



LINEAR™



Fixed Lens
Bullet Camera

Motorized Varifocal
Lens Bullet Camera

Fixed Lens &
Motorized Varifocal
Lens Dome Camera

Fixed Lens
Turret Camera

IV200

Smart Surveillance Cameras | 2MP SERIES

User Manual

Table of Contents

Overview.....	3
Revision History.....	4
Read Before Use.....	4
Package Contents.....	5
Symbols and Statements in this Document.....	5
The Cameras.....	6
Fixed Lens Bullet Camera.....	6
Motorized Varifocal Lens.....	7
Fixed / Motorized Dome Camera.....	8
Turret Dome Fixed Lens Camera.....	9
Hardware Installation.....	11
Network Deployment.....	14
General Connection (PoE).....	14
Network > IP.....	15
Network Type.....	15
Network > Streaming protocols.....	19
Network > QoS (Quality of Service).....	23
Network > SNMP (Simple Network Management Protocol).....	24
Network > FTP.....	25
Accessing the Network Camera.....	26
Using Web Browsers.....	26
Using RTSP Players.....	29
Using 3GPP-compatible Mobile Devices.....	30
Main Page.....	31
LINEAR Logo.....	31
Host Name.....	31
Camera Control Area.....	31
Configuration Area.....	32
Hide Button.....	32
Settings.....	35
System > General settings.....	36
System > Home page layout.....	37
System > Logs.....	39
System > Parameters.....	40
System > Maintenance.....	41
Camera > Image.....	44
Camera > Video.....	53
Security > Users.....	62
Security > HTTPS (Hypertext Transfer Protocol over SSL).....	63
Security > Access List.....	66
Security > IEEE 802.1X.....	68
Events > Event settings.....	70
Events > General.....	83
Events > Motion Detector.....	85
Events > Camera Tamper Detector.....	85
Events > Intrusion Detector.....	86
Recording > Recording settings.....	87
Local storage > SD card management.....	91
Storage > Content management.....	93
Electromagnetic Compatibility (EMC).....	95

Overview

The IV200 family of 2MP indoor/outdoor cameras incorporate our intelligent video analytics and are capable of 1920 x 1080 at 30 fps. With the most updated LINEAR[®] 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 cameras support 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 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 home pages 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. The camera should be installed at least 4 inches away from the building's eave.
3. Maintenance and repair work must always be carried out by qualified technical personnel.
4. Disconnect power from the unit when performing a maintenance task.






Package Contents

- IV200 Camera
- Screw pack.
- Alignment sticker.
- Quick Installation Guide.
- 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.

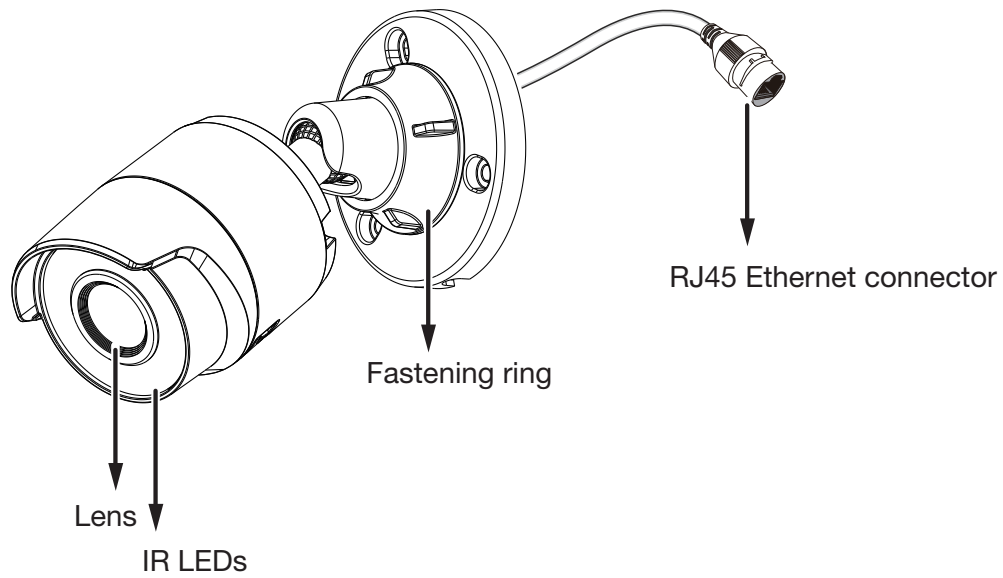
IMPORTANT:

