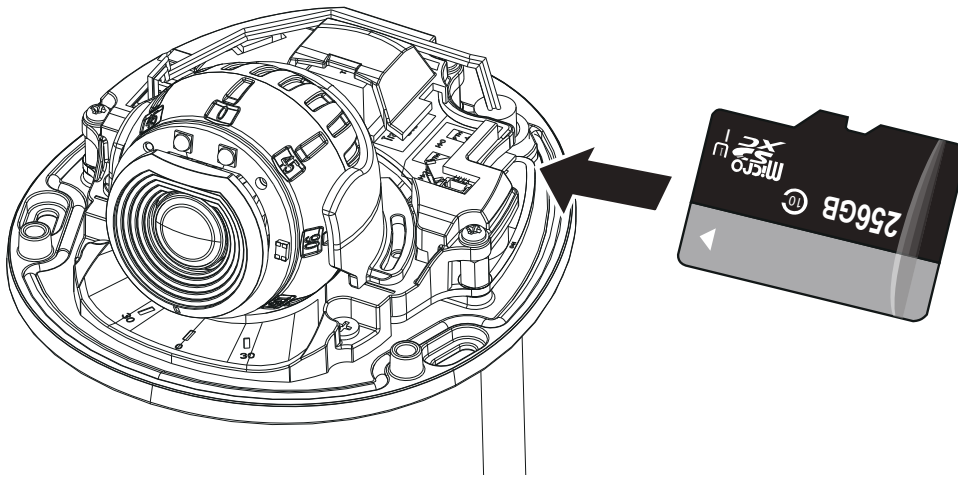


4. Connect the ground wire to an appropriate grounding connection.

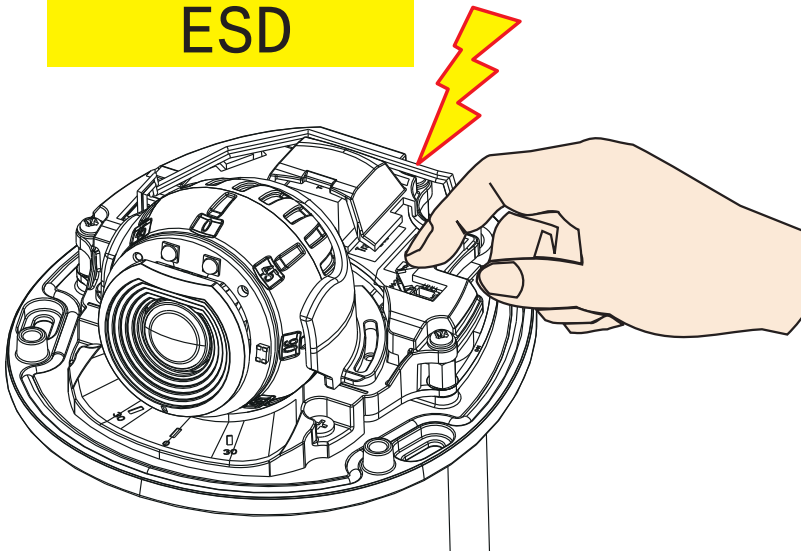


to ground

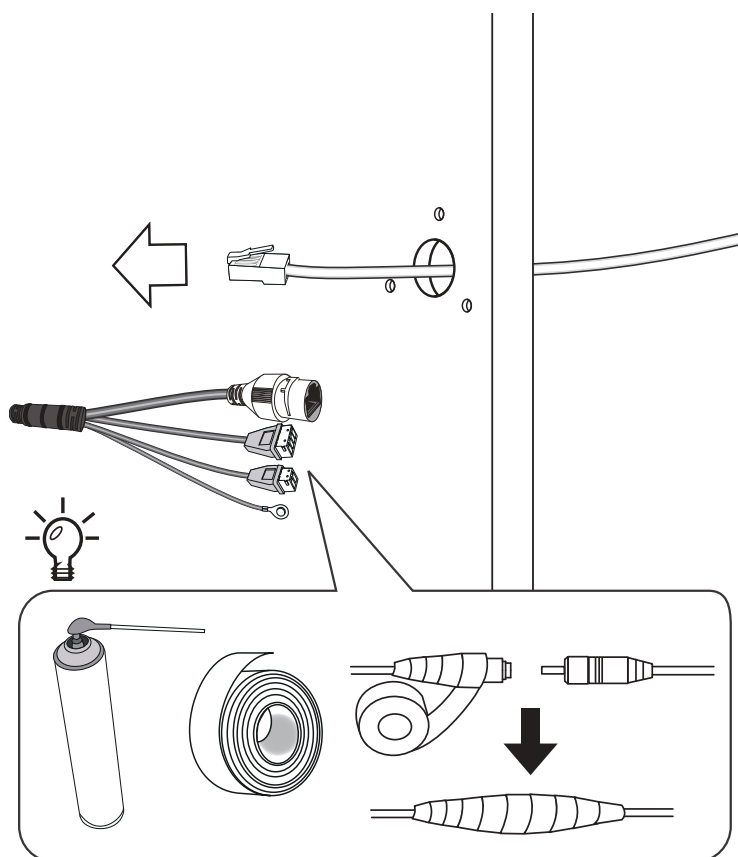
5. Install a MicroSD card if onboard storage is preferred.



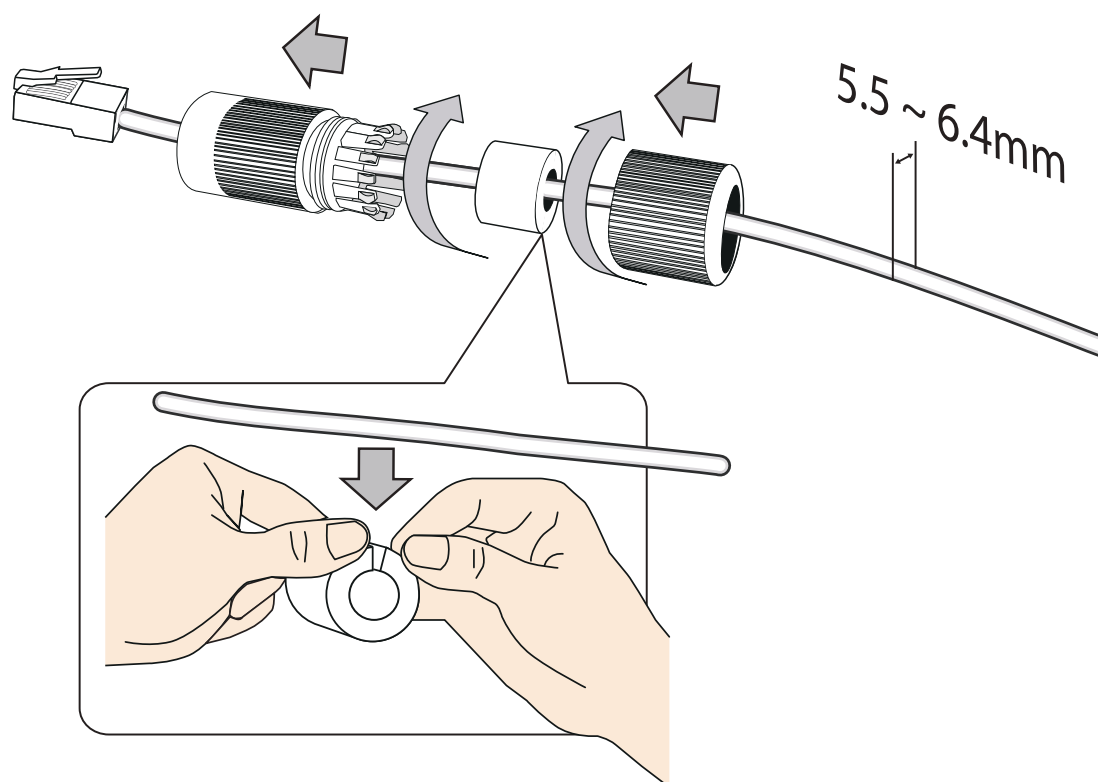
Avoid touching the circuit board to prevent the damage from electro-static discharge. If available, it is recommended to wear an anti-static wrist band.



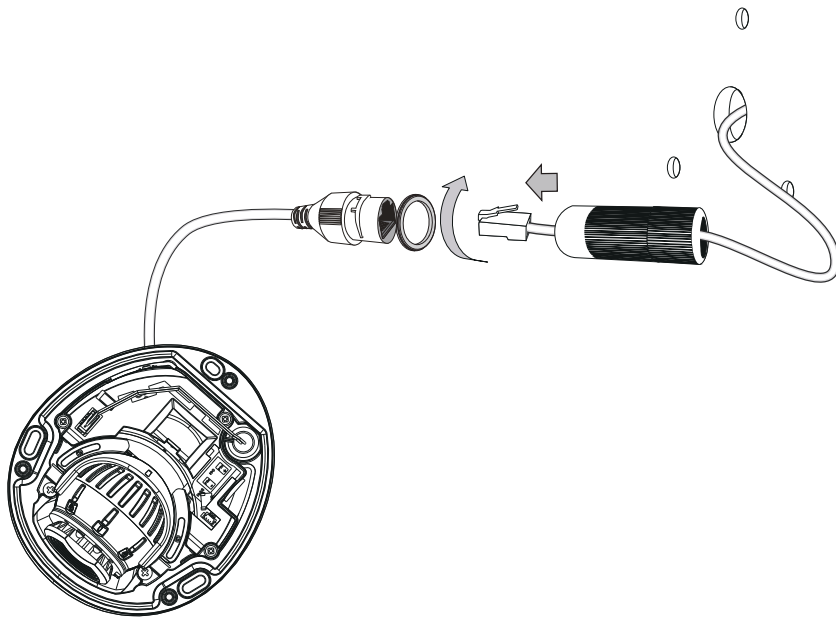
6. If external wiring is made, make sure the connections are waterproof by applying putties or tapes to seal the connections.



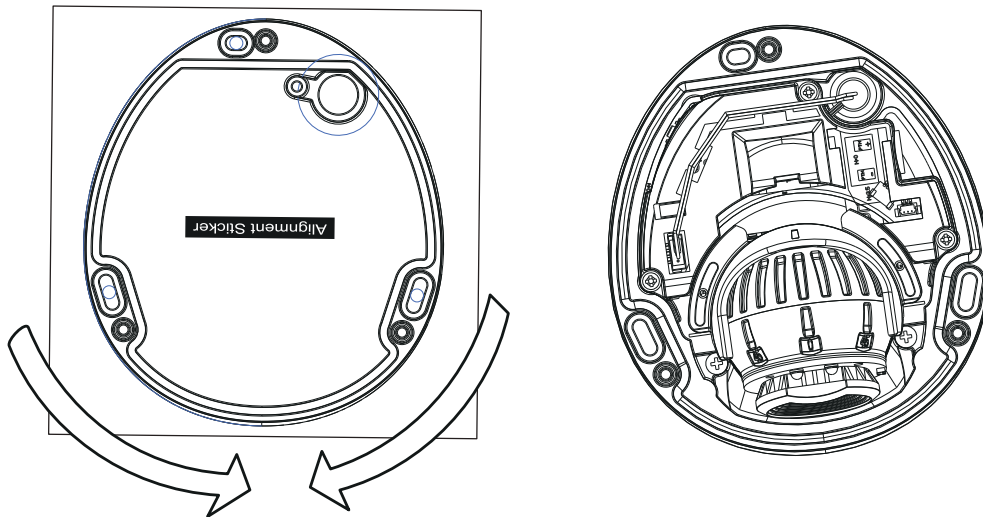
7. Pass an Ethernet cable through the waterproof cable gland components, and through the rubber seal as shown below. Connect the Ethernet cable to the camera's RJ45 connector.



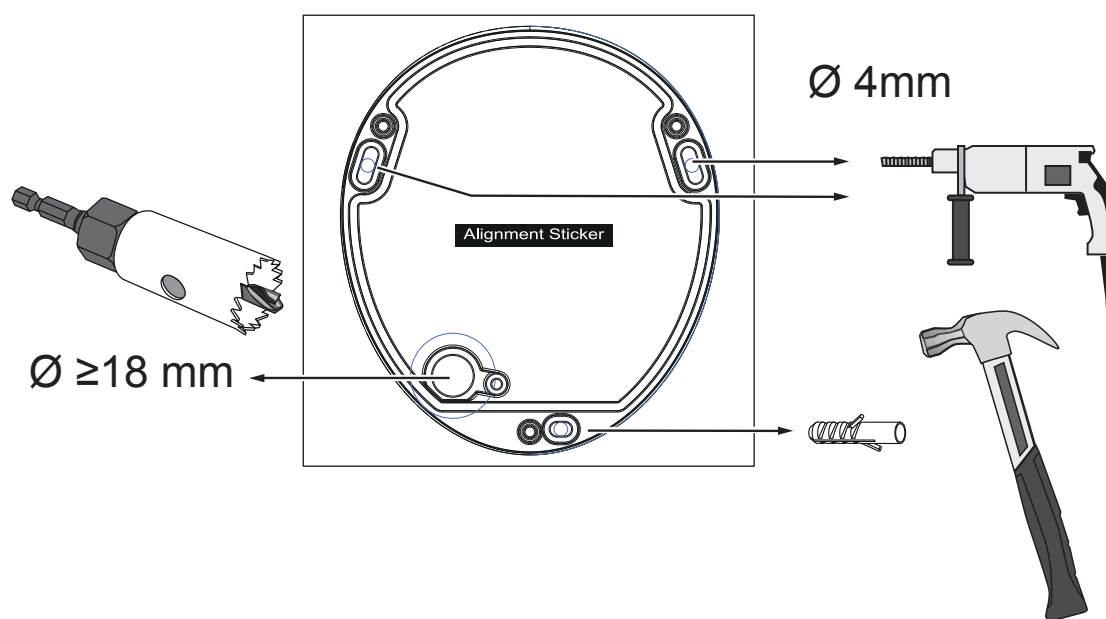
8. Install the seal ring and tighten the waterproof components.



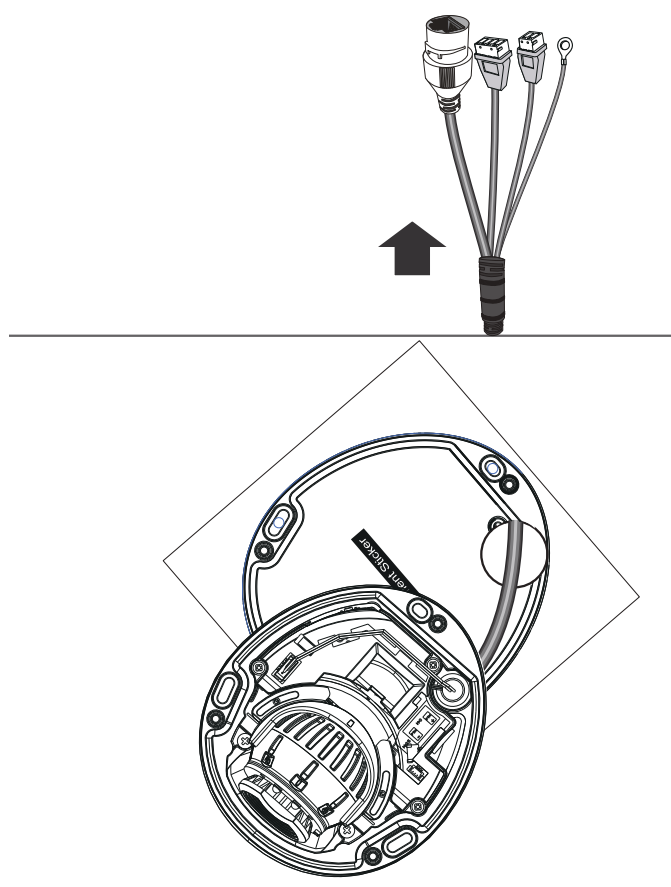
9. Use the alignment sticker to drill mounting holes on the wall or ceiling. Drill a cabling routing hole if preferred.



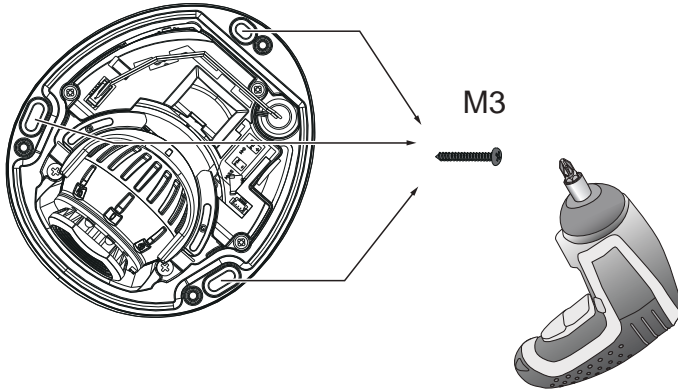
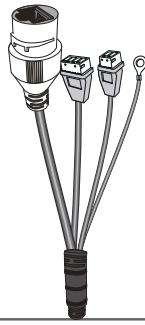
10. Install the camera to wall using the included screws.



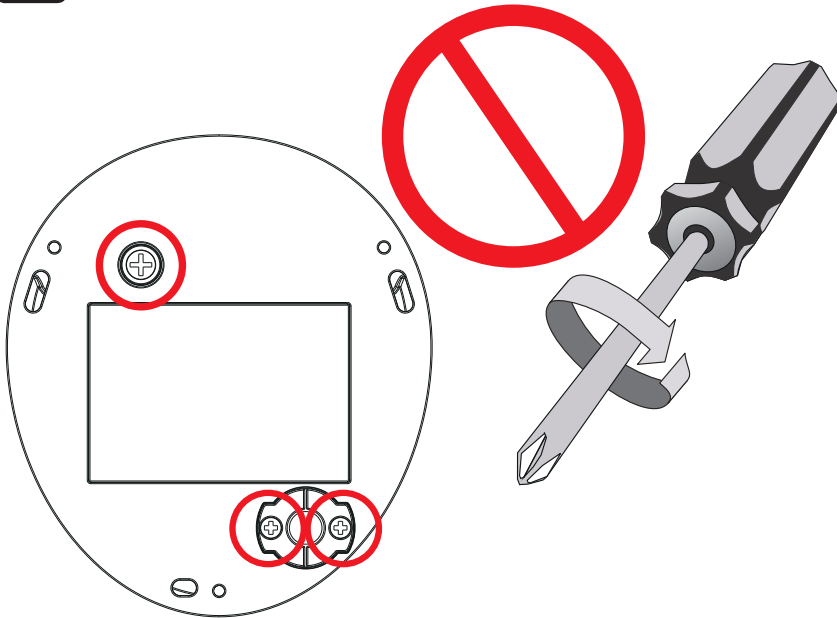
11. Route cables through the routing hole.



12. Secure the camera to wall or ceiling using the included M3 screws.

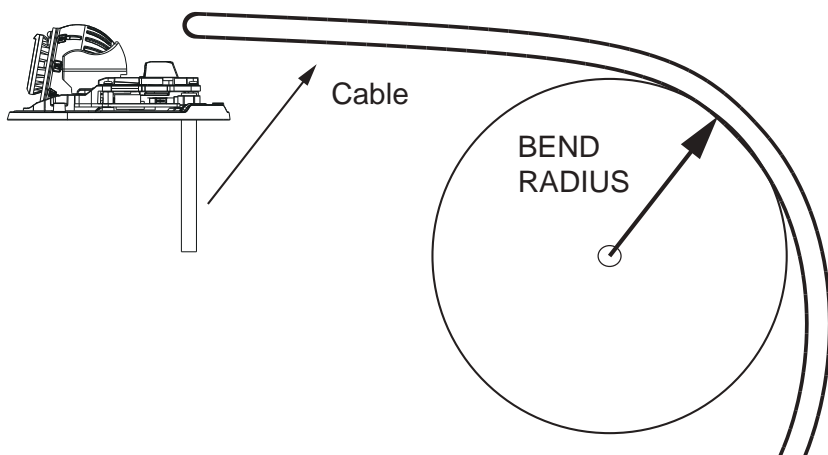


Please do not loosen these screws. These screws are used as assembly components.





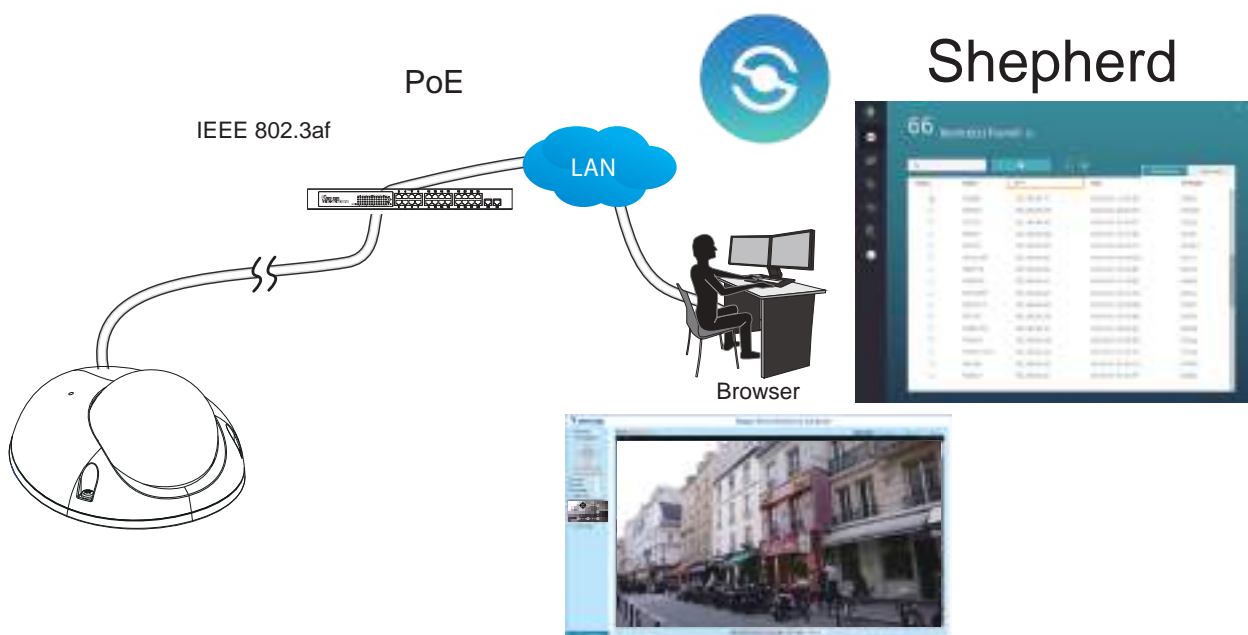
The cable assembly can be rigid, please note the bend radius if you need to pass it through a narrow space. Do not fold the cable.



Cable min. bend radius    67.5mm (9x O.D.) during installation  
    37.5mm (5x O.D.) during operation

13. Please visit VIVOTEK’s website to Install the "Shepherd" software utility. The program will search for VIVOTEK Video Receivers, Video Servers or Network Cameras on the same LAN.

Double-click on the camera’s MAC address to open a web console to the camera.



## Software Installation

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



13-1. Run the Shepherd utility.

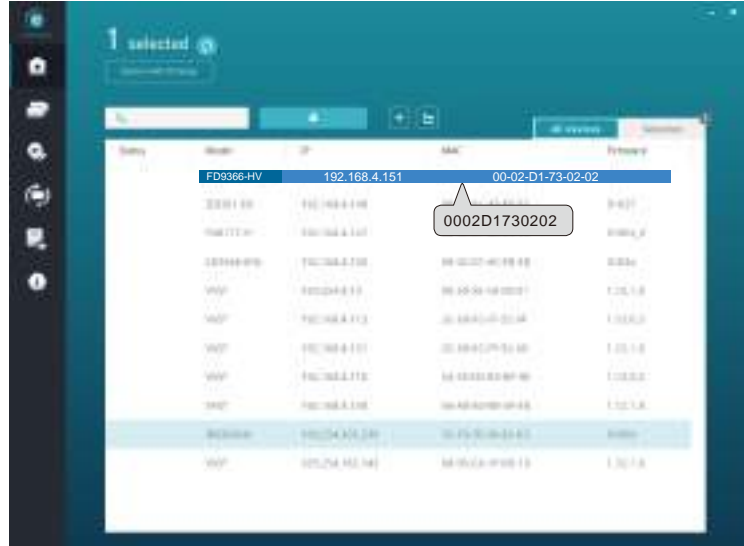
13-2. The program will conduct an analysis of your network environment.





13-3. The program will search for all VIVOTEK network devices on the same LAN.

13-4. After a brief search, the installer window will prompt. Click on the MAC and model name that matches the one printed on the product label. You can then double-click on the address to open a management session with the Network Camera.



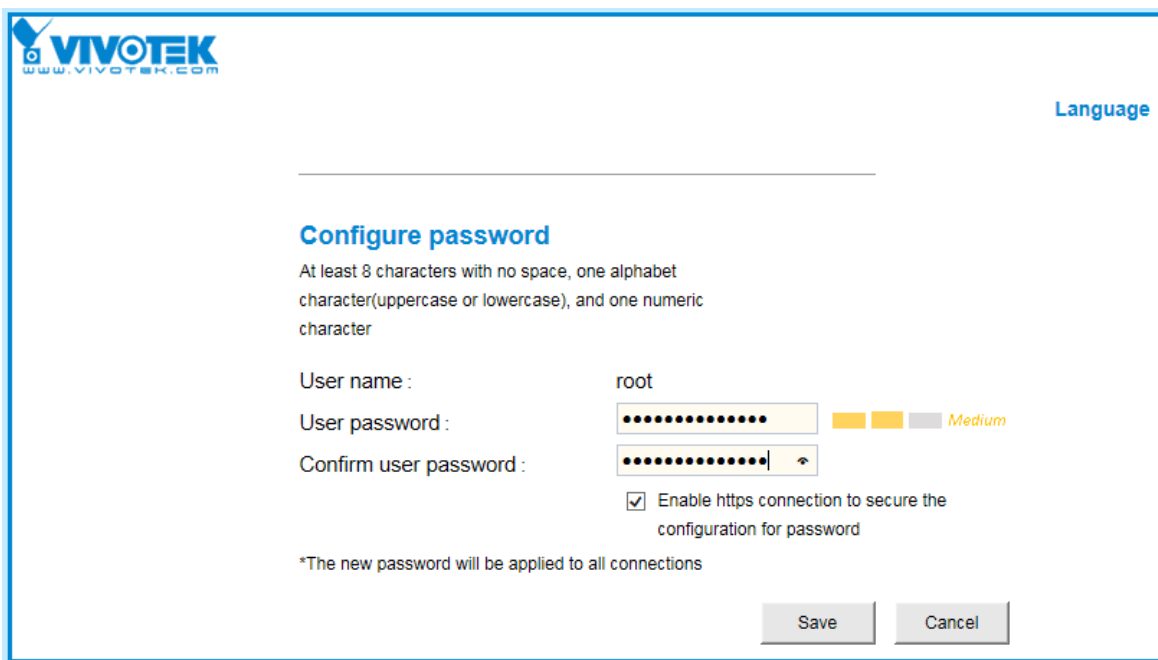
## Forceful Password Configuration

14. The first time you log in to the camera, the firmware will prompt for a password configuration for security concerns.

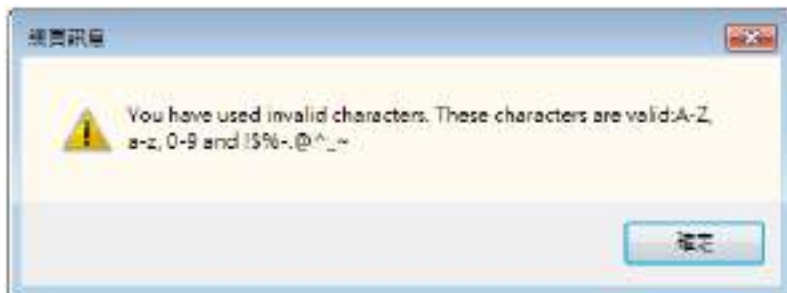
14-1. Since your camera is used for the first time, there is no password. Enter “root” as the user name, and nothing for the password.



14-2. Enter the combination of alphabetic and numeric characters to fulfill the password strength requirement. The default name for the camera administrator is “root”, and can not be changed.



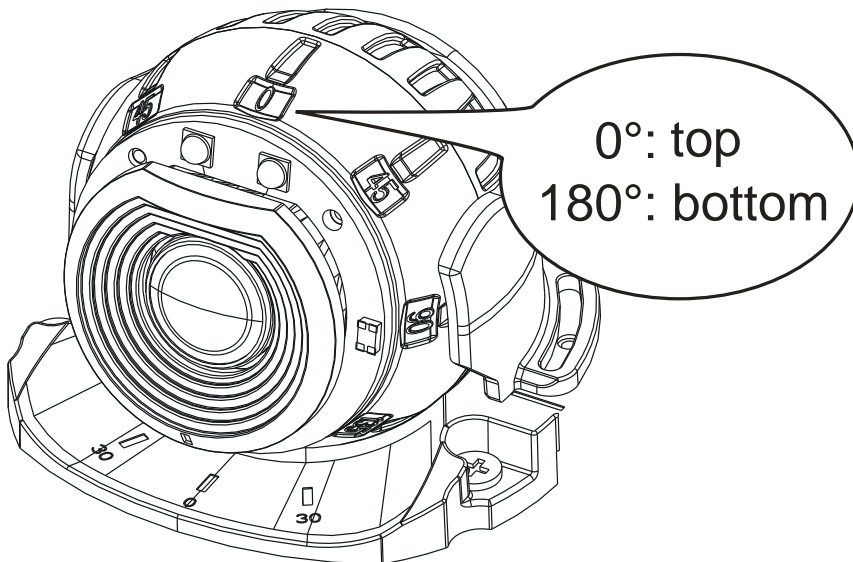
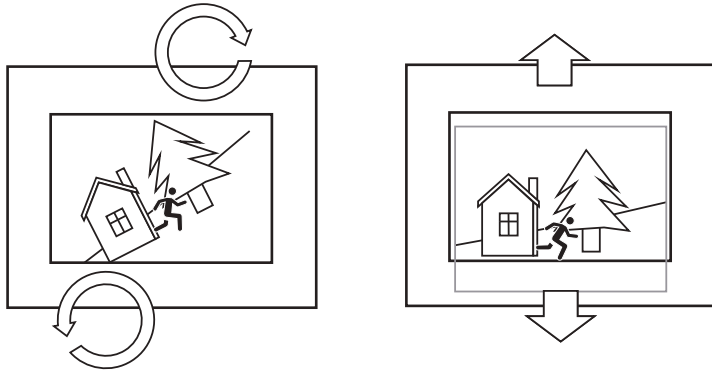
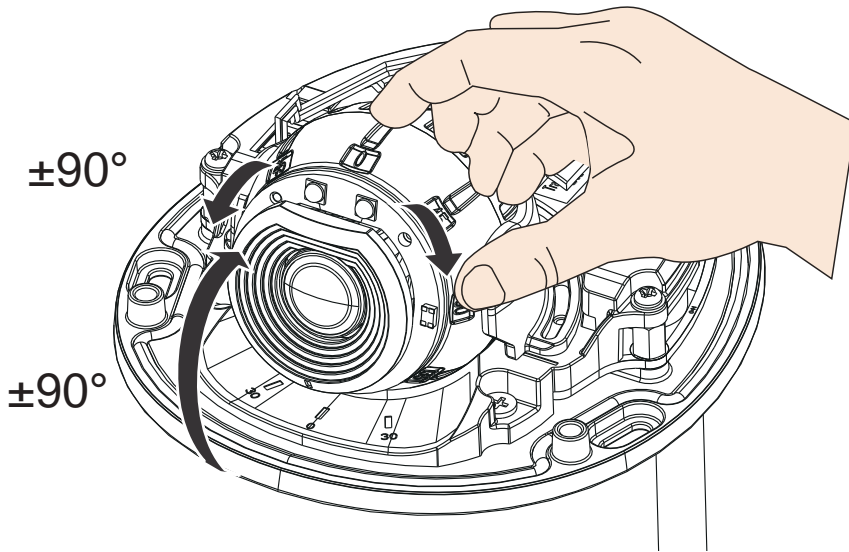
Some, but not all special ASCII characters are supported: !, \$, %, -, ., @, ^, \_, and ~. You can use them in the password combination.



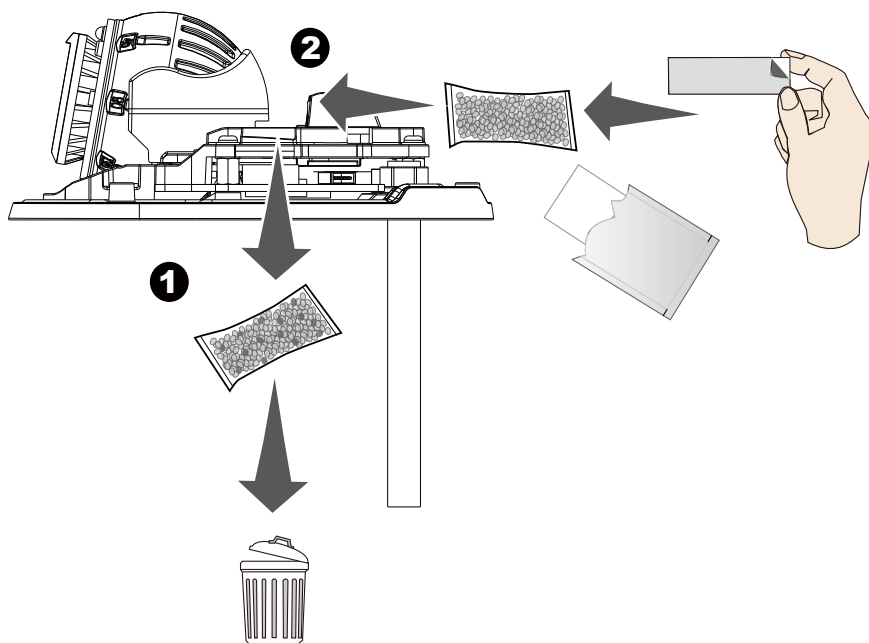
14-3. Another prompt will request for the password you just configured. Enter the password and then you can start configure your camera and see the live view.



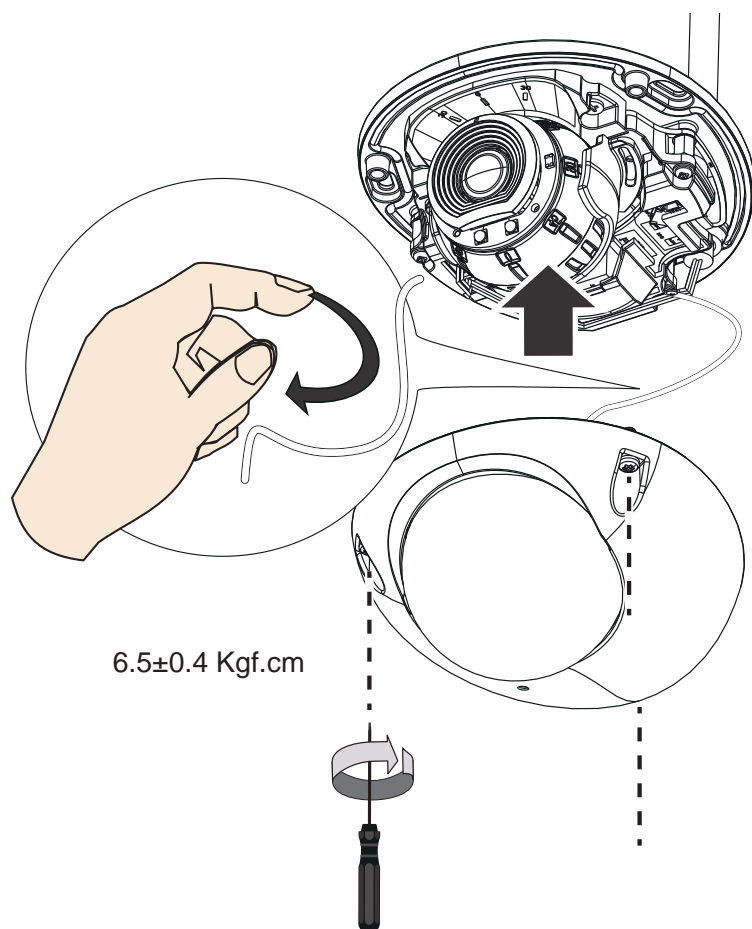
15. With a live view on your computer, rotate, pan, or tilt the camera until you acquire an optimal field of view.