1. The camera is only to be connected to PoE networks.
2. For PoE connection, use only UL listed I.T.E. with PoE output.

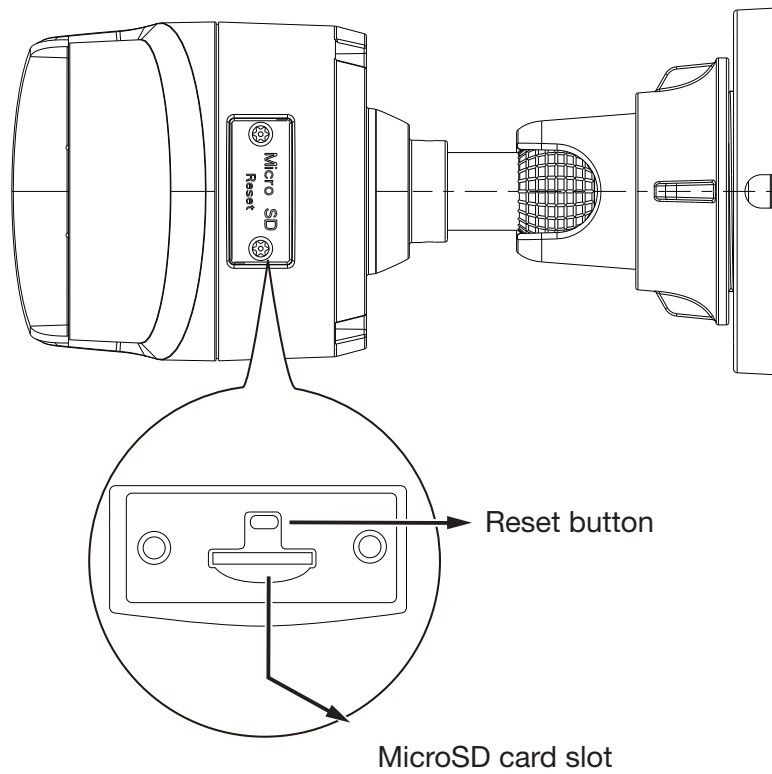
The Cameras

Fixed Lens Bullet Camera

Outer View

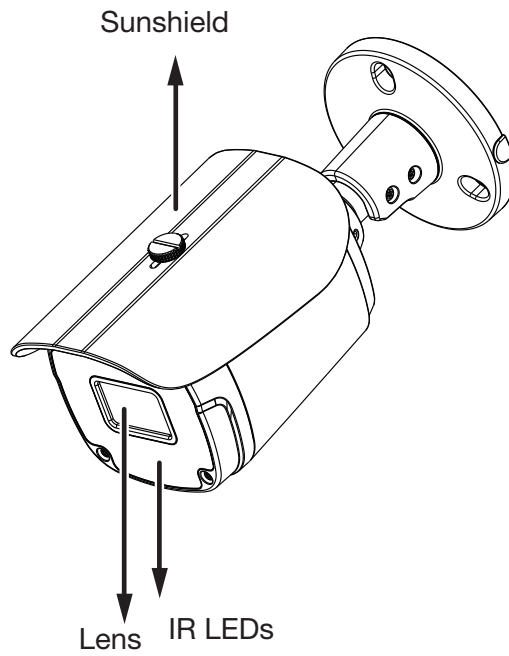


Inner View

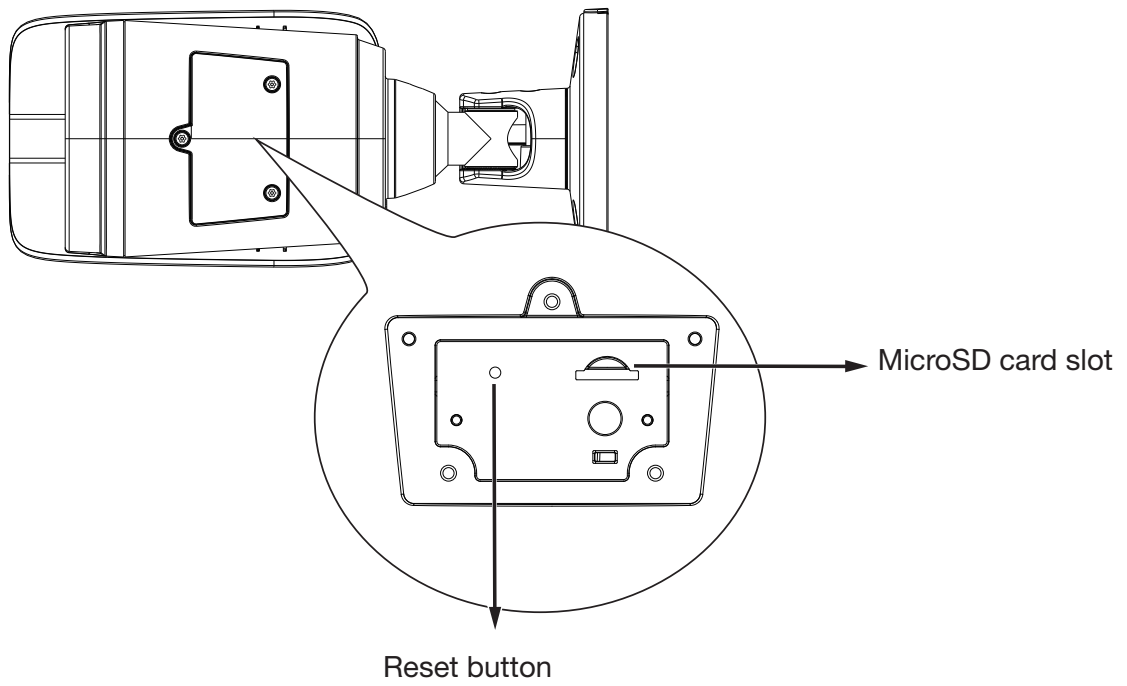


Motorized Varifocal Lens

Outer View

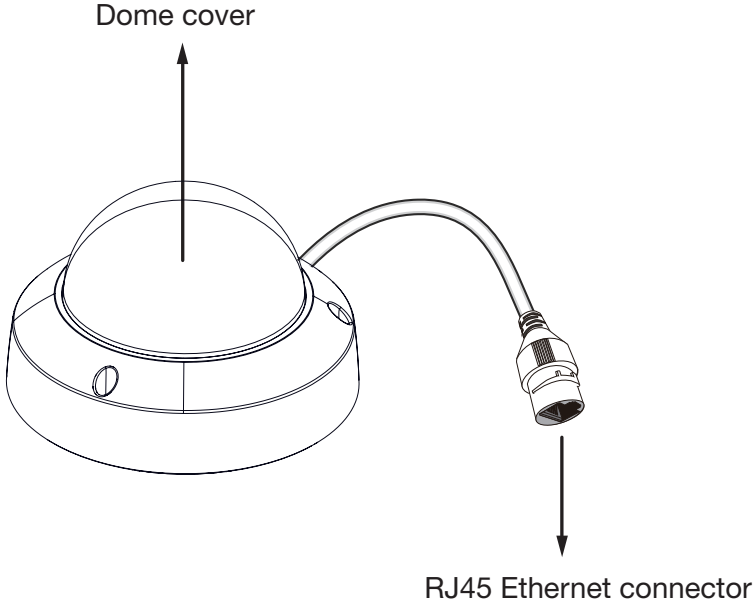


Inner View

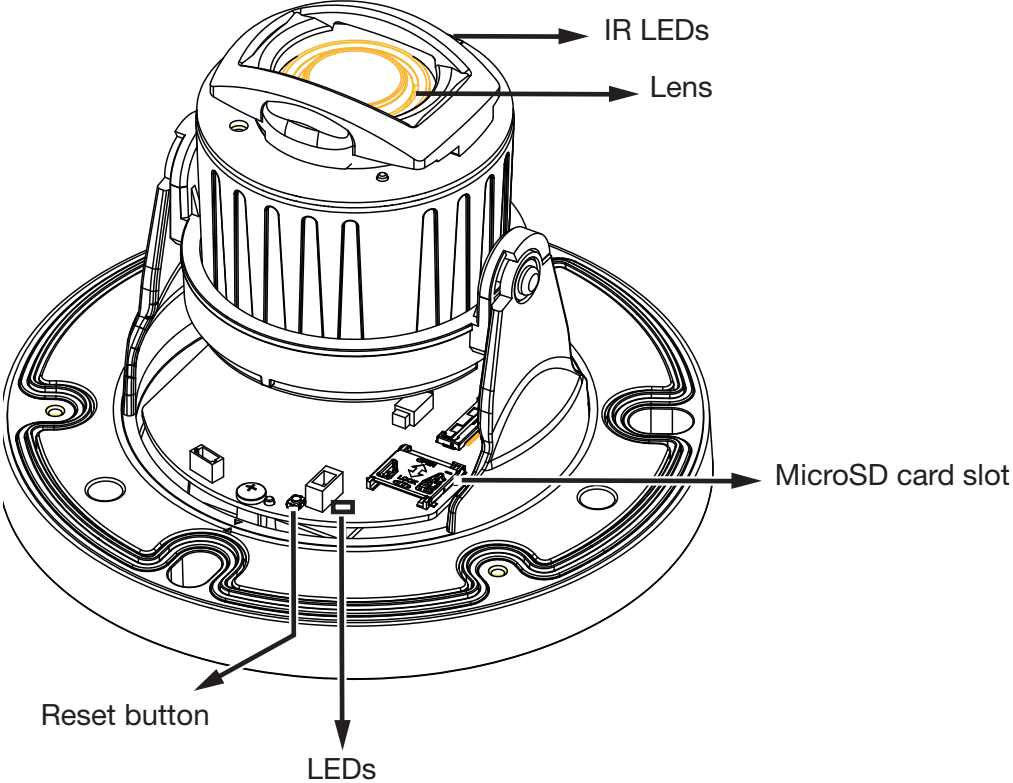


Fixed / Motorized Dome Camera

Outer View

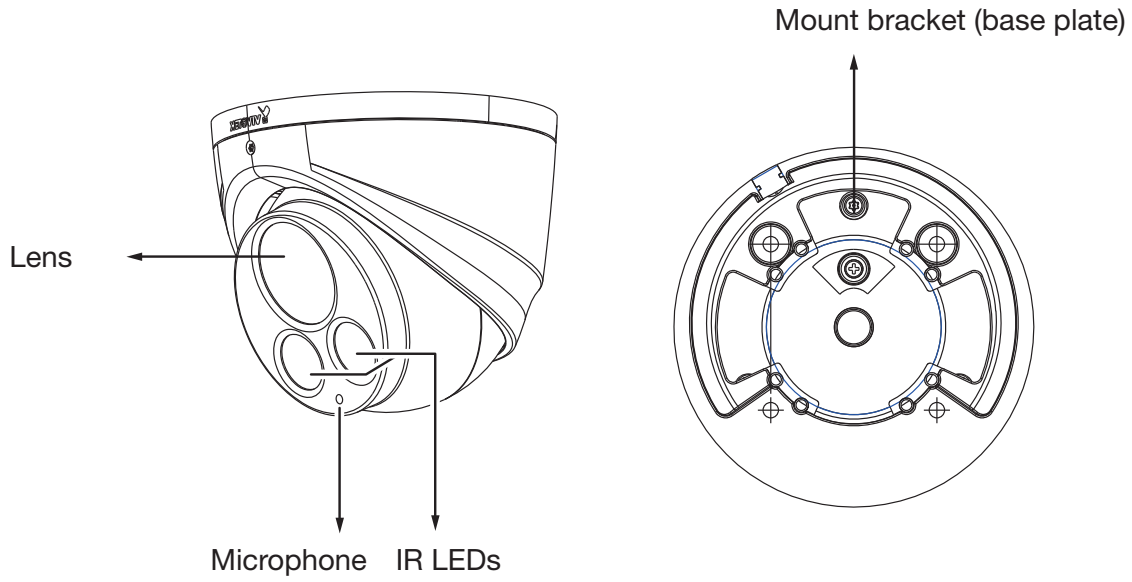


Inner View

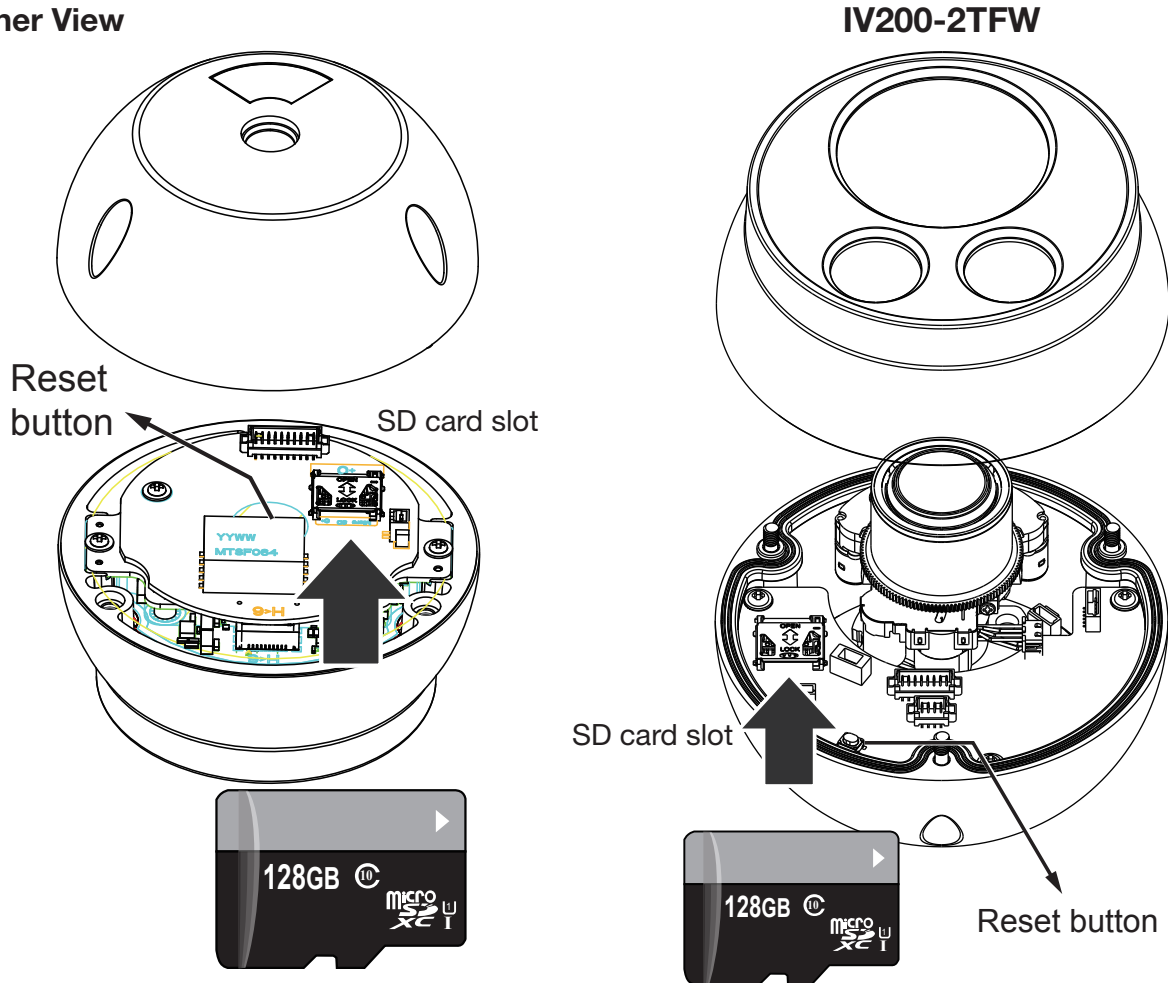


Turret Dome Fixed Lens Camera

Outer View



Inner View

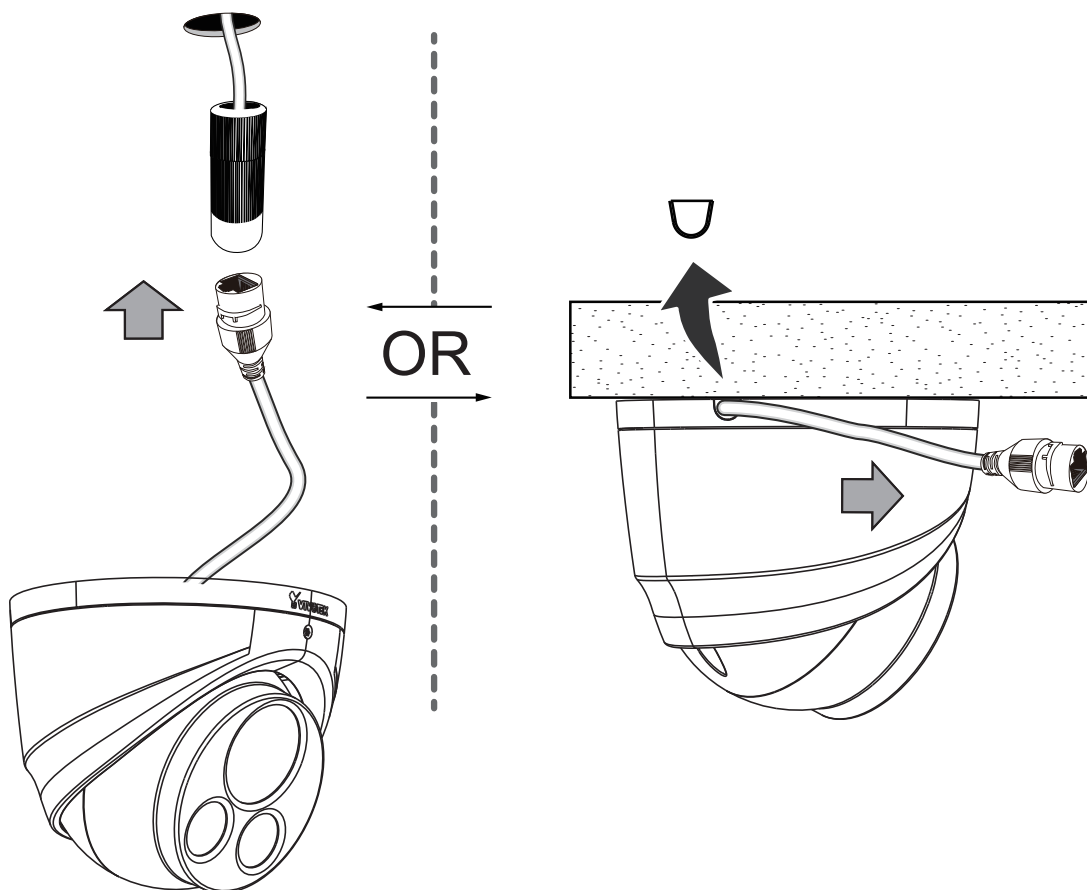


⚠ IMPORTANT:

Many copper coated aluminum (CCA) and other non-standard conductors cabling products are masqueraded as CAT5E or CAT6 cables. Avoid using these CCA products especially when connecting PoE cameras. It is a must to use Ethernet cables compliant with the 3P/ETL standard.