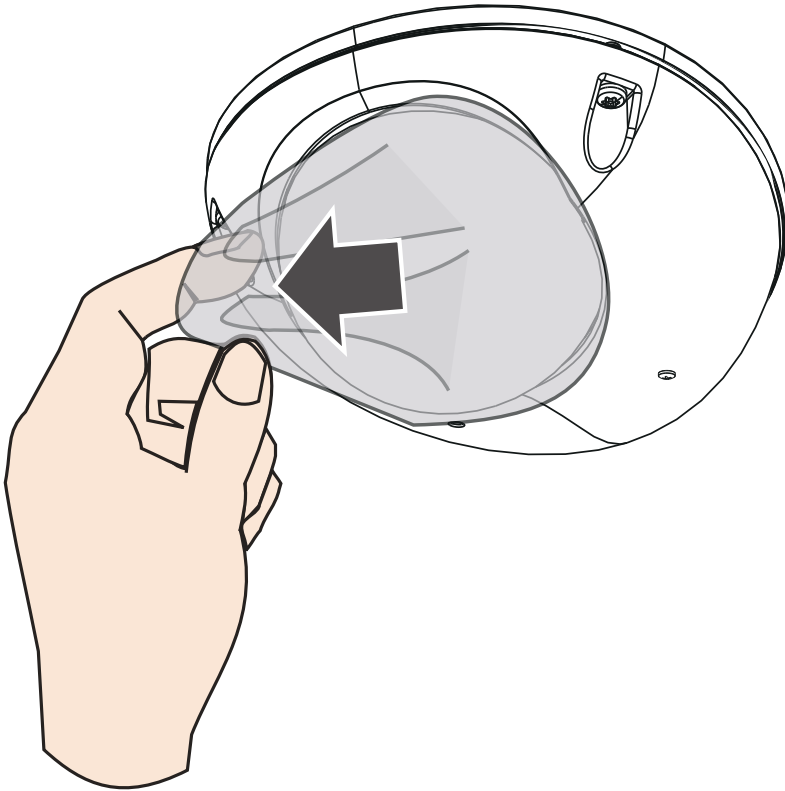
16. Replace the desiccant from the inside of the dome cover.



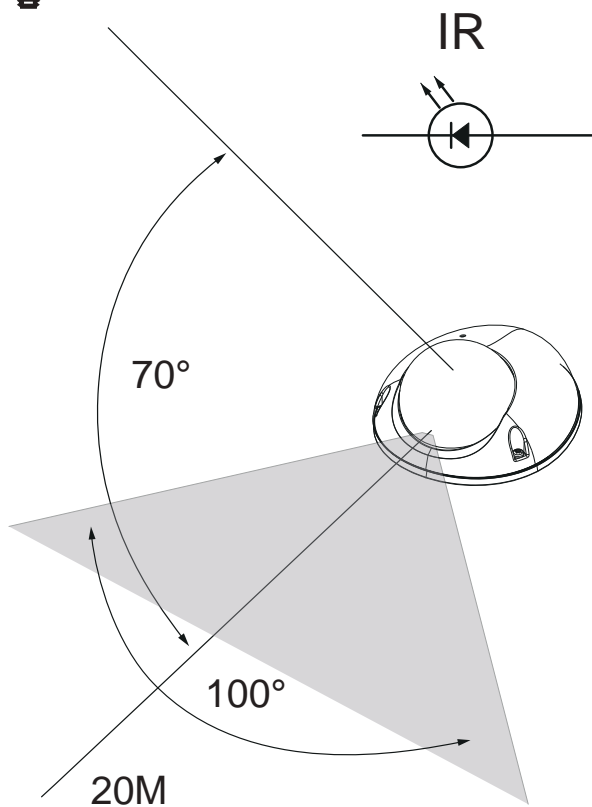
17. Install the dome cover. Note that you should carefully fit the tether wire in case it will get in the way between the top cover and the edge of camera main body.



18. Remove the protective sheet from the dome cover.



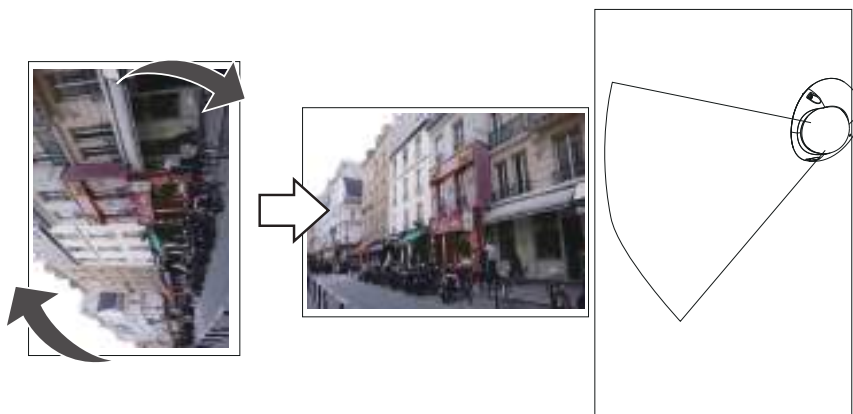
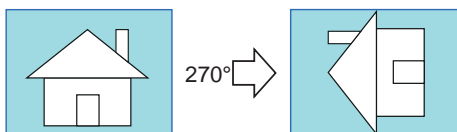
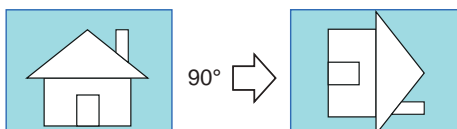
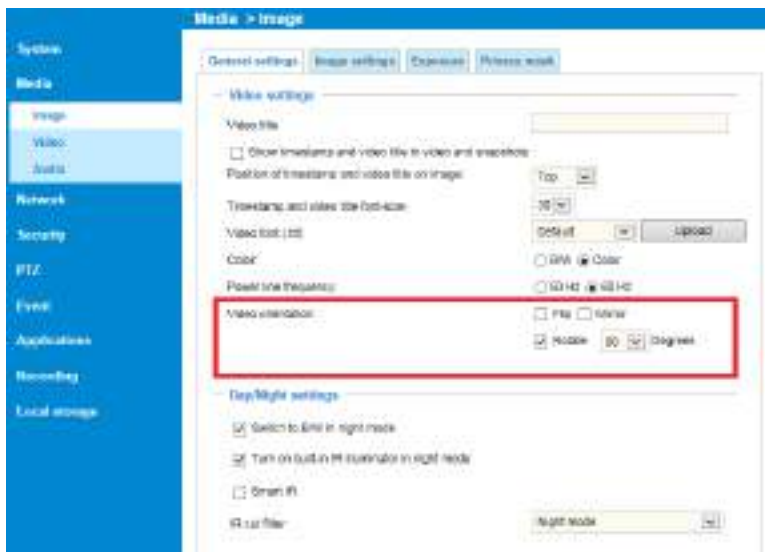
Below is the coverage range of the IR illuminator.





If the need should arise, you can rotate your image. For example, if you install the camera on a wall and you need to cover a long narrow corridor.

### Configuration > Media > Image > General Settings



## Hardware Reset

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

**Reset:** Press the recessed reset button. Wait for the Network Camera to reboot.

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

## MicroSD/SDHC/SDXC Card Capacity

This network camera is compliant with **MicroSD/SDHC/SDXC 16GB / 8GB / 32GB / 64GB / 128GB** and other preceding standard SD cards.

## LED Definitions

	Item	LED status	Description
LED Definitions	1	Steady Red	Powered and system booting, or network failed
		Red LED off	Power off
		Green LED off	Network is disconnected
	2	Steady Red and Green LED blinks every 1 sec.	Connected to network
	3	Green LED blinks every 1 sec. and RED LED blinks consecutively every 0.15 sec.	Upgrading firmware
	4	Green and RED blink every 0.15 sec, Green and RED light on, then blink again.	Restoring defaults
	5	RED LED is on, Green LED blinks and RED LED is constantly on.	Status after a reset (network connected)
		Green and RED LEDs are constantly on.	Status after a reset (network disconnected)

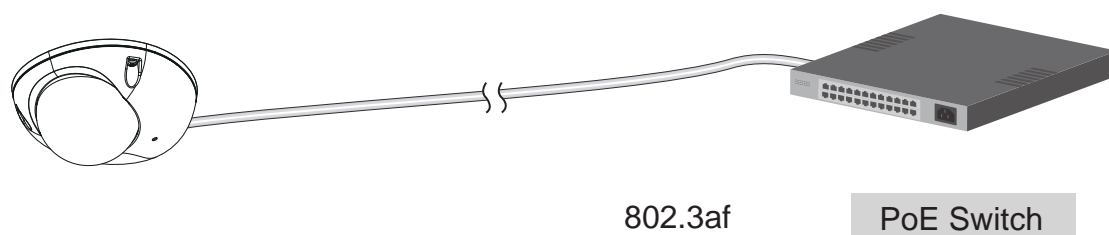


## Network Deployment

### General Connection (PoE)

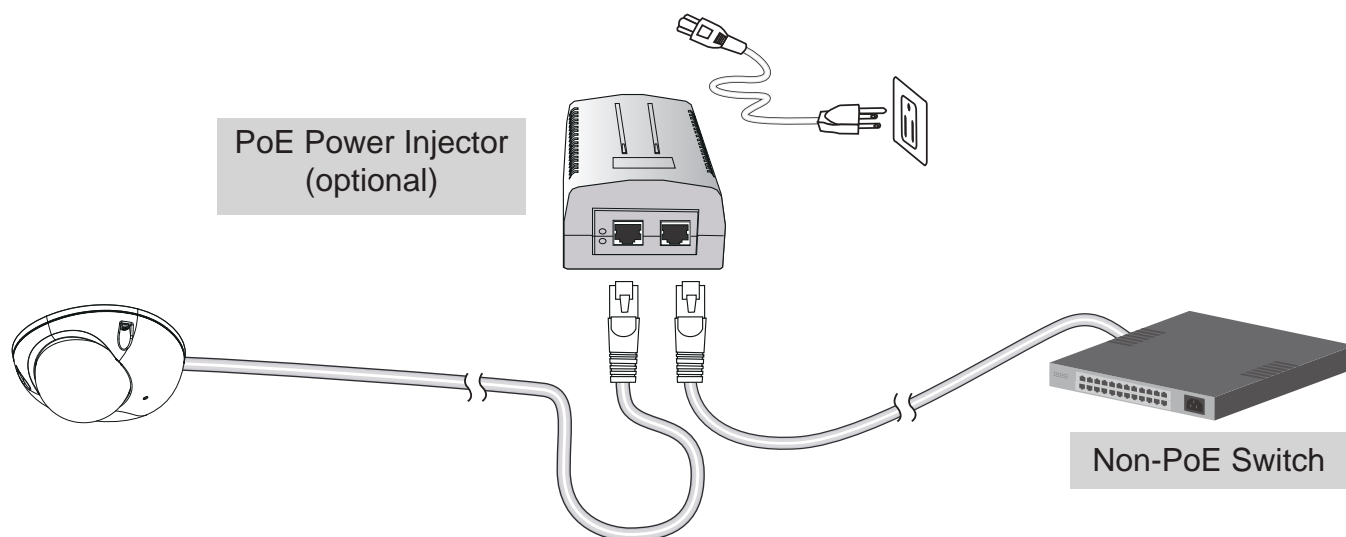
#### ● When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via Ethernet cable.



#### ● When using a non-PoE switch

Use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



#### NOTE:

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

## Ready to Use

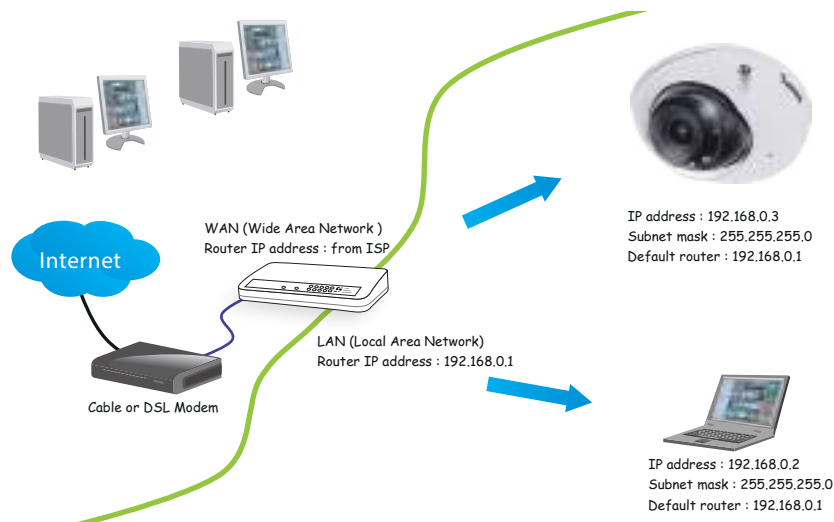
1. A browser session to the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the VAST recording software from VIVOTEK's website in a deployment consisting of multiple cameras. For its installation details, please refer to its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



## Internet connection via a router

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

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 20 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

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

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

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 82 for details.

## Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN setting on page 81 for details.

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

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 82 for details.

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

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

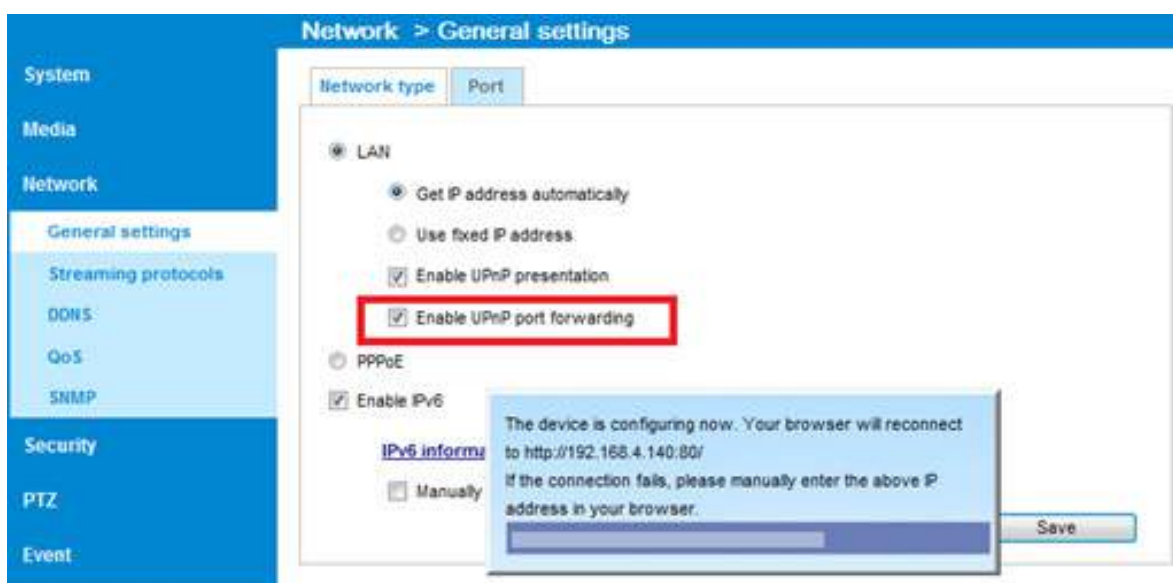
Configure the router, virtual server or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

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

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

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

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



# Accessing the Network Camera

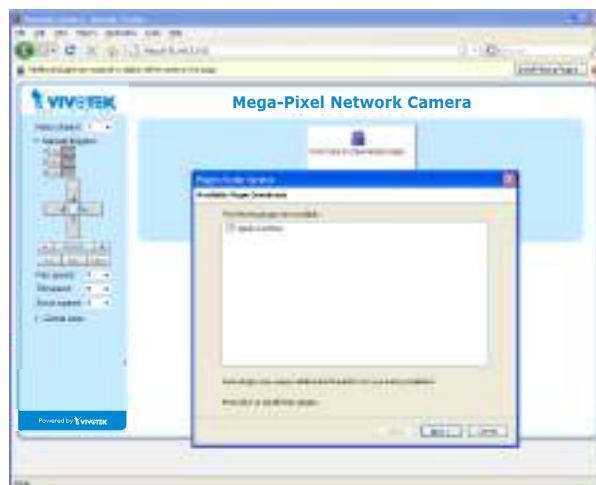
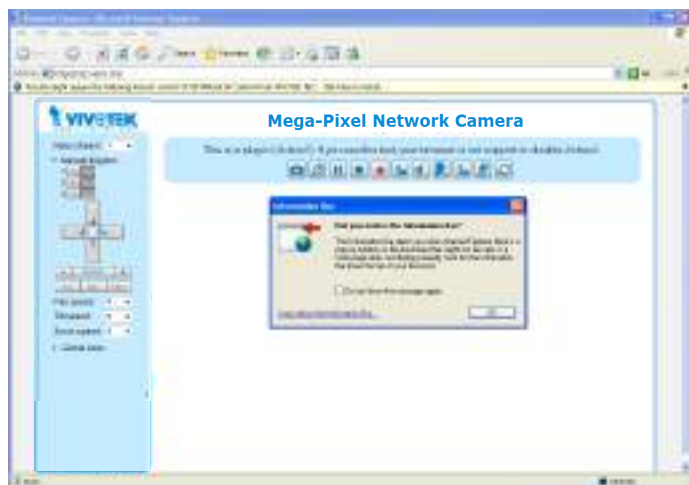
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

## Using Web Browsers

Use Installation Wizard 2 (IW2) to access the Network Cameras on LAN.

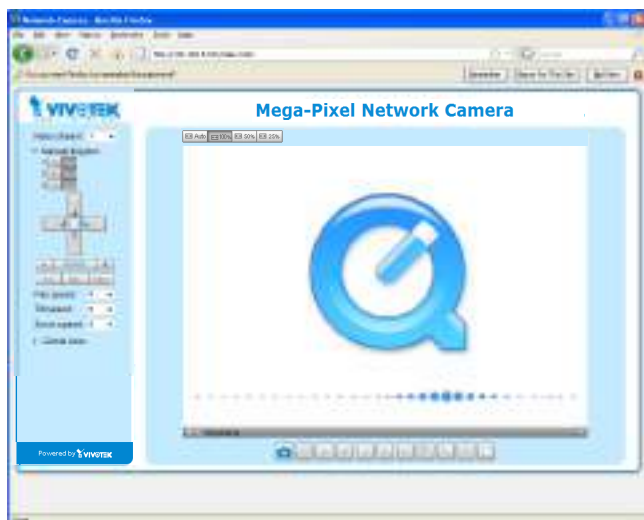
If your network environment is not a LAN, follow these steps to access the Network Camera:

1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. Live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will prompt as shown below. Follow the instructions to install the required plug-in on your computer.



### NOTE:

- For Mozilla Firefox or Chrome users, your browser will use QuickTime to stream the live video. If you don't have QuickTime on your computer, please download it first, then launch the web browser.



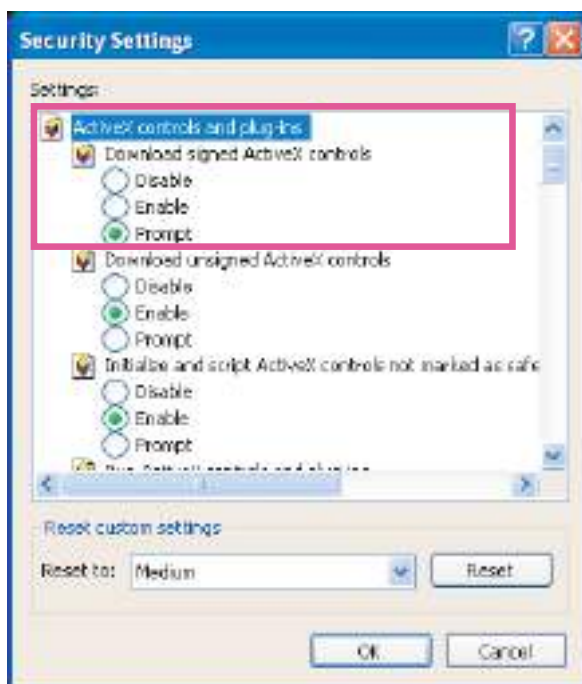
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera. For more information about how to enable password protection, please refer to Security on page 100.*

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

1. *Choose Tools > Internet Options > Security > Custom Level.*



2. *Look for Download signed ActiveX® controls; select Enable or Prompt. Click OK.*



3. *Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.*

**! IMPORTANT:**

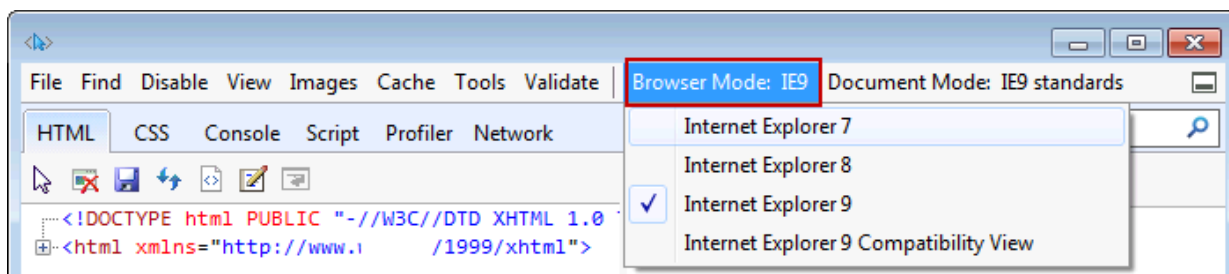
- Currently the Network Camera utilizes a 32-bit ActiveX plugin. You CAN NOT open a management/view session with the camera using a 64-bit IE browser.
- If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\SysWOW64. A 32-bit version of IE browser will be installed.
- On Windows 7, the 32-bit explorer browser can be accessed from here:  
[C:\Program Files \(x86\)\Internet Explorer\Iexplore.exe](C:\Program Files (x86)\Internet Explorer\Iexplore.exe)
- If you open a web session from the Shepherd utility, a 32-bit IE browser will be opened.

**💡 Tips:**

1. The onscreen Java control can malfunction under the following situations: A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.
2. If you encounter problems with displaying the configuration menus or UI items, try disable the Compatibility View on IE8 or IE9.



You may also press the F12 key to open the developer tools utility, and then change the Browser Mode to the genuine IE8 or IE9 mode.



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



## Using RTSP Players

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



QuickTime Player

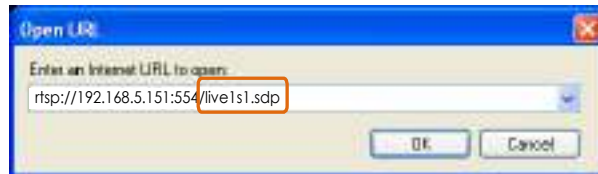


VLC media player

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

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 89.

For example:



4. The live video will be displayed in your player.  
For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 88 for details.





## Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 25.

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

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.  
For more information, please refer to RTSP Streaming on page 89.
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video streaming parameters as listed below.  
For more information, please refer to Stream settings on page 70.

Video Mode	H.264
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps

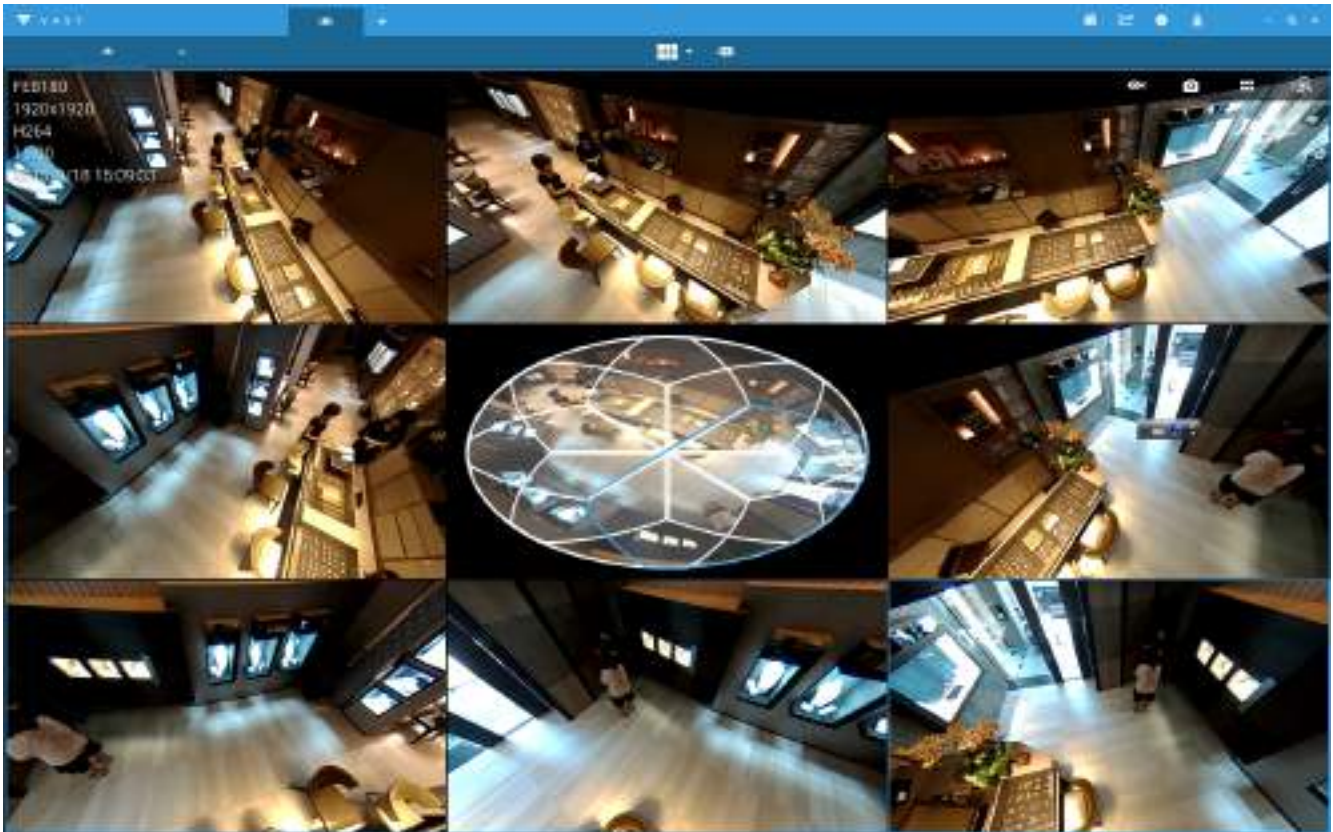
3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 89.
4. Launch the player on the 3GPP-compatible mobile devices (e.g., QuickTime).
5. Type the following URL commands into the player.  
The address format is `rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream # with small frame size and frame rate>`.  
For example:



You can configure Stream #2 into the suggested stream settings as listed above for live viewing on a mobile device.

## Using VIVOTEK Recording Software

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



### Tips:

1. If you encounter problems with displaying live view or the onscreen plug-in control, you may try to remove the plug-ins that might have been installed on your computer. Remove the following folder: C:\Program Files (x86)\Camera Stream Controller\.
2. If you forget the root (administrator) password for the camera, you can restore the camera defaults by pressing the reset button for longer than 5 seconds.
3. If DHCP is enabled in your network, and the camera cannot be accessed, run the Shepherd utility to search the network. If the camera has been configured with fixed IP that does not comply with your local network, you may see its default IP 169.254.x.x. If you still cannot find the camera, you can restore the camera to its factory defaults.
4. If you change your network parameters, e.g., added a connection to a LAN card, re-start the Shepherd utility.

# Main Page

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



## VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

## Host Name

The host name can be customized to fit your needs. The name can be changed especially there are many cameras in your surveillance deployment. For more information, please refer to System on page 46.

## Camera Control Area

**Video Stream:** This Network Camera supports multiple streams (streams 1 and 2) simultaneously. You can select any of them for live viewing. For more information about multiple streams, please refer to page 70 for detailed information.

**Manual Trigger:** Click to enable/disable an event trigger manually. Please configure an event setting on the Application page before you enable this function. A total of 3 event configuration can be configured. For more information about event setting, please refer to page 118. If you want to hide this item on the homepage, please go to **Configuration > System > Homepage Layout > General settings > Customized button** to deselect the "show manual trigger button" checkbox.

## Configuration Area

**Client Settings:** Click this button to access the client setting page. For more information, please refer to Client Settings on page 40.

**Configuration:** Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 45.

**Language:** Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡體中文, and 繁體中文. Please note that you can also change a language on the Configuration page; please refer to page 45.

## Hide Button

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

## Resize Buttons



Click the Auto button, the video cell will resize automatically to fit the monitor.

Click 100% is to display the original homepage size.

Click 50% is to resize the homepage to 50% of its original size.

Click 25% is to resize the homepage to 25% of its original size.

## Live Video Window

- The following window is displayed when the video mode is set to H.264 or H.265:  
H.265/264 Protocol and Media Options



**Video Title:** The video title can be configured. For more information, please refer to Video Settings on page 58.

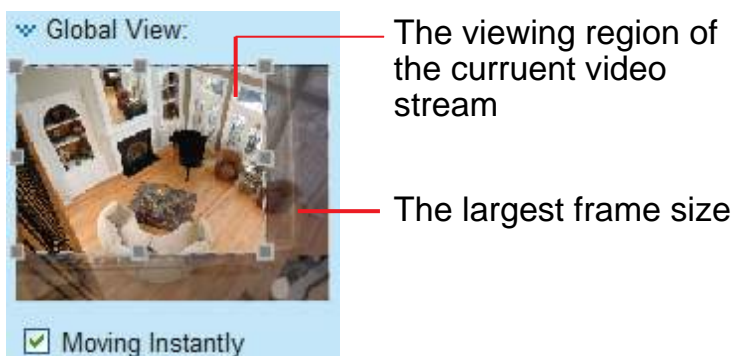
**H.264 or H. 265 Protocol and Media Options:** The transmission protocol and media options for H.264 or H.265 video streaming. For further configuration, please refer to Client Settings on page 40.

**Time:** Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 58.

**Title and Time:** The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 63.


**PTZ Panel:** This Network Camera supports “digital” (e-PTZ) pan/tilt/zoom control, which allows roaming a smaller view frame within a large view frame. Please refer to PTZ settings on page 115 for detailed information.


**Global View:** Click on this item to display the Global View window. 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, please refer to E-PTZ Operation on page 115. For more information about how to set up the viewing region of the current video stream, please refer to page 115.





Note that 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.



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



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



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







 **Pause:** Pause the transmission of the streaming media. The button becomes the  **Resume** button after clicking the Pause button.



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




 **Start MP4 Recording:** Click this button to record video clips in MP4 file format to your computer. Press the  **Stop MP4 Recording** button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 41 for details.


 **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.

 **Talk:** Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button  again to end talking transmission.

 **Mic Volume:** When the  **Mute** function is not activated, move the slider bar to adjust the microphone volume on the local computer.

 **Mute:** Turn off the  **Mic volume** on the local computer. The button becomes the  **Mic 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.

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





**Video Title:** The video title can be configured. For more information, please refer to Media > Image on page 63.

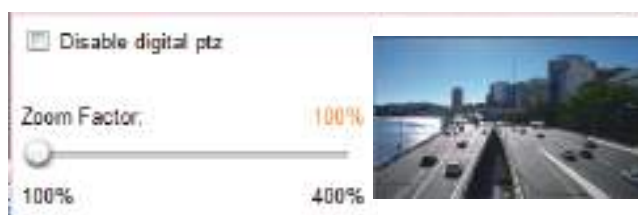
**Time:** Display the current time. For more information, please refer to Media > Image on page 63.



**Title and Time:** Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 63.


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

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

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



 **Start MP4 Recording:** Click this button to record video clips in MP4 file format to your computer. Press the  **Stop MP4 Recording** button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 41 for details.

 **Full Screen:** Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

# Client Settings

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

## H.265/H.264 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264.

## H.265/H.264 Protocol Options

H.265/H.264 protocol options

TCP

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

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

**UDP multicast:** This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 88.

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

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




## MP4 Saving Options

**MP4 saving options**

Folder:

File name prefix:

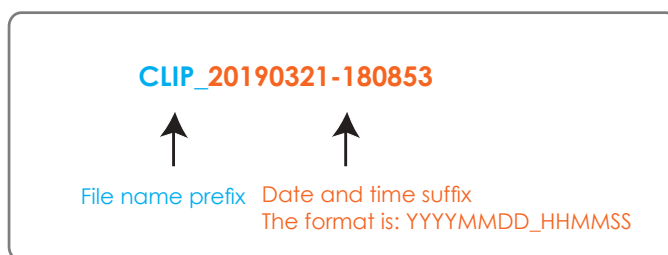
Add date and time suffix to file name

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

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

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

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



## Local Streaming Buffer Time

**Local streaming buffer time**

Millisecond

In the case of encountering unsteady bandwidth, live streaming may lag and video streaming may not be very smoothly. If you enable this option, the live streaming will be stored temporarily on your PC's cache memory for a few milli seconds before being played on the live viewing window. This will help you see the streaming more smoothly. If you enter 3,000 Millisecond, the streaming will delay for 3 seconds.

## Joystick settings

### Enable Joystick

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

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

1. Select a detected joystick, if there are multiple, from the Selected joystick menu. If your joystick is not detected, it may be defective.
2. Click Calibrate or Configure buttons to configure the joystick-related settings.

**Joystick settings**

Selected joystick: Macally AirStick



### NOTE:

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

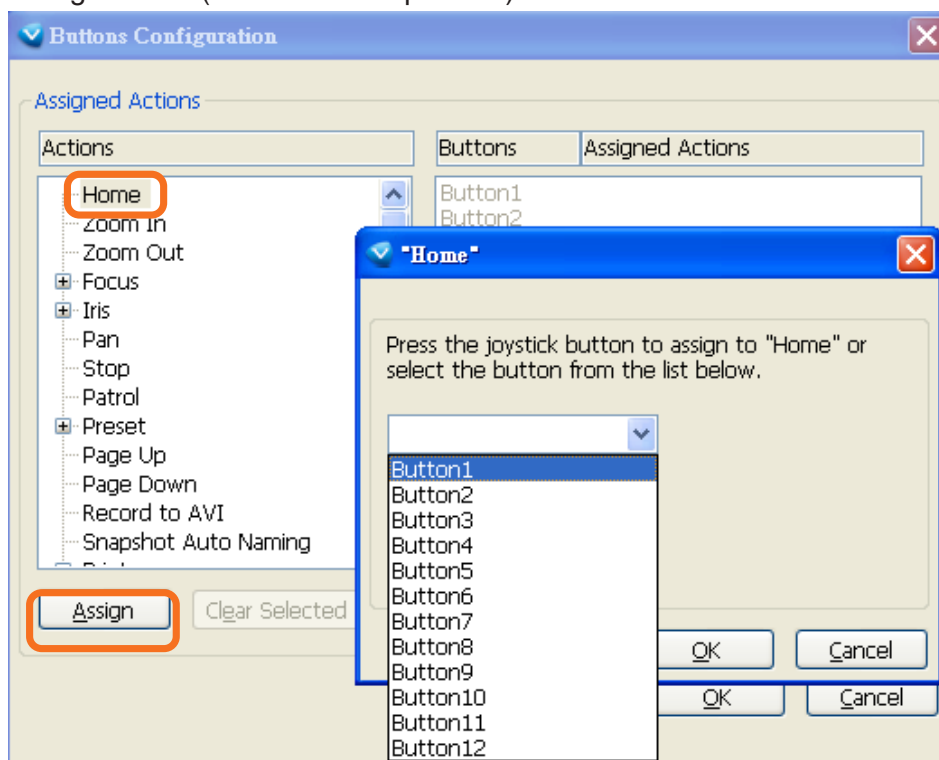


## Buttons Configuration

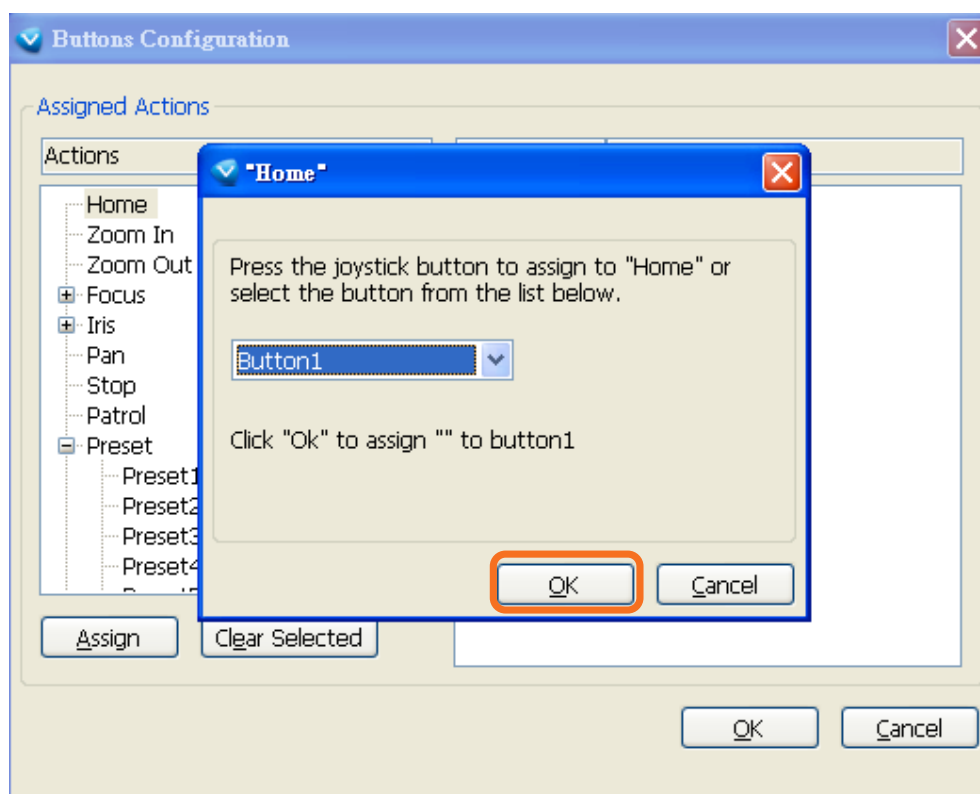
In the Button Configuration window, the left column shows the actions you can assign, and the right column shows the functional buttons and assigned actions. The number of buttons may differ from different joysticks.