The camera's cable can be routed through a drilled hole or through the opening on the side of camera. Observe and look for the best installation position.



⚠ IMPORTANT:

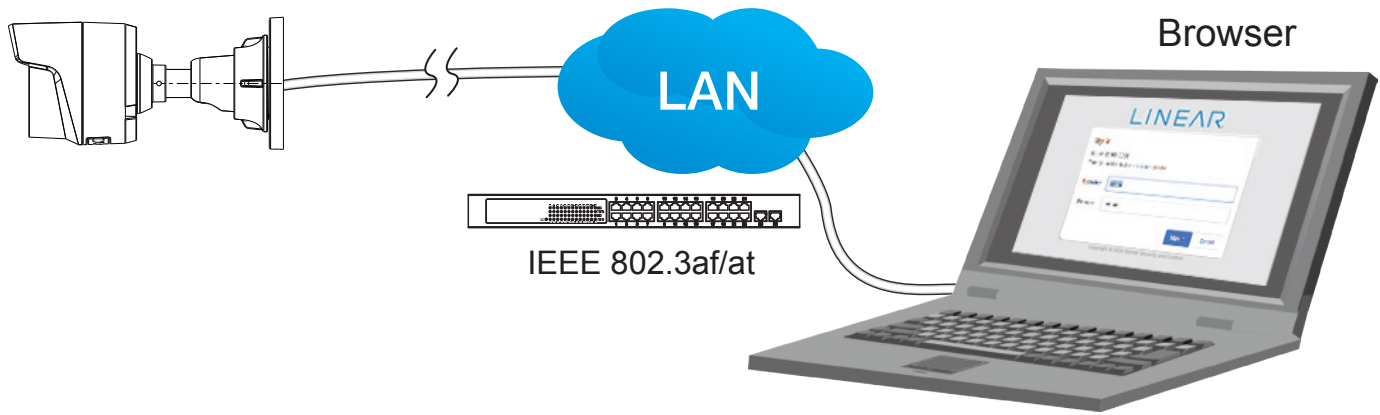
Power Consumption & Power Input

IR ON: 6W

IR Off: 3.3W

Hardware Installation

For hardware installation instructions, refer to the *Quick Start Guide* for your particular camera.



1. The camera requires IEEE 802.3af/at PoE power to function properly. Use Only UL listed I.T.E active PoE Switch or Mid-Span.
2. When connected to a Linear Network Video Recorder (NVR) directly or over the network, the NVR will automatically find the camera regardless of IP network settings.

For direct camera login and management, open a browser to the default IP Address:
192.168.0.230 - username = **admin**, password = **linear**

Only one camera should be configured at a time to avoid default IP Address conflicts.

Forceful Password Configuration

1. The first time you log in to the camera, the firmware will prompt for a password configuration for security concerns.
2. Enter “admin” as the user name. The default password is “linear”.

Sign in

http://192.168.0.230

Your connection to this site is not private

Username

Password

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

LINEAR

Language

IV200-2TFW

Configure password

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

User name : (null)

User password : ■■■ Strong

Confirm user password :

*For security purpose, it is strongly recommended to reset password for Operator and Viewer

Save Cancel

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

192.168.0.230 says

Password successfully reset!

OK

- 4. Another prompt will request for the password you just configured. Enter the password, and then begin to configure your camera for live view.