Please follow the steps below to configure your joystick buttons:

1. Choosing one of the actions and click **Assign** will pop up a dialog. Then you can assign this action to a button by pressing the joystick button or select it from the drop-down list.  
For example: Assign **Home** (move to home position) to Button 1.



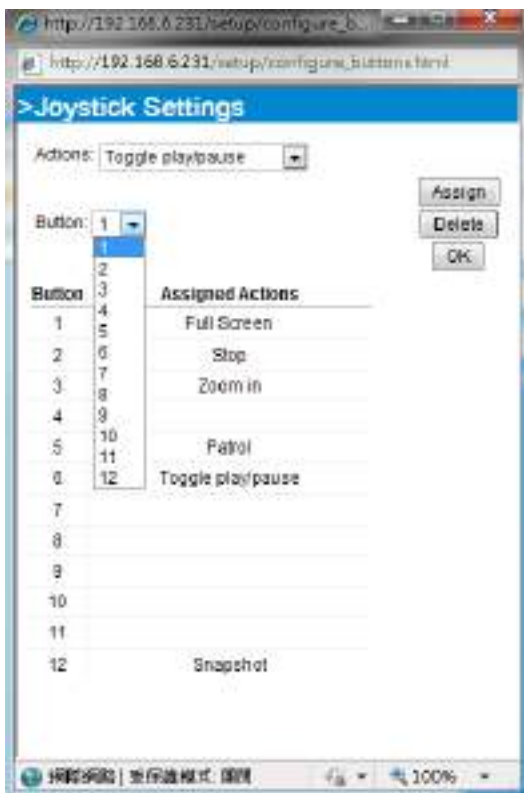
2. Click **OK** to confirm the configuration.



## Buttons Configuration

Click the **Configure Buttons** button, a window will prompt as shown below. Please follow the steps below to configure your joystick buttons:

1. Select a button number from the Button # pull-down menu.



### Tips:

If you are not sure of the locations of each button, use the **Properties** window in the **Game Controllers** utility.



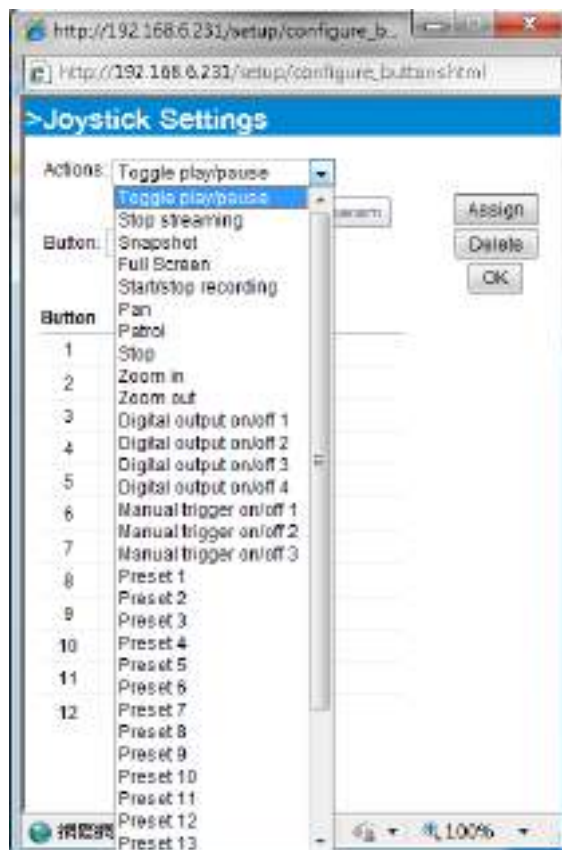
2. Select a corresponding action, such as Patrol or Preset#.

3. Click the **Assign** button to assign an action to the button. You can delete an association by selecting a button number, and then click the **Delete** button.

Repeat the process until you are done with the configuration of all preferred actions.

The buttons you define should appear on the button list accordingly.

4. Please remember to click the **Save** button on the Client settings page to preserve your settings.

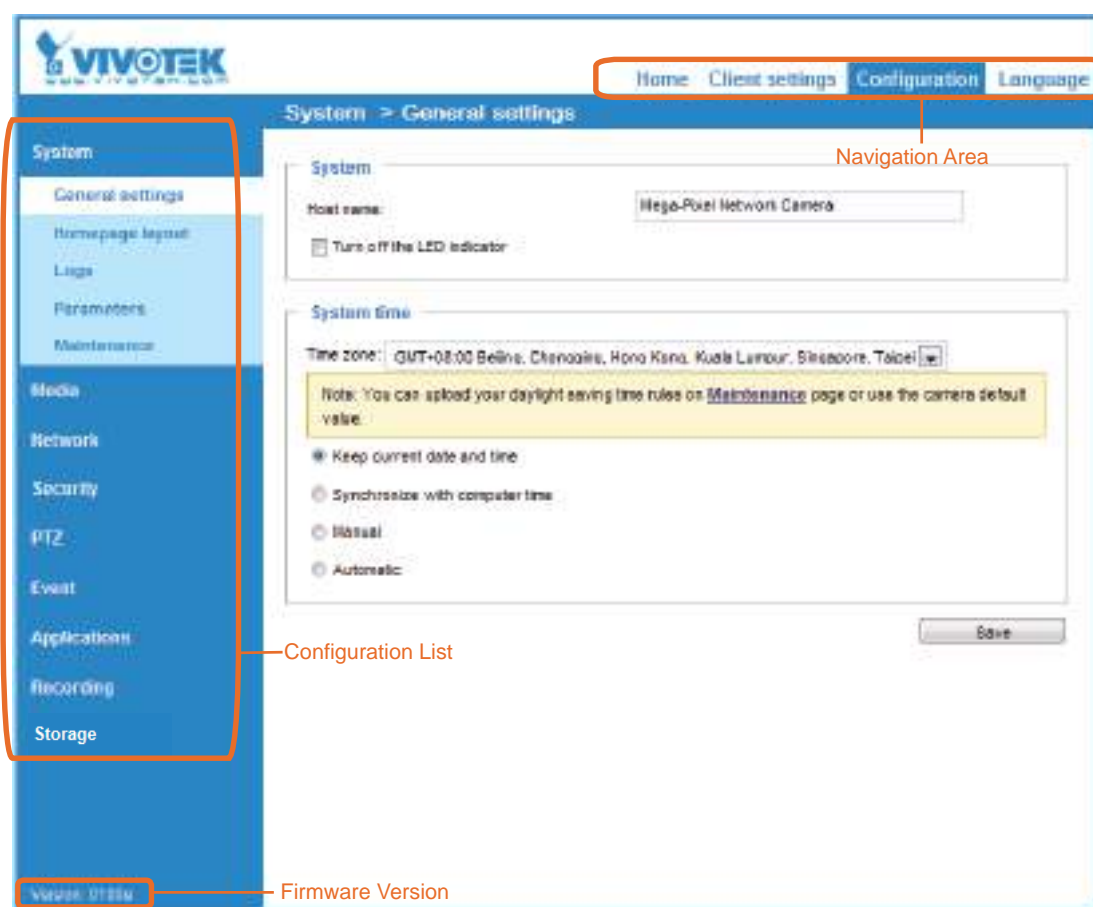


# Configuration

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

VIVOTEK 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; 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 main page:



Each function on the configuration list will be explained in the following sections.

The Navigation Area provides access to all different views from the **Home** page (for live viewing), **Configuration** page, and multi-language selection.

## System > General settings

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

### System

**System**

Host name:

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 ST7501 and VAST management software.

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

## System time

System time

Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

Note: You can upload your daylight saving time rules on [Maintenance](#) page or use the camera default value.

Keep current date and time

Synchronize with computer time

Manual

Automatic

Save

**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.

**Time zone :** Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 55 for details.

## System > Homepage layout

This section explains how to set up your own customized homepage layout.

### General settings

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



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


### Logo graph

Here you can change the logo that is placed at the top of your homepage.

**Logo graph**

A customized logo (Gif, JPG or PNG) can be uploaded for main page. It will be resized to 160x50 pixels to replace the previous logo.

Default
  Custom



Logo link:

Follow the steps below to upload a new logo:

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

### Customized button

If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

**Customized button**

Show manual trigger button



## Theme Options

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

■ Follow the steps below to set up the customized homepage:

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.



4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

## System > Logs

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

### Log server settings

**Log server settings**

Enable remote log

IP address:

port:

Follow the steps below to set up the remote log:

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

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

Date	Time	Priority	Channel	Message
06/12/2010	11:00:00	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:01	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:02	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:03	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:04	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:05	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:06	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:07	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:08	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:09	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:10	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:11	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:12	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:13	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:14	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:15	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:16	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:17	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:18	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:19	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:20	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:21	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:22	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:23	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:24	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:25	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:26	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:27	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:28	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:29	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:30	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:31	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:32	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:33	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:34	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:35	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:36	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:37	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:38	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:39	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:40	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:41	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:42	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:43	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:44	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:45	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:46	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:47	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:48	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:49	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:50	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:51	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:52	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:53	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:54	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:55	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:56	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:57	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:58	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:00:59	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0
06/12/2010	11:01:00	System Info	192.168.4.100	LinkUp! 1.0.0.0.0.0.0

### System log

**System log** | Access log

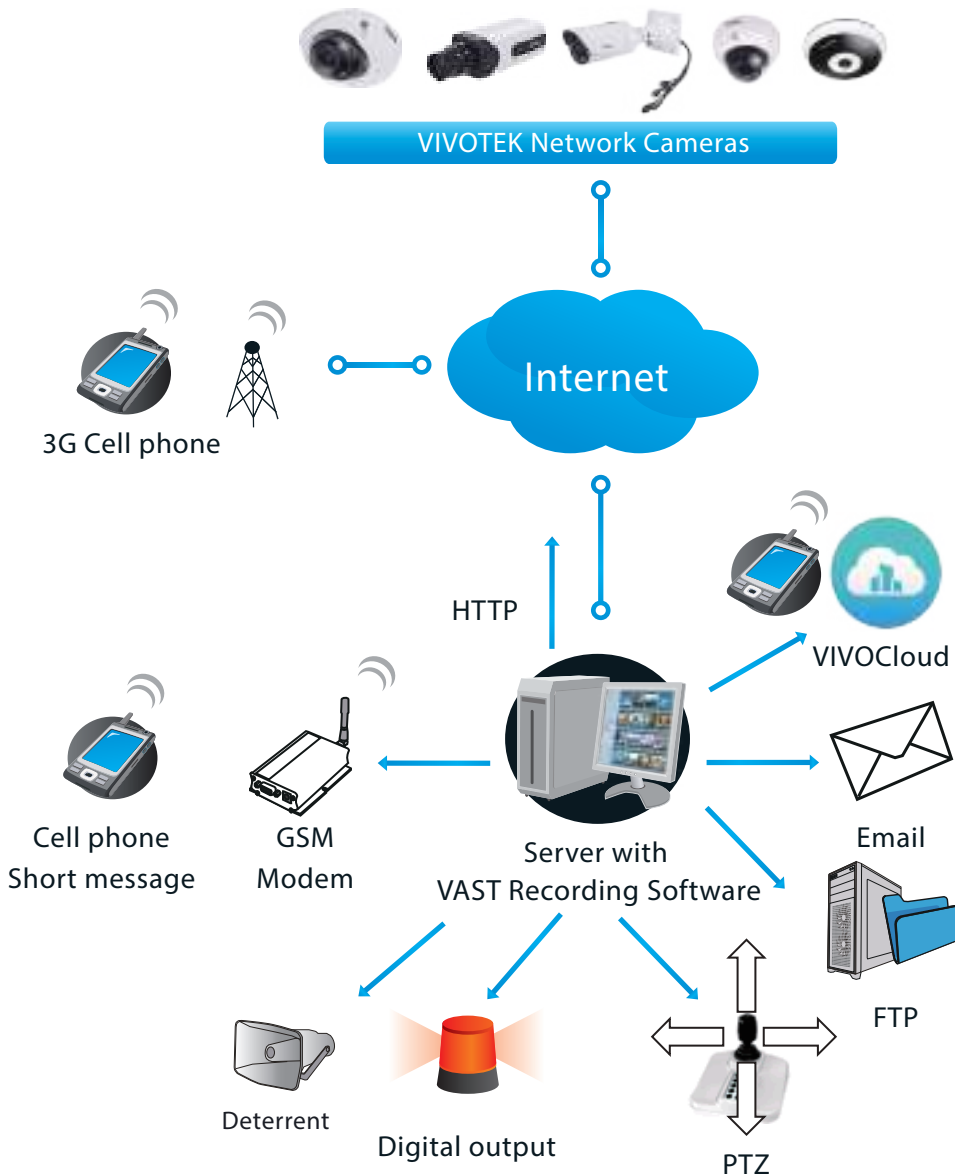
```

Jan 5 11:36:07 syslogd 1.5.0: restart.
Jan 5 11:36:08 [watchdog]: Ready to watch httpd.
Jan 5 11:36:09 [EVENT MGR]: Starting eventmgr with support for EcTun
Jan 5 11:36:11 [DRM Service]: Starting DRM service.
Jan 5 11:36:20 [JFmPigDCP]: Search IGD failed
Jan 5 11:36:23 automount[718]: => mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address.
Jan 5 11:36:23 automount[718]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Jan 5 11:36:23 [IR Cut Control]: Day mode
Jan 5 11:36:23 automount[728]: => mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address.
Jan 5 11:36:23 automount[728]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Jan 5 11:36:23 [IR Cut Control]: Day mode
Jan 5 11:36:23 [SYS]: Serial number = 0002D10ED4C9
Jan 5 11:36:23 [SYS]: System starts at Wed Jan 5 11:36:23 UTC 2011

```

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

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



## Access log

System log

**Access log**

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

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

## VADP log

The VADP log displays information for the pre-loaded VADP module, such as the TrendMicro IoT security package. The information includes, package size, activation time, memory size taken, records of automated updates, etc.

## System > Parameters

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

**Parameters**

```

system_hostname='FD9366-HV'
system_ledoff='0'
system_lowlight='1'
system_date='2020/03/04'
system_time='11:51:55'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160'
system_updateinterval='0'
system_info_modelname='FD9366-HV'
system_info_extendedmodelname='FD9366-HV'
system_info_serialnumber='0002D18C48B5'
system_info_firmwareversion='FD9366-VVTK-0222d'
system_info_language_count='10'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9='Русский'
system_info_language_i10=''
system_info_language_i11=''

```

## System > Maintenance

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

### General settings > Upgrade firmware

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

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

Follow the steps below to upgrade the firmware:

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

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

The following message is displayed when the upgrade has succeeded.

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

### General settings > Reboot

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

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

## General settings > Restore

### Restore

Restore all settings to factory default except settings in

Network  Daylight saving time  Custom language  VADP  Focus position

Restore

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

**Network:** Select this option to retain the Network Type settings (please refer to Network Type on page 82).

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

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

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

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



## Import/Export files

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

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

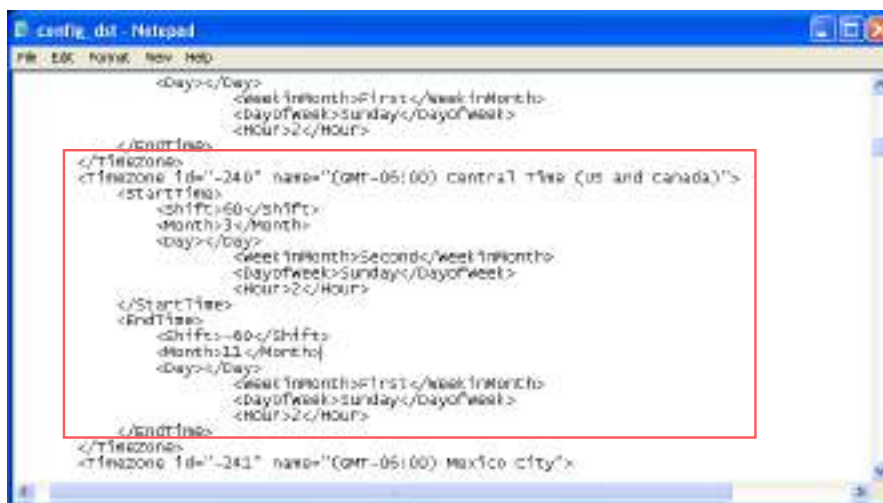
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



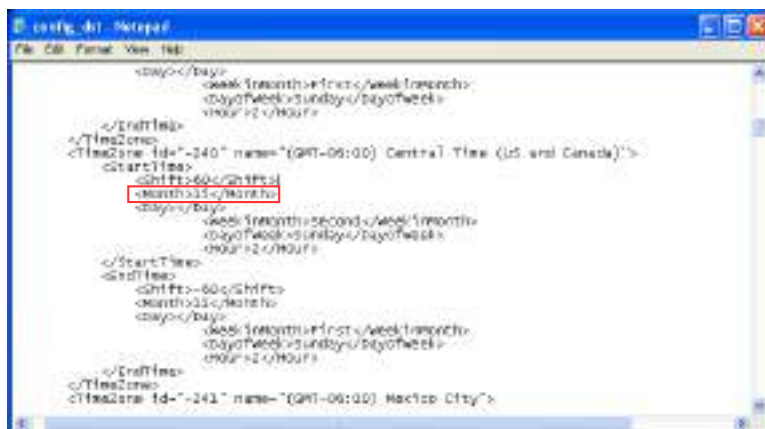
- Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



Update daylight saving time rules: Click **Browse...** and specify the XML file to update.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.





The following message is displayed when attempting to upload an incorrect file format.



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

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

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

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

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

#### **Tips:**

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

Applicable scenario:

- (a) Power disconnected during firmware upgrade.
- (b) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

You can use the following methods to activate the camera with its backup firmware:

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

## Media > Image

This section explains how to configure the image settings of the Network Camera. It is composed of the following columns: General settings, IR control, Image settings, Exposure, Focus, and Privacy mask. The Focus window is available only for models that come with motorized lens.

### General settings

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

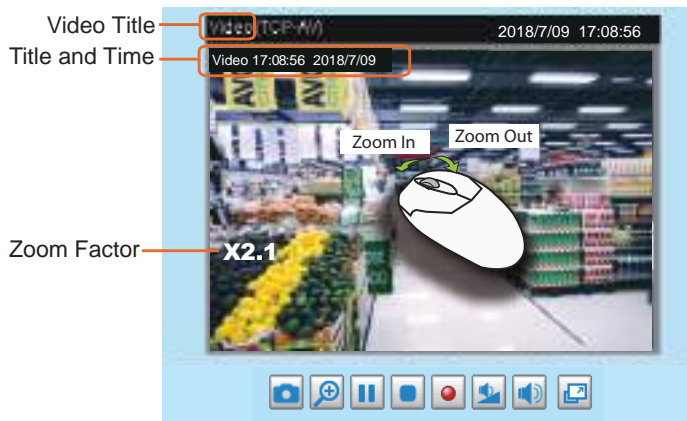
Power line frequency:  50 Hz  60 Hz

Video orientation:  Flip  Mirror

Rotate

#### Video title

Show timestamp and video title in video and snapshots: Enter a name that will be displayed on the title bar of the live video as the picture shown below. A zoom indicator will be displayed on the Home page when you zoom in/out on the live viewing window as shown below. You may zoom in/out on the image by scrolling the mouse wheel inside the live viewing window, and the maximum zoom in will be up to 12 times.



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

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

Video font (.ttf): You can select a True Type font file for the display of textual messages 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. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

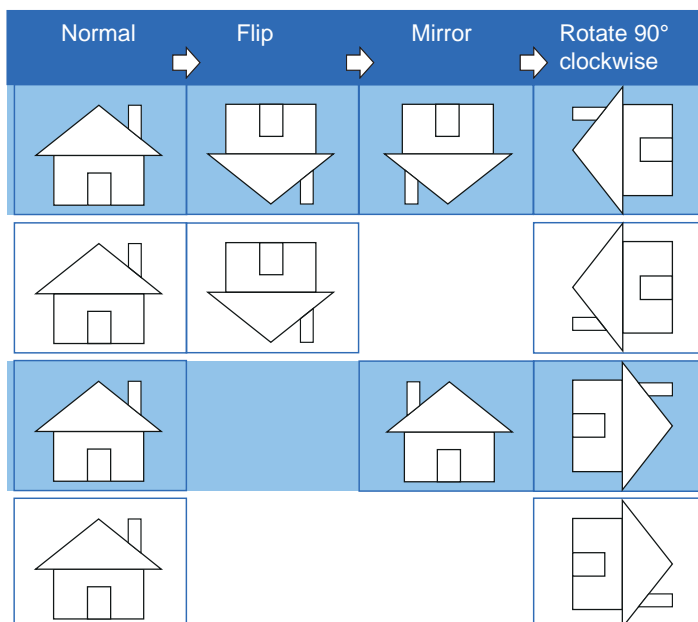
**Video orientation:** Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that if you have preset locations, those locations will be cleared after flip/mirror setting.

**Rotate -**

Rotate  Degrees

The rotation here indicates clockwise rotation. 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.



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.

**Day/Night Settings**

**Day/Night settings**

Switch to B/W in night mode

IR cut filter:

Light sensor sensitivity:

**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.
- **Synchronize with digital input**  
If an external IR device is connected that comes with its own light sensor, you can use a digital input from it to trigger the IR cut filter. Doing so can synchronize the detection of light level between the camera and the external IR device.
- **Schedule mode**  
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

### 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.

## Illuminators

### 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.

### Turn on external IR illuminator in night mode

Select Digital output to enable external IR when the camera enters the night mode.

Anti-overexposure: When enabled, the camera automatically adjusts the IR projection to adjacent objects in order to avoid over-exposure in the night mode.

The Smart IR function is more beneficial when the spot of intrusions or an object of your interest is close to the lens and the IR lights. For example, if an intruder has a chance of getting near the range of 3 meters, Smart IR can effectively reduce the over-exposure. For a surveillance area at a greater distance, e.g., 5 meters or farther away, the Smart IR function may not bring as significant benefits as in close range.

Smart IR disabled; distance: 5M



Smart IR enabled; distance: 5M



Smart IR disabled; distance: 3M



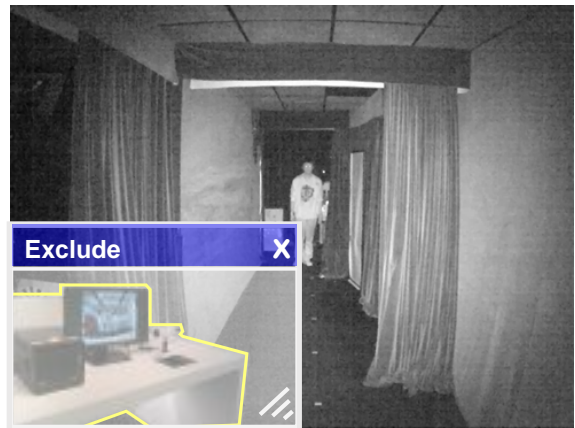
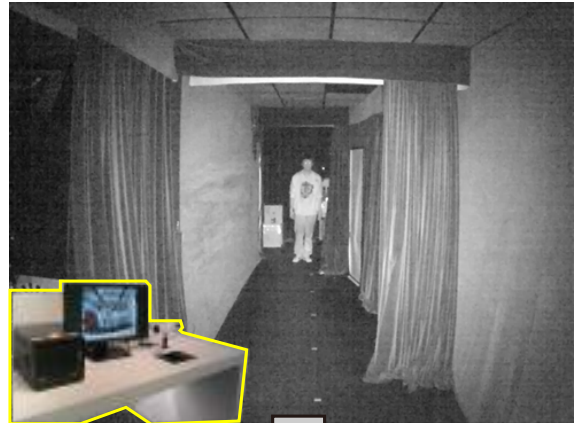
Smart IR enabled; distance: 3M



 **Tips:**

If there is an object in close proximity, the IR lights reflected back from it can mislead the Smart IR's calculation of light level. To solve this problem, you can place an "Exposure Exclude" window on an unavoidable object in the Exposure setting window. See page 66 for how to do it.

You can also configure the "Exposure Exclude" window in a night mode "Profile" setting so that your day time setting is not affected.



Profile of exposure settings

F06853(TCP-A) 2013/08/10 10:46:08



Exclude X

Add include window Add exclude window

Active period

Create and apply the profile to:

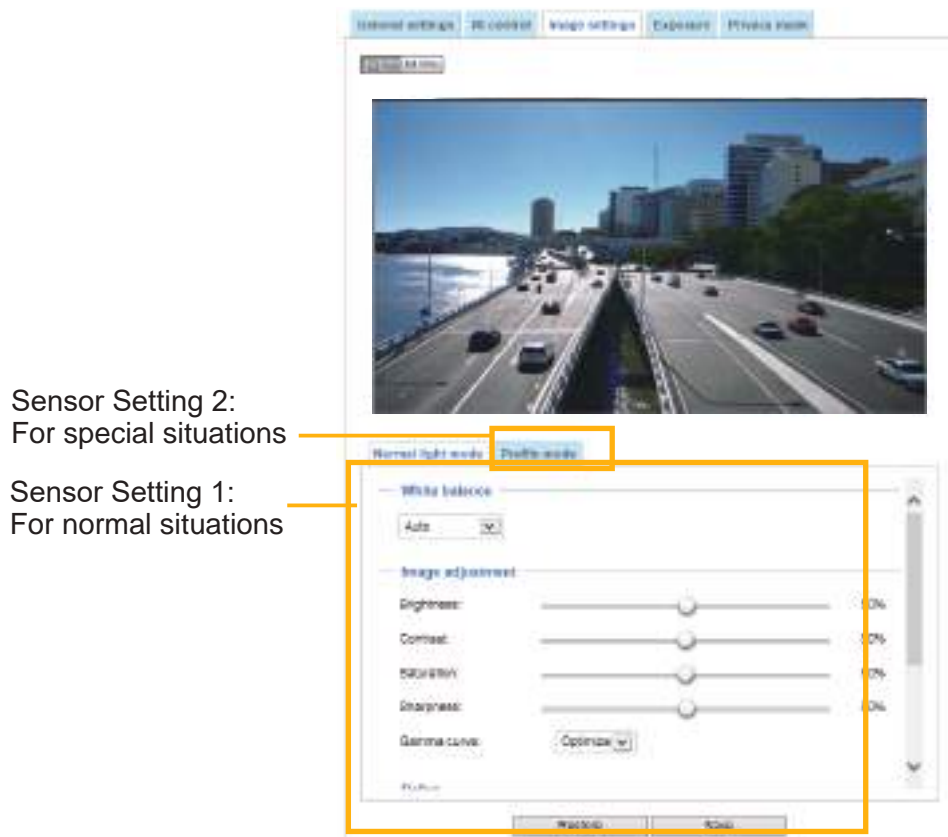
- Day mode
- Night mode
- Schedule mode

Measurement window

- Full view
- Custom
- BLC

## Image settings

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



Sensor Setting 2:  
For special situations

Sensor Setting 1:  
For normal situations

**White balance:** Adjust the value for the best color temperature.

■ You may follow the steps below to adjust the white balance to the best color temperature.

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

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

### Image Adjustment

- **Brightness:** Adjust the image brightness level, which ranges from 0% to 100%.
- **Contrast:** Adjust the image contrast level, which ranges from 0% to 100%.
- **Saturation:** Adjust the image saturation level, which ranges from 0% to 100%.
- **Sharpness:** Adjust the image sharpness level, which ranges from 0% to 100%.
- **Gamma curve:** Adjust the image sharpness level, which ranges from 0.45 to 1, from Detailed to Contrast. You may let firmware **Optimize** your display or select the **Manual** mode, and pull the slide bar pointer to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

This option is disabled when the WDR feature is enabled.

**Defog:** Defog helps improve the visibility quality of captured image in poor weather conditions such as smog, fog, or smoke.

### Noise reduction

- **Enable 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 slide bar to adjust the reduction strength. Note that 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 after-images may occur. You may then select a lower strength level or disable the function.

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

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



## Exposure

On this page, you can set the Exposure measurement window, Exposure level, Exposure mode, Exposure time, Gain control, and Day/Night mode settings. You can configure two sets of Exposure settings: one for normal situations, the other for special situations, such as the day/night/schedule mode.

Sensor Setting 2:  
For special situations

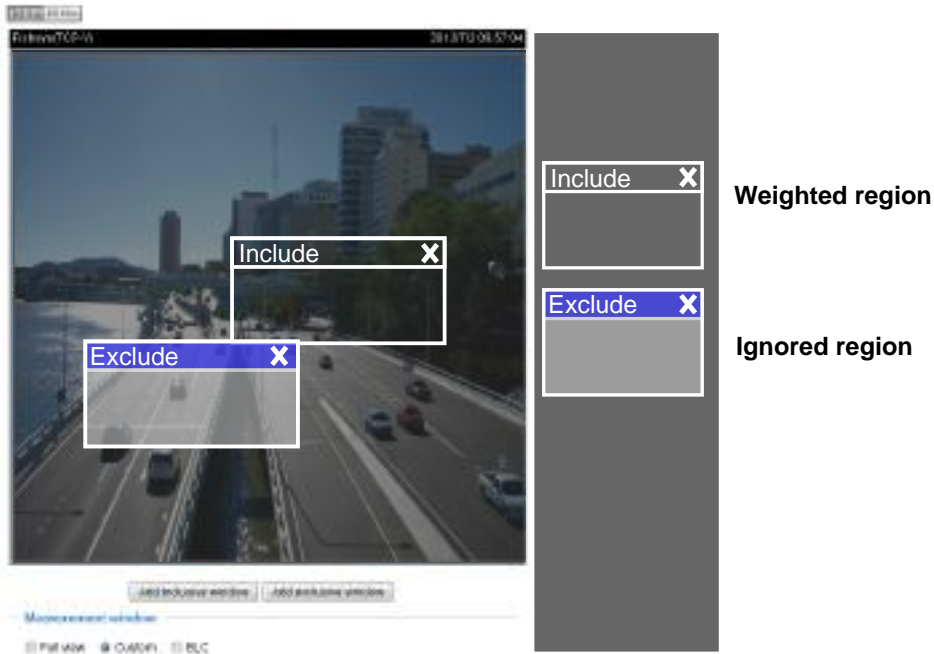
Sensor Setting 1:  
For normal situations

### Exposure strategy:

**Measurement window:** 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. You may want to exclude the bright sunlight shining through a building's corridor.

- **Full view:** Calculate the full range of view and offer appropriate light compensation.
- **Custom:** This option allows you to manually add customized windows as inclusive or exclusive regions. A total of 10 windows can be configured. Please refer to the next page for detailed illustration.
- **Auto:** Firmware automatically determines an optimal exposure level.

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



- **Center:** Use the center portion of the screen to determine the exposure level.
- **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 on affected spots to enhance the overall image quality. For example, the HLC helps reduce the glares produced by spotlights or headlights.

### Exposure control:

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

■ **Exposure mode:**

You can click and drag the semi-circular pointers on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automatically tune to an optimal imaging result. You can also configure the iris size to control the amount of light. For example, you may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

■ **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, and the range of Exposure time (the shutter time) will be limited to a range in order to match the AC power frequency. When selected, the exposure time will be forced to stay longer than 1/120 second. For cameras that come with fixed iris lens, setting the exposure time to longer than 1/120 second may introduce too much light to the lens. Users can use this option to observe whether the result of long exposure time is satisfactory.

■ **AE Speed Adjustment:**

This function applies when you need to monitor fast changing lighting conditions. For example, the camera may need to monitor 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. The same applies if the camera is installed on a vehicle, and when it needs to adapt to fast changes of light when entering and leaving a tunnel.

■ **WDR Pro:**

This refers to the Wide Dynamic Range function that enables the camera to capture details in a high contrast environment. Use the checkbox to enable the function, and use the slide bar to select the strength of the WDR Pro functionality, depending on the lighting condition at the installation site. You can select a higher effect when the contrast is high (between the shaded area and the light behind the objects).

Enable WDR enhanced: This function allows users to identify more image details with an extreme contrast from an object of interest with one shadowed side against a bright background, e.g., an entrance. You may select the **Enable WDR enhanced** checkbox, and then adjust the strength (low, medium, high) to reach the best image quality.

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

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

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

Please follow the steps below to set up a profile:

1. Select the **Profile mode** tab.
2. Select the applicable mode: Night mode or Schedule mode. Please manually enter a range of time if you choose the Schedule mode.
3. Configure Exposure control settings in the following columns. Please refer to previous discussions for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.



## Privacy mask

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



- To configure privacy mask windows,
  1. Click **New** to add a new window.
  2. 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.
  3. Enter a Window Name and click **Save** to enable the setting.
  4. Click on the **Enable privacy mask** checkbox to enable this function.



### NOTE:

- ▶ *Up to 5 privacy mask windows can be configured on the same screen.*
- ▶ *If you want to delete the privacy mask window, please click the 'x' mark on the side of window name.*

## Media > Video

### Stream settings

Stream

- ❖ Video settings for stream 1 [Viewing Window](#)
- ❖ Video settings for stream 2 [Viewing Window](#)
- ❖ Video settings for stream 3

This Network Camera supports multiple streams with frame sizes ranging from 480 x 272 to 1920 x 1080 pixels

The definition of multiple streams:

- 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 360.
- 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** and the **Output Frame Size** for a video stream. For example, 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. As the picture shown below, the area of your interest in a parking lot should be the vehicles. The blue sky is of little value for the surveillance purpose.





Please follow the steps below to set up those settings for a stream:

1. Select a stream for which you want to set up the viewing region.
2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Global View window on the home page, will resize accordingly. If you want to set up a customized viewing region, 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 list according to the size of your monitoring device.

**NOTE:**

► All the items in the “Region of Interest” should not be larger than the “Output Frame Size” (current maximum resolution).

■ The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	1920 x 1080 ~ 480 x 272 (Selectable)	1920 x 1080 ~ 480 x 272 (Selectable)
Stream 2	1920 x 1080 ~ 480 x 272 (Selectable)	1920 x 1080 ~ 480 x 272 (Selectable)
Stream 3	Fixed	Fixed

When completed with the settings in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected **Output Frame Size** will immediately be applied to the **Frame size** of each video stream. Then you can go back to the home page to test the e-PTZ function. For more information about the e-PTZ function, please refer to page 115.

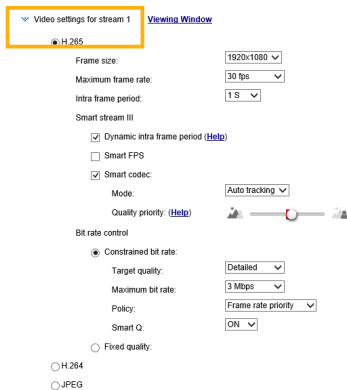


Output Frame Size  
(Size of the Live View Window)

Click the stream item to display the detailed information. The maximum frame size will follow your settings in the above Viewing Window sections.



This Network Camera provides real-time H.265, H.264 and MJPEG compression standards (Triple Codec) 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 through which you can adjust the video performance:



■ **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.

■ **Maximum frame rate**

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

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



The frame rate will decrease if you select a higher resolution.