Sign in

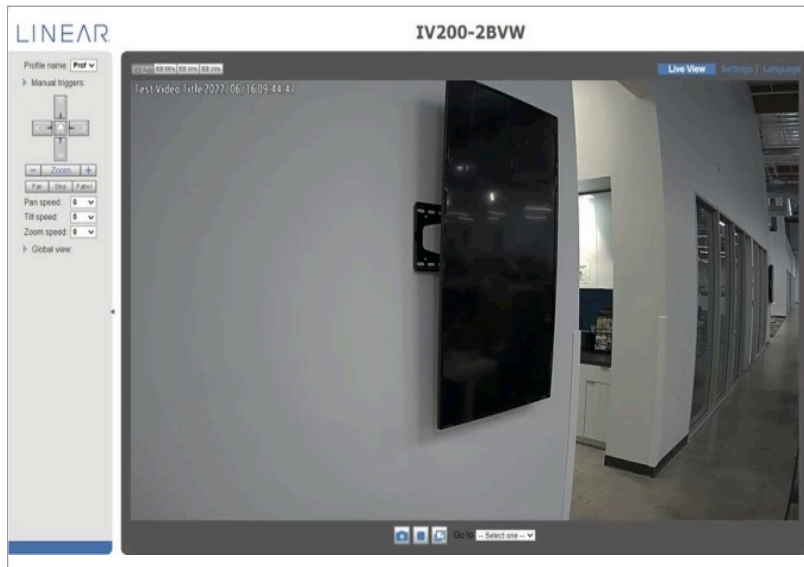
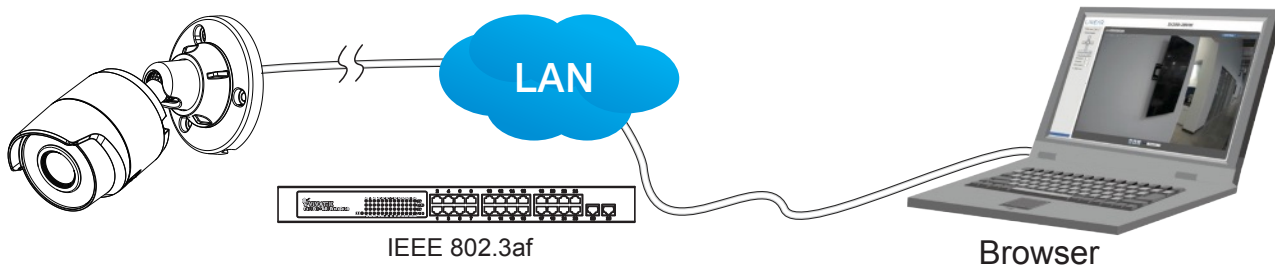
http://192.168.0.230

Your connection to this site is not private

Username

Password

Sign in Cancel



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. Following a successful restore, the status LED will blink green and red during normal operation.

MicroSD/SDHC/SDXC Card Capacity

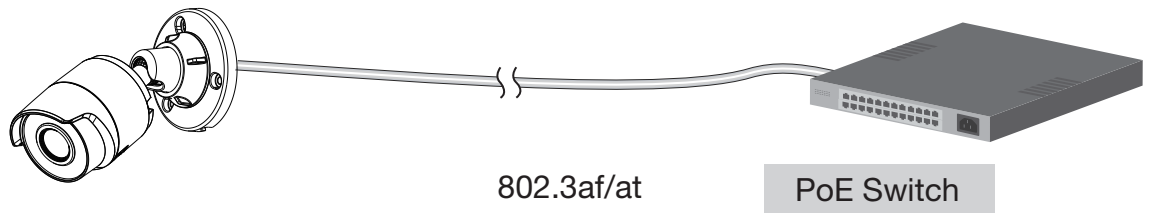
This network camera is compliant with **MicroSD/SDHC/SDXC** up to 128GB and other preceding standard SD cards.

Network Deployment

General Connection (PoE)

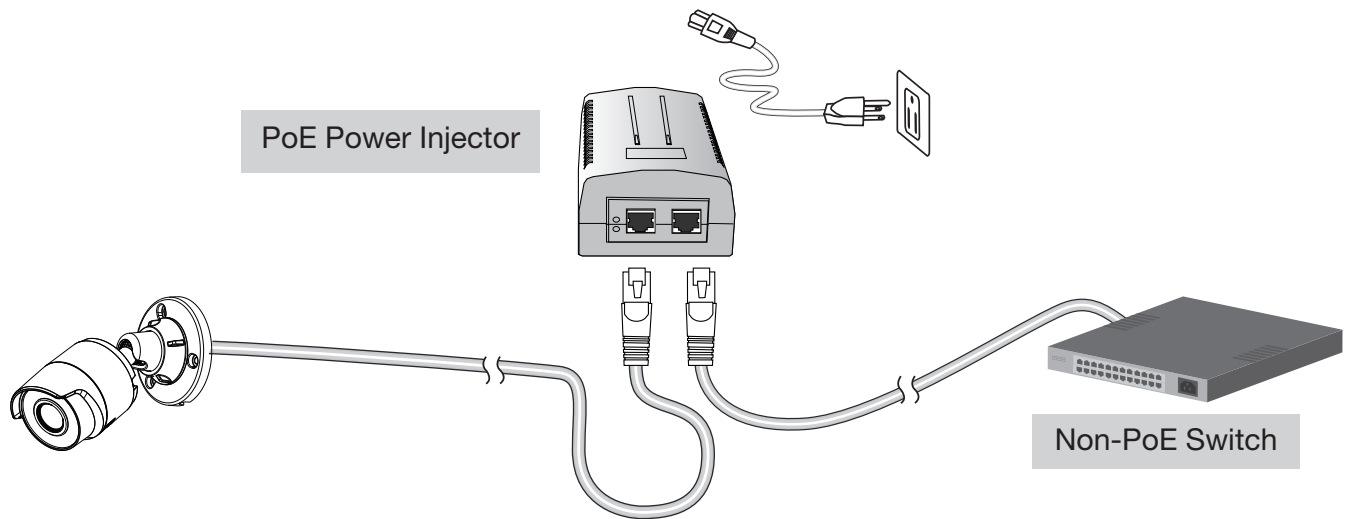
● When using a PoE-enabled switch

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 an Ethernet cable.



● When using a non-PoE switch

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



NOTE:

1. For PoE connection, use only UL listed I.T.E. with PoE output.

Network > IP

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

Network Type

Network type

LAN

- Get IP address automatically
- Use fixed IP address
- Enable UPnP presentation
- Enable UPnP port forwarding

PPPoE

Enable IPv6

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. 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.
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.