■ Intra frame period

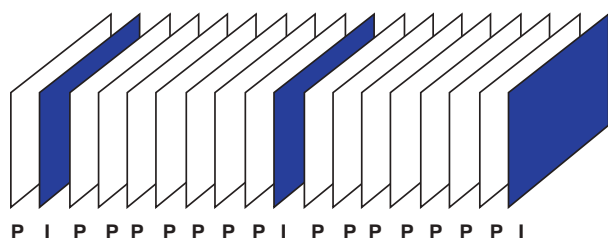
Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds,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

■ Smart stream III

■ Dynamic Intra frame period

High quality motion codecs, such as H.265, utilize the redundancies between video frames to deliver video streams at a balance of quality and bit rate.

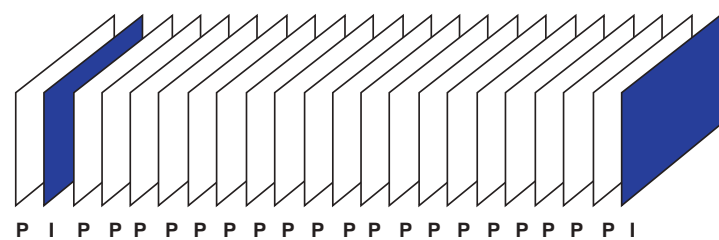
The encoding parameters are summarized and illustrated below. The **I-frames** are completely self-referential and they are largest in size. The **P-frames** are predicted frames. The encoder refers to the previous I- or P-frames for redundant image information.



H.264/265 Frame Types

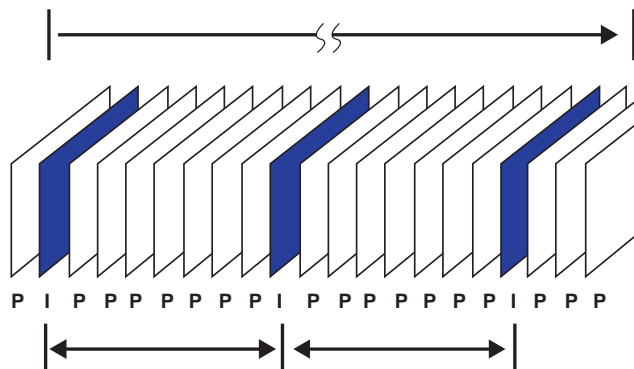
By dynamically prolonging the intervals for I-frames insertion to up to 10 seconds, the bit rates required for streaming a video can be tremendously reduced. When streaming a video of a static scene, the Dynamic Intra frame feature can save up to 53% of bandwidth. The amount of bandwidth thus saved is also determined by the activities in the field of view. If activities occur in the scene, firmware automatically shortens the I-frame insertion intervals in order to maintain image quality. In the low light or night conditions, the sizes of P-frames tend to be enlarged due to the noises, and hence the bandwidth saving effect is also reduced.

Streaming a typical 2MP scene normally requires 3~4Mb/s of bandwidth. With the Dynamic Intra frame function, the bandwidth for streaming a medium-traffic scene can be reduced to 2~3Mb/s, and during the no-traffic period of time, down to 500kb/s.



Dynamic Intra Frame w/ static scenes

Static scene



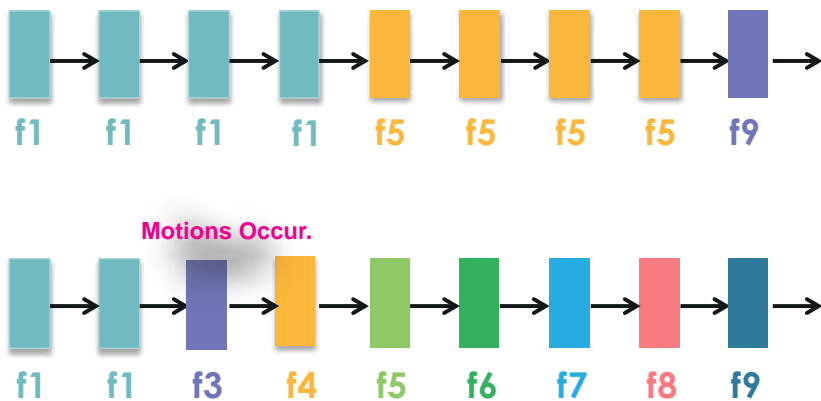
Dynamic Intra Frame w/ activities in scenes

Activities

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

■ Smart FPS

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



By queuing the old frames from a static scene, both the computing efforts and the size of P frames are reduced. It is beneficial for keeping up with the frame rate requirements.

A default frame difference threshold, 1%, is embedded in firmware for returning from Smart FPS to normal encoding when motions occur.

 **NOTE:**

Comparing with Smart Stream II, Smart Stream III has two more configurable options: [Smart Q](#), and [Smart FPS](#).

- **Smart codec:** Smart codec effectively reduces the quality of the whole or the non-interested areas on a screen 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 Smart codec is preferred.

- **Auto tracking:** The Auto mode configures the whole screen into the non-interested area. 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 (no pixel changes) will still be transmitted in low-quality format.
- **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 as the non-interested areas. The details in the ROI areas will be transmitted in a higher-quality video format.

As illustrated below, the upper screen may contain little details of your interest, while the sidewalk on the lower screen is included in an ROI window.



As the result, the lower screen is constantly displayed in high details, while the upper half is transmitted using a lower-quality format. Although the upper half is transmitted using a lower quality format, you still have an awareness of what is happening on the whole screen.



- **Hybrid:** The major difference between the “Manual” mode and the “Hybrid” mode is that:

In the “**Hybrid**” mode, any objects entering the non-interested area will restore the video quality of the moving objects and the area around them. The video quality of the associated non-interested area is immediately restored to normal to cover the moving objects.

In the “**Manual**” mode, the non-interested area is always transmitted using a low-quality format regardless of the activities occurring inside.

Quality priority: ([Help](#))



- **Quality priority:** Use the slide bar to tune the quality contrast between the ROI and non-interested areas.

The farther the slide bar button is to the right, the higher the image quality of the ROI areas. On the contrary, the farther the slide bar button to the left, the higher the image quality of the non-interested area.

In this way, you may set up an ROI window as a privacy mask by covering a protected area using an ROI window, while the rest of the screen becomes the non-interested area. You may then configure the non-interested area to have a high image quality, or vice versa.

You should also select the Maximum bit rate from the pull-down menu as the threshold to contain the bandwidth consumption for both the high- and low-quality video sections in a smart stream.

## ■ Bit rate control

Constrained bit rate:

A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8Mbps, 10Mbps, 12Mbps, 14Mbps, ~ to 80Mbps. You can also select **Customize** and manually enter a value up to 40Mbps.

- - **Target quality:** Select a desired quality ranging from Medium to Excellent.
- **Maximum bit rate:** select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 80Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.
- **Policy:** If Frame Rate Priority is selected, the Network Camera will try to maintain the frame rate per second performance, while the image quality will be compromised. If Image quality priority is selected, the Network Camera may drop some video frames in order to maintain image quality.

**Smart Q:** Select ON or OFF to enable or disable the feature. Smart Q is scene-aware. The Smart Q reduces frame size and bit rate consumption through the following:

- Dynamically adjusting the image quality for scenes in different luminosities in low light frames. Less noises means less of the bandwidth consumed.
- Endorsing different qualities for the I frames and P frames, and hence reduces 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 actually poses little effects on human eyes.

Unnecessary quality is unrecognized by human eyes and wastes the bit rate.

The Smart Q streaming can save up to 50% to 80% of bandwidth in different illumination conditions while keeping the same imaging quality. These numbers come from the comparison between Smart Stream II and Smart Stream III streamings.

**Fixed quality:**

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

**Maximum bit rate:** With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 80Mbps.

The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

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

If the **JPEG** mode is selected, the Network Camera sends consecutive JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:

JPEG

Frame size: 1920x1080 ▾

Maximum frame rate: 10 fps ▾

Bit rate control

Constrained bit rate:

Fixed quality:

Quality: Good ▾

Maximum bit rate: 80 Mbps ▾

#### ■ Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

#### ■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

If the power line frequency is set to 50Hz (at the 5MP resolution), the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, and 20fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, and 20fps. 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, refer to the previous page for details.



#### NOTE:

- ▶ *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*
- ▶ *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurrence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

## Media > Audio

### Audio Settings

Audio settings

Mute

Microphone source: Internal ▾

Internal microphone input gain: 70%

External microphone input gain: 70%

Audio type

G.711: pcmu ▾

G.726 bit rate: 32 Kbps ▾

Save

**Mute:** Select this option to disable audio transmission from the Network Camera to all clients. Note that if muted, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



**Internal microphone input:** Select the gain of the external audio input according to ambient conditions. Adjust the gain from 0% to 100%.

**External microphone input:** 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 ( $\mu$ -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.

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



## Network > General settings

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

### Network Type

### LAN

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

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

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

1. You can make use of VIVOTEK's Shepherd utility to easily set up the Network Camera on LAN. Please refer to Software Installation on page 16 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

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

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

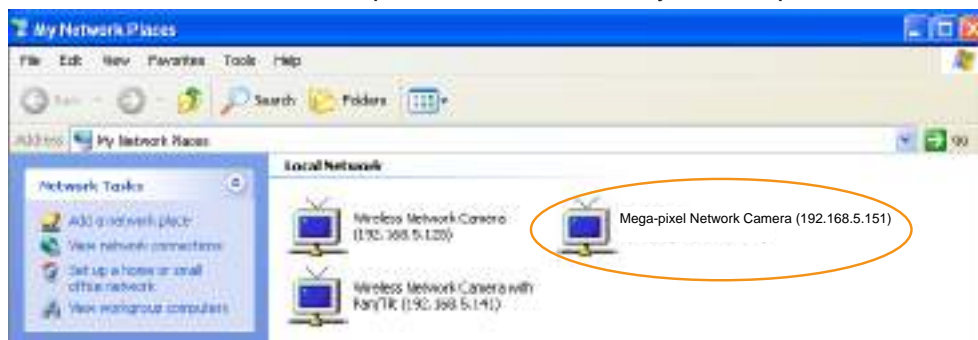
**Primary DNS:** The primary domain name server that translates hostnames into IP addresses.

**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 UPnP™ 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, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ 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 UPnP™ and it is activated.

### PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 123) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 128).

Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.

4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

 A screenshot of the 'Network type' configuration window. The window has a title bar 'Network type'. There are three radio button options: 'LAN', 'PPPoE', and 'Ethernet'. The 'PPPoE' option is selected. Below these options are three text input fields labeled 'User name:', 'Password:', and 'Confirm password:'. At the bottom left, there is a checkbox labeled 'Enable IPv6'. At the bottom right, there is a 'Save' button.

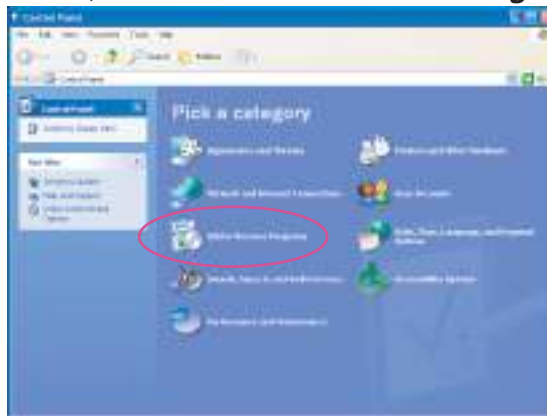
5. The Network Camera will reboot.

6. Disconnect the power to the Network Camera; remove it from the LAN environment.

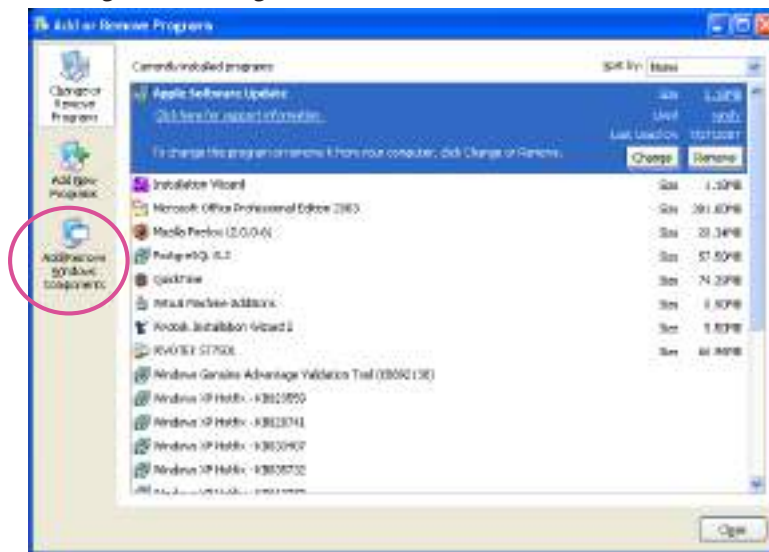
**NOTE:**

- ▶ If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.
- ▶ If UPnP™ is not supported by your router, you will see the following message:  
**Error: Router does not support UPnP port forwarding.**
- ▶ Steps to enable the UPnP™ user interface on your computer:  
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

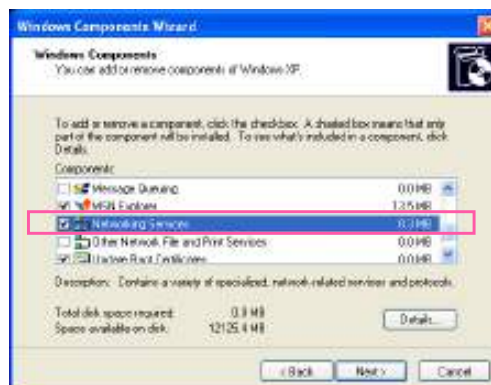
1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.



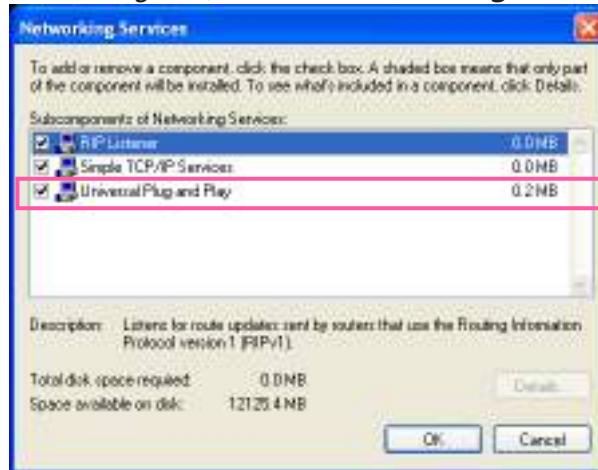
2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.



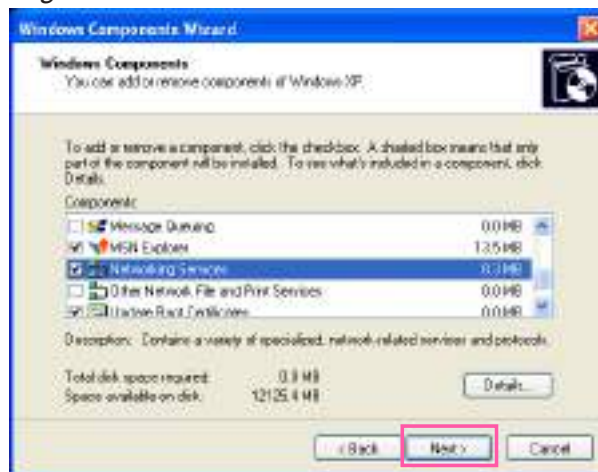
3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.



4. In the Networking Services dialog box, select **Universal Plug and Play** and click **OK**.



5. Click **Next** in the following window.



6. Click **Finish**. UPnP™ is enabled.

- ▶ **How does UPnP™ work?**  
 UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.
- ▶ **Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.**

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

- ▶ **If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 55 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.**

### Enable IPv6

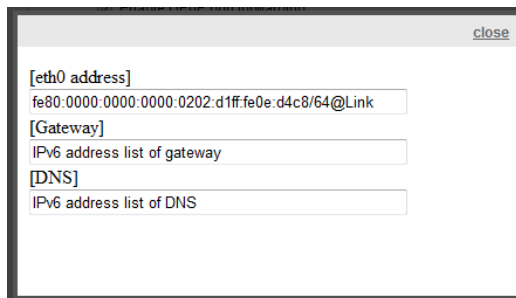
Select this option and click **Save** to enable IPv6 settings.

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



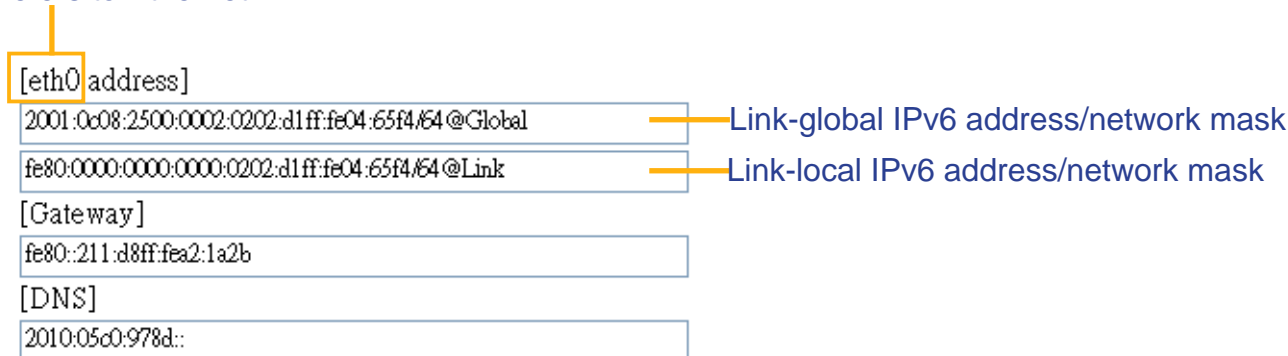
When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.