Network type

LAN

- Get IP address automatically
- Use fixed IP address

IP address:

Subnet mask:

Default router:

Primary DNS:

Secondary DNS:

Primary WINS server:

Secondary WINS server:

- Enable UPnP presentation
- Enable UPnP port forwarding

PPPoE

Enable IPv6

Primary DNS	The primary domain name server that translates host names into IP addresses.
Secondary DNS	Secondary domain name server that backups the Primary DNS.
Primary WINS server	The primary WINS server that maintains the database of computer names and IP addresses.
Secondary WINS server	The secondary WINS server that maintains the database of computer names and IP addresses.
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.

Enable IPv6

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

Network type

LAN

PPPoE

User name:

Password:

Confirm password:

Enable IPv6

[IPv6 information](#)

Manually setup the IP address

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.

[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe0e:d4c8/64@Link

[Gateway]
IPv6 address list of gateway

[DNS]
IPv6 address list of DNS

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

Refers to Ethernet

[eth0] address	
2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global	Link-global IPv6 address/network mask
fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link	Link-local IPv6 address/network mask
[Gateway]	
fe80::211:d8ff:fea2:1a2b	
[DNS]	
2010:05c0:978d::	

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: (Refer to **HTTP** streaming on page 19 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.

[eth0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299#64@Link

[ppp0 address]
fe80:0000:0000:0000:0202:d1ff:fe11:2299#10@Link
2001:b100:01c0:0002:0202:d1ff:fe11:2299#64@Global

[Gateway]
fe80::90:1a00:4142:8ced

[DNS]
2001:b000::1

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

Enable IPv6

IPv6 information

Manually setup the IP address

Optional IP address / Prefix length /

Optional default router

Optional primary DNS

Streaming protocols

To utilize HTTP authentication, make sure that you have set a password for the Network Camera first; refer to **Security > User account** on page 63 for details.

HTTP RTSP

Authentication:

HTTP port:

Secondary HTTP port:

Access name for stream 1:

Access name for stream 2:

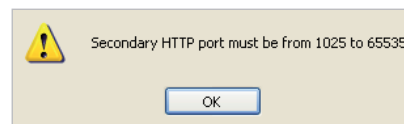
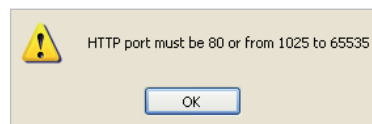
Access name for stream 3:

Save

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 access.

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. To access a video stream using http the video mode must be set to JPEG.

To configure JPEG video go to Camera>Video> Stream and select JPEG.

Stream names for http video are:

stream1.mjpg

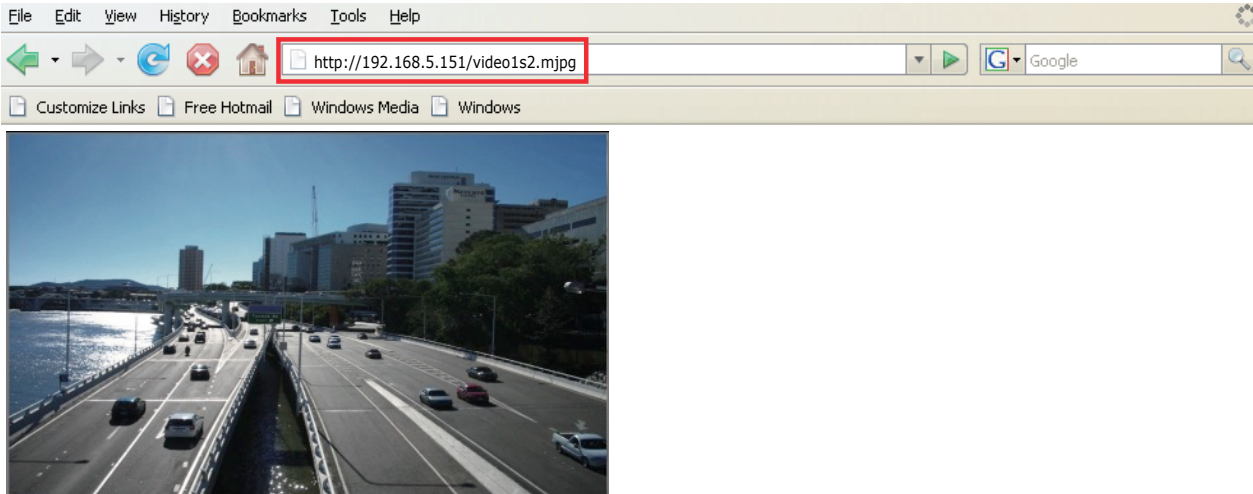
stream2.mjpg

stream3.mjpg

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 **stream2.mjpg**:

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



RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first.

HTTP
RTSP

Authentication:

RTSP port:

RTP port for video:

RTCP port for video:

RTP port for metadata:

RTCP port for metadata:

RTP port for audio:

RTCP port for audio:

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. This provides better protection against unauthorized access.

The availability of the RTSP streaming for the three authentication modes is listed below:

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

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

RTSP stream names are:

stream1.sdp

stream2.sdp

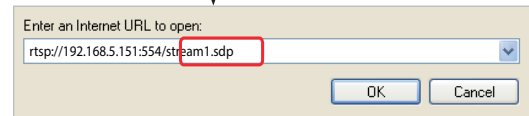
stream3.sdp

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 [stream1.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.

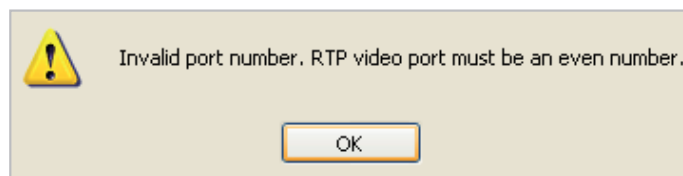


RTSP port /RTP port for video, audio/ RTCP port for video, audio

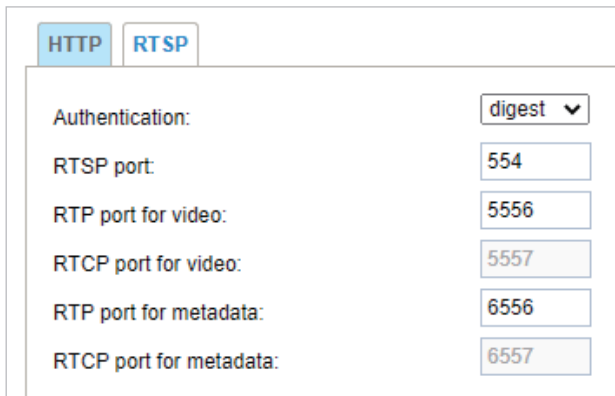
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556.
- The RTCP (Real-time Transport 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:

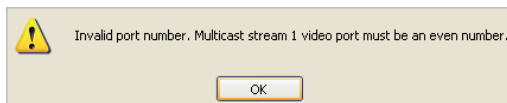


Multicast settings for streams: Click the pull-down menu for **Multicast settings for** and select stream 1, 2 or 3.