If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

### Refers to Ethernet

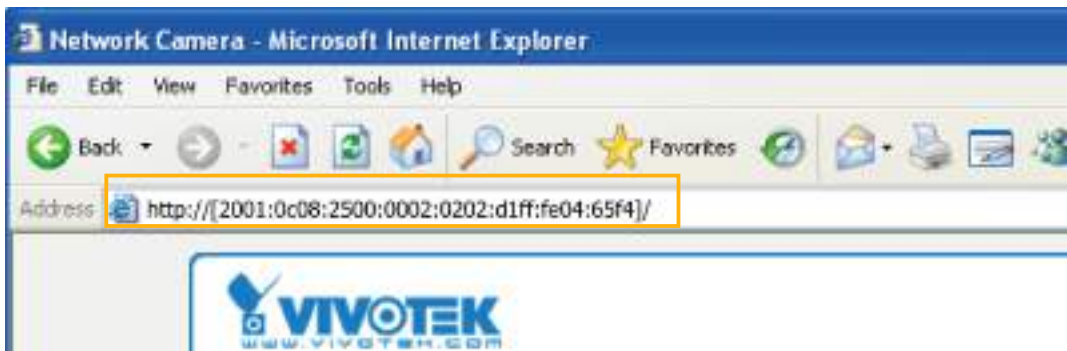


Please follow the steps below to link to an IPv6 address:

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



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

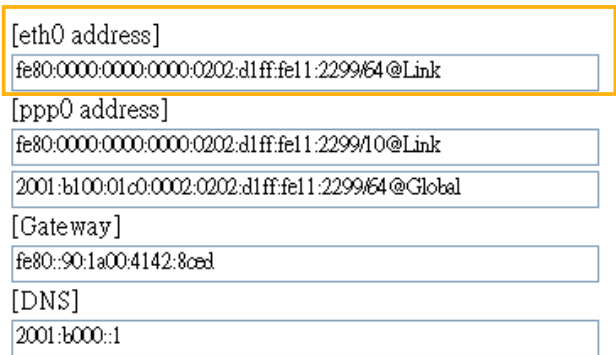


**NOTE:**

- ▶ If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage using the following address format: (Please refer to **HTTP** streaming on page 88 for detailed information.)



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



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

Enable IPv6**IPv6 information** Manually setup the IP addressOptional IP address / Prefix length  / Optional default router Optional primary DNS

## Network > Streaming protocols

### HTTP streaming

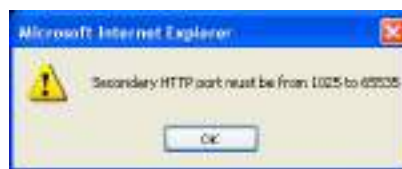
To utilize HTTP authentication, make sure that you have set a password for the Network Camera first; please refer to Security > User account on page 100 for details.

HTTP	RTSP
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, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

On the LAN

http://192.168.4.160 or  
http://192.168.4.160:8080

Access name for stream 1 ~ 3: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 70.

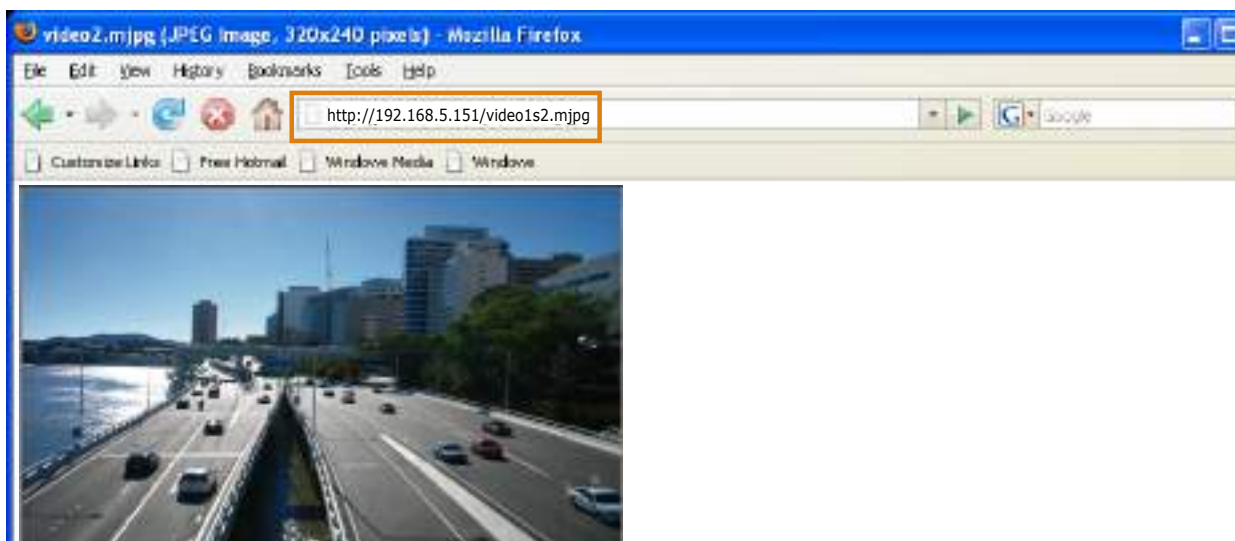
When using **Mozilla Firefox** to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox.



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 or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



#### NOTE:

- ▶ *Microsoft® Internet Explorer does not support server push technology; therefore, you will not be able to access a video stream using <http://<ip address>:<http port>/<access name for stream 1, 2, 3>>.*

## RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 100 for details.

HTTP
RTSP

Authentication:	<input type="text" value="digest"/>
RTSP port:	<input type="text" value="554"/>
RTP port for video:	<input type="text" value="5556"/>
RTCP port for video:	<input type="text" value="5557"/>
RTP port for metadata:	<input type="text" value="6556"/>
RTCP port for metadata:	<input type="text" value="6557"/>
RTP port for audio:	<input type="text" value="5558"/>
RTCP port for audio:	<input type="text" value="5559"/>
Access name for stream 1:	<input type="text" value="live1s1.sdp"/>
Access name for stream 2:	<input type="text" value="live1s2.sdp"/>
Access name for stream 3:	<input type="text" value="live1s3.sdp"/>
<ul style="list-style-type: none"> <li>✦ Multicast settings for stream 1</li> <li>✦ Multicast settings for stream 2</li> <li>✦ Multicast settings for stream 3</li> </ul>	

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

	QuickTime player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

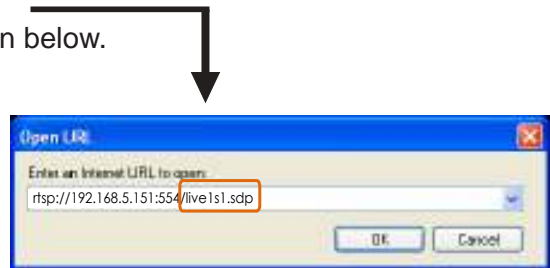
**Access name for stream 1 ~ 3:** This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an **RTSP player** to access the Network Camera, you have to set the video mode to **H.264 or H.265** and use the following RTSP URL command to request transmission of the streaming data.

`rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 3>`

For example, when the access name for **stream 1** is set to **live1s1.sdp**:

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.

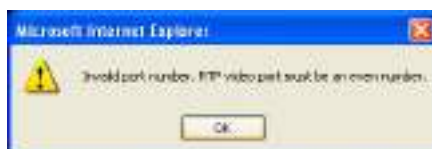


**RTSP port /RTP port for video, audio/ RTCP port for video, audio**

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557.

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

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



**Multicast settings for streams:** Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for video streams.

Multicast settings for stream 1

Always multicast

Multicast group address:

Multicast video port:

Multicast RTCP video port:

Multicast metadata port:

Multicast RTCP metadata port:

Multicast audio port:

Multicast RTCP audio port:

Multicast TTL [1~255]:

Multicast settings for stream 2

Always multicast

Multicast group address:

Multicast video port:

Multicast RTCP video port:

Multicast metadata port:

Multicast RTCP metadata port:

Multicast audio port:

Multicast RTCP audio port:

Multicast TTL [1~255]:

Multicast settings for stream 3

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

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

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



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

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



### IMPORTANT:

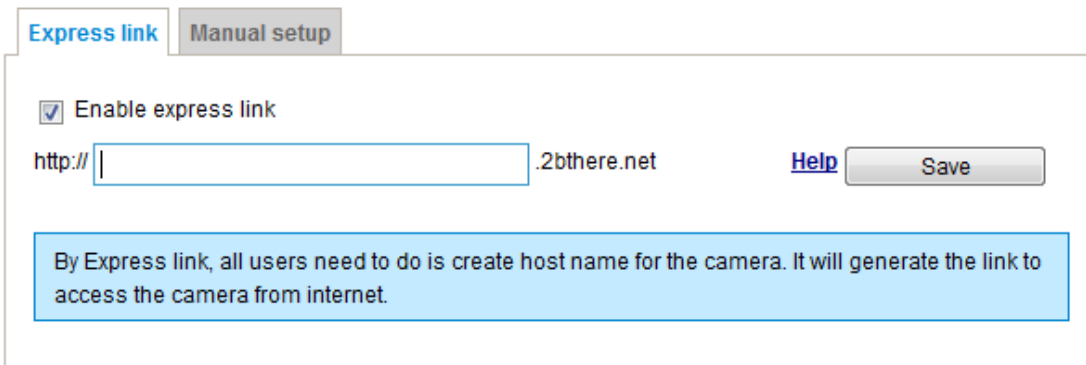
The Multicast metadata port is utilized by VIVOTEK VADP modules to transfer video analytics results, PTZ stream, textual data, and event messages between the camera and the client side running and observing the video analysis. If your client side computer is located outside the local network, you may need to open the associated TCP port on routers and firewall.

## Network > DDNS

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

### Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.



Please follow the steps below to enable Express Link:

1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will display a message as shown below.



## Manual setup

### DDNS: Dynamic domain name service

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

**Provider:** Select a DDNS provider from the provider drop-down list.

VIVOTEK offers [Safe100.net](#), a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register [Safe100.net](#) to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.

Note that before utilizing this function, please apply for a dynamic domain account first.

#### ■ [Safe100.net](#)

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

copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings'."/>

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

The image shows two parts of a web interface for configuring Dynamic Domain Name Service (DDNS).

The top section is titled "DDNS: Dynamic domain name service". It has a checkbox labeled "Enable DDNS" which is checked. Below it are fields for "Provider" (a dropdown menu showing "Safe100.net"), "Host name" (a text box containing "WTK.safe100.net"), "Email" (a text box containing "wtk@vivotek.com"), and "Key" (a text box with four asterisks). A "Save" button is located to the right of these fields.

The bottom section is titled "Register". It has fields for "Host name" (containing "WTK.safe100.net"), "Email" (containing "wtk@vivotek.com"), "Key" (with four asterisks), and "Confirm key" (with four asterisks). There is a "Forget key" button next to the Key field. Below these fields is a "Register" button. Underneath is a "DDNS Registration Result" section with a message: "[Register] Successfully Your account information has been mailed to registered e-mail address". At the bottom of this section, there is a link for "copy" and a note: "Upon successful registration, you can click [copy](#) to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click 'Save' to save new settings."

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

#### ■ CustomSafe100

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

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

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

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

- [Dyndns.org\(Dynamic\) / Dyndns.org\(Custom\)](http://www.dyndns.com/): visit <http://www.dyndns.com/>

## Network > QoS (Quality of Service)

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

The following are the main benefits of a QoS-aware network:

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

### Requirements for QoS

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

- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

### QoS models

#### CoS (the VLAN 802.1p model)

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

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

**CoS**

Enable CoS

VLAN ID:	<input type="text" value="1"/>
Live video:	<input type="text" value="0"/> ▼
Live audio:	<input type="text" value="0"/> ▼
Event/Alarm:	<input type="text" value="0"/> ▼
Management:	<input type="text" value="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 may fail if the CoS setting is incorrect.
- ▶ 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.
- ▶ Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.

### QoS/DSCP (the DiffServ model)

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

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

**QoS/DSCP**

Enable QoS/DSCP

Live video:

Live audio:

Event/Alarm:

Management:

Note that different vendors of network devices might have different methodologies and unique implementations. Shown below is a sample corresponding information from a Cisco switch. You should enter a DSCP tag value according to the information provided by the network devices.

Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue	Ingress DSCP	Output Queue
DGE	1	16(CS2)	2	32(CS4)	3	48(CS6)	3
1	1	17	3	33	5	49	3
2	1	18(AF21)	2	34(AF41)	3	50	3
3	1	19	2	35	3	51	3
4	1	20(AF22)	2	36(AF42)	3	52	3
5	1	21	2	37	3	53	3
6	1	22(AF23)	2	38(AF43)	3	54	3
7	1	23	2	39	3	55	3
8(CS1)	1	24(CS3)	3	40(CS5)	4	56(CS7)	3
9	1	25	3	41	4	57	3
10(AF11)	1	26(AF31)	3	42	4	58	3
11	1	27	3	43	4	59	3
12(AF12)	1	28(AF32)	3	44	4	60	3
13	1	29	3	45	4	61	3
14(AF13)	1	30(AF33)	3	46(EF)	4	62	3
15	1	31	3	47	4	63	3

Queue 1 has the lowest priority, queue 4 has the highest priority.

**QoS/DSCP**

Enable QoS/DSCP

Live video:

Live audio:

Event/Alarm:

Management:

### QoS Baseline/Technical Marketing Classification and Marking Recommendations

Application	Layer3 Classification			Layer 2 CoS/MPLS EXP	
	IPP	PHB	DSCP		
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	



## Network > SNMP (Simple Network Management Protocol)

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

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

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

### SNMP Configuration

#### Enable SNMPv1, SNMPv2c

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

Enable SNMPv1, SNMPv2c

**SNMPv1, SNMPv2c Settings**

Read/Write community:

Read only community:

#### Enable SNMPv3

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

- Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.
- Authentication type: Select MD5 or SHA as the authentication method.
- Authentication password: Enter the password for authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).

Enable SNMPv3

**SNMPv3 Settings**

Read/Write Security name:

Authentication Type:

Authentication Password:

Encryption Password:

Read only Security name:

Authentication Type:

Authentication Password:

Encryption Password:

## Network > FTP

The newer firmware disabled the FTP port for security concerns. You can manually enable the FTP server service to enable the FTP function. You can disable the FTP server function when it is not in use.

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



### Tips:

You can FTP the camera's IP address to download videos recorded in the SD card, or use the "<http://ip/cgi-bin/admin/lscrtl.cgi?cmd=search>" command to examine the recorded files on your SD card.

---

## Bonjour

To access the camera from a Mac computer, go to Safari, click on Bonjour and select the camera from a drop-down list.

You can go to Safari > Preferences to enter your user name and password, and provide the root password the first time you access the camera. The camera main page will open in your browser.



Some later iOSes may come without the Bonjour option. Install the Discovery utility instead.

Find the Discovery (formerly Bonjour Browser) from the Mac App Store.

Discovery is a utility that displays all the Bonjour services on your local network or on Wide-Area Bonjour domains. The utility is previously called Bonjour Browser, it is now distributed on the Mac App Store.

Discovery requires macOS 10.12 or higher. For older versions of Mac OS you can download the old version of Bonjour Browser.

Bonjour Browser (obsolete)

<http://www.tildesoft.com/files/BonjourBrowser.dmg> - Version 1.5.6

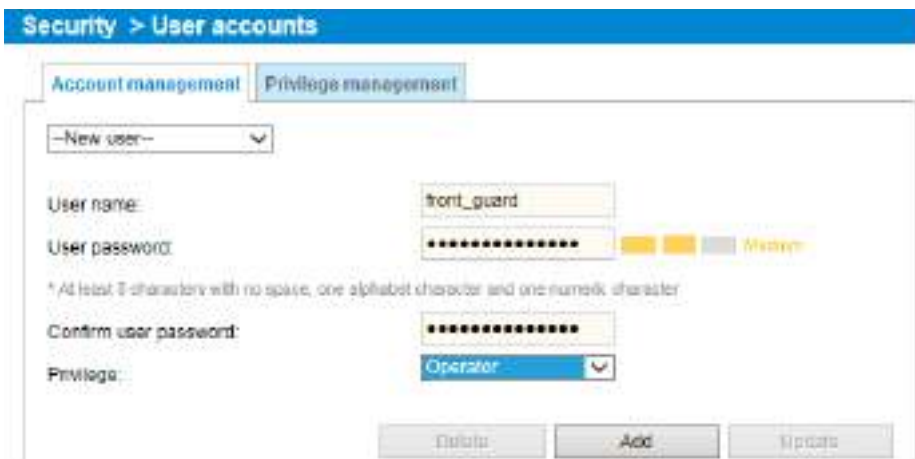
Discovery for iOS

<https://itunes.apple.com/us/app/discovery-dns-sd-browser/id305441017?mt=8>

## Security > User accounts

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

### Account management



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, please 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 unfold the pull-down menu. Select **New user**.
2. Enter the new user’s name and password. Type the password identically in both text boxes.  
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. Click **Add** to enable the setting. The privilege levels are listed below:

Administrator	Full control
Operator	Control DO, white-light illuminator, snapshot, and PTZ; unable to enter the camera Configuration page.
Viewer	Control DO, white-light illuminator, view, listen, PTZ, and talk through the camera interface.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Although operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 154. Viewers can only access the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

## Privilege management

Account management	Privilege management
<input type="checkbox"/> Allow anonymous viewing	
Operator:	<input checked="" type="checkbox"/> Digital output <input checked="" type="checkbox"/> PTZ control
Viewer:	<input type="checkbox"/> Digital output <input checked="" type="checkbox"/> PTZ control
<input type="button" value="Save"/>	

Digital Output & PTZ control: You can modify the management privilege as operators or viewers. Select or de-select the checkboxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page.

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

## Security > HTTPS (Hypertext Transfer Protocol over SSL)

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

### Create and Install Certificate Method

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

#### Create self-signed certificate

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

The screenshot shows the 'HTTPS' configuration page. The 'Enable HTTPS secure connection' checkbox is checked. Under 'Mode', 'HTTP & HTTPS' is selected. Under 'Certificate', the 'method' dropdown is set to 'Create self-signed certificate'. The 'Certificate information' section contains the following fields: Status (Not installed), method (Create self-signed certificate), Country (TW), State or province (Asia), Locality (Asia), Organization (VIVOTEK, Inc.), Organization unit (VIVOTEK, Inc.), Common name (www.vivotek.com), and Validity (3650 days). A 'Create certificate' button is located at the bottom right of the form. A blue dialog box with the text 'Please wait while the certificate is being generated...' is overlaid on the form.

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

The screenshot shows the 'Certificate information' dialog box. The 'Status' is 'Active'. The 'method' is 'Create self-signed certificate'. The 'Country' is 'TW', 'State or province' is 'Asia', and 'Locality' is 'Asia'. The 'Organization' is 'VIVOTEK, Inc.', 'Organization unit' is 'VIVOTEK, Inc.', and 'Common name' is 'www.vivotek.com'. At the bottom, there are two buttons: 'Certificate properties' and 'Remove certificate'. The 'Certificate properties' button is highlighted with a yellow box.

5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from “<http://>” to “<https://>” in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

**https://**