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 (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 metadata 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 LINEAR 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 > 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 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 CoS 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 style="width: 50px;" type="text" value="1"/>
Live video:	<input style="width: 40px;" type="text" value="0"/> ▼
Live audio:	<input style="width: 40px;" type="text" value="0"/> ▼
Event/Alarm:	<input style="width: 40px;" type="text" value="0"/> ▼
Management:	<input style="width: 40px;" 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, reserving the right amount of bandwidth.

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:

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, 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.

<input checked="" type="checkbox"/>	Enable SNMPv1, SNMPv2c
Read/Write community:	<input type="text" value="private"/>
Read only community:	<input type="text" value="public"/>

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).

<input checked="" type="checkbox"/>	Enable SNMPv3
Read/Write security name:	<input type="text" value="private"/>
Authentication type:	<input type="text" value="MD5"/>
Authentication password:	<input type="text"/>
Encryption password:	<input type="text"/>
Read only security name:	<input type="text" value="public"/>
Authentication type:	<input type="text" value="MD5"/>
Authentication password:	<input type="text"/>
Encryption password:	<input type="text"/>

Network > FTP

FTP is disabled by default. 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. By default, the FTP port is set to 21. It can also be assigned to another port number between 1025 and 65535.

Tips:

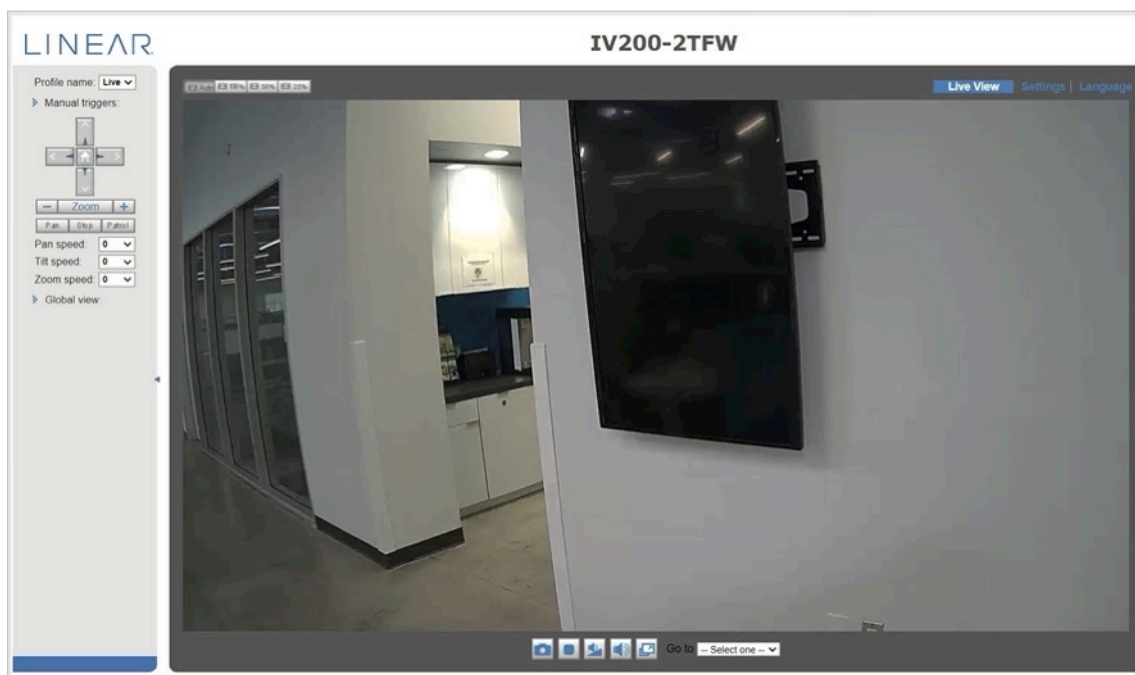
You can FTP the camera's IP address to download videos recorded in the SD card, or use the "<http://ip/cgi-bin/admin/lscrtl.cgi?cmd=search>" command to examine the recorded files on your SD card.

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices and LINEAR® NVR.

Using Web Browsers

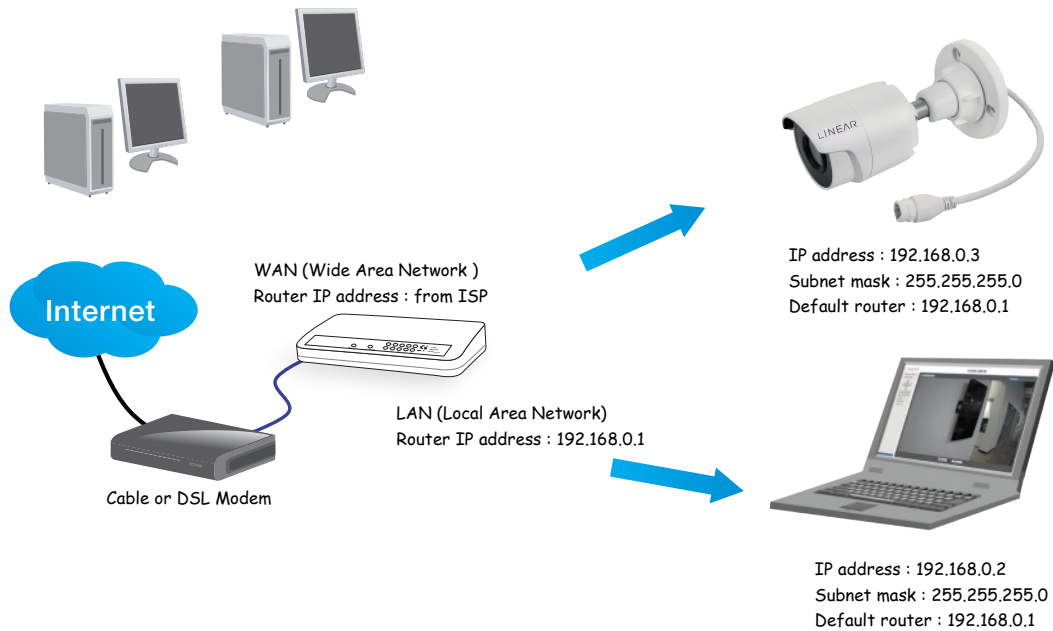
1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
 2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
 3. Live video will be displayed in your web browser.
- *By default, the Network Camera has a **user name: admin** and **password: linear**. It is highly recommended to change both for security purposes. For more information about how to enable password protection, refer to **Security** on page 62.*



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.



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

NOTE:

For information on how to forward ports on the router, refer to your router's user's manual.

Port forwarding can provide a security vulnerability to the local network from the Internet. For a more secure method consider using a VPN connection.

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	192.168.0.1	
Camera 1	192.168.0.2:80	122.146.57.120:8000
Camera 2	192.168.0.3:80	122.146.57.120:8001
...

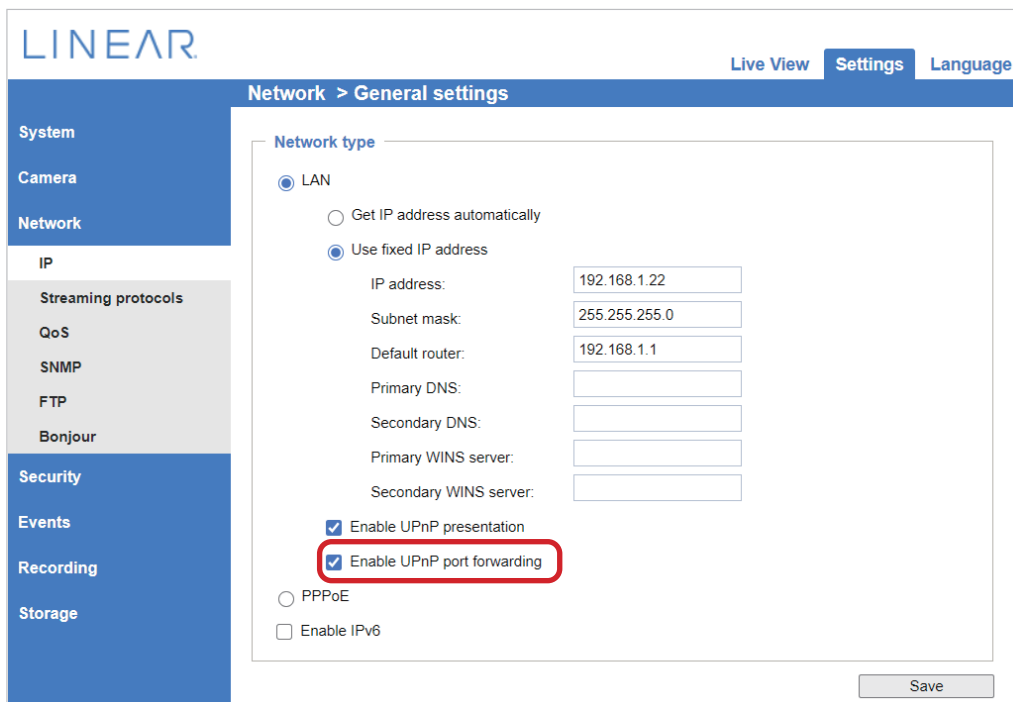
Configure the router, virtual server or firewall so that the router can forward any data coming into a pre-configured port number to a network camera on the private network, in order to allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.0.1:80
122.146.57.120:8001	192.168.0.3:80
...	...

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, 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. 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), refer to Settings > Network > IP. Also provided is the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.



Using RTSP Players

To view the streaming media using RTSP players, use one of the following players that support RTSP streaming:

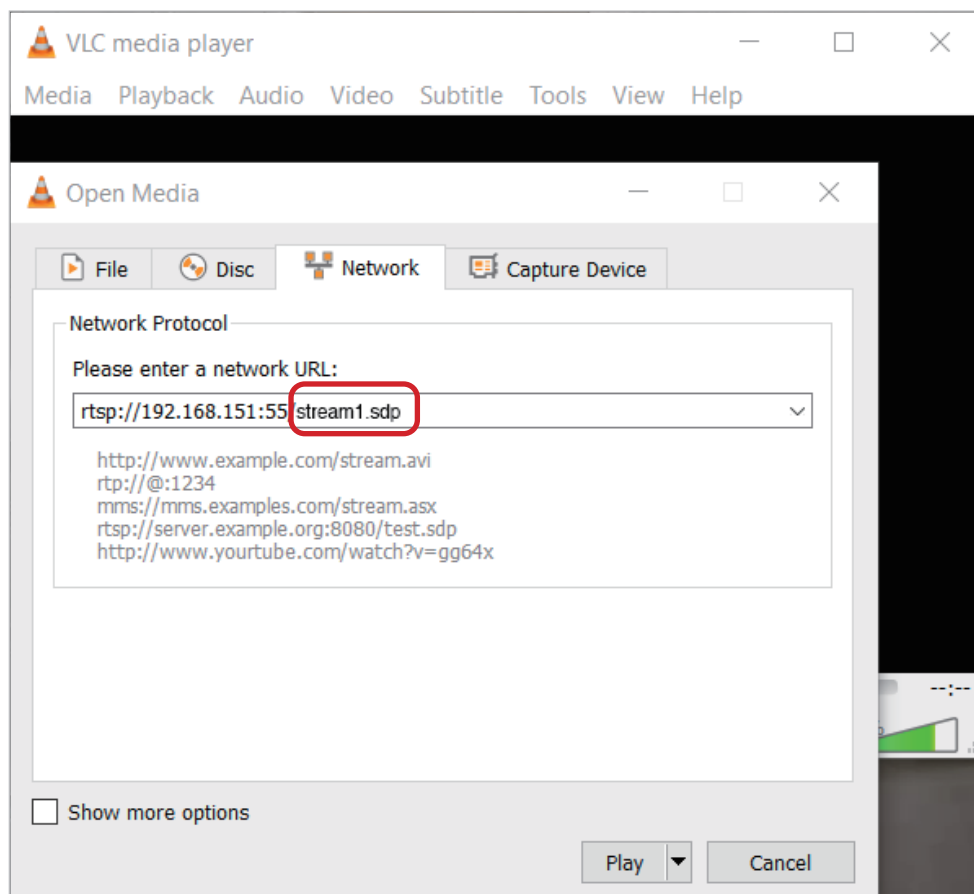
	Quick Time Player
	VLC media player

1. Launch the RTSP player.
2. 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, set the RTSP port to 554. For more information, refer to **RTSP Streaming** on page 20.

For example:

3. The live video will be displayed in your player.



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, refer to **Accessing the Network Camera** on page 26.

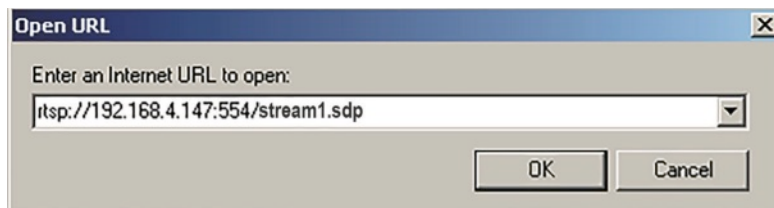
To utilize this feature, check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
2. As the bandwidth on 3G networks is limited, you will not be able to use a large video size. Go to Settings > Camera > Video to set the video streaming parameters as listed below.

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, set the RTSP port to 554.
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>`.

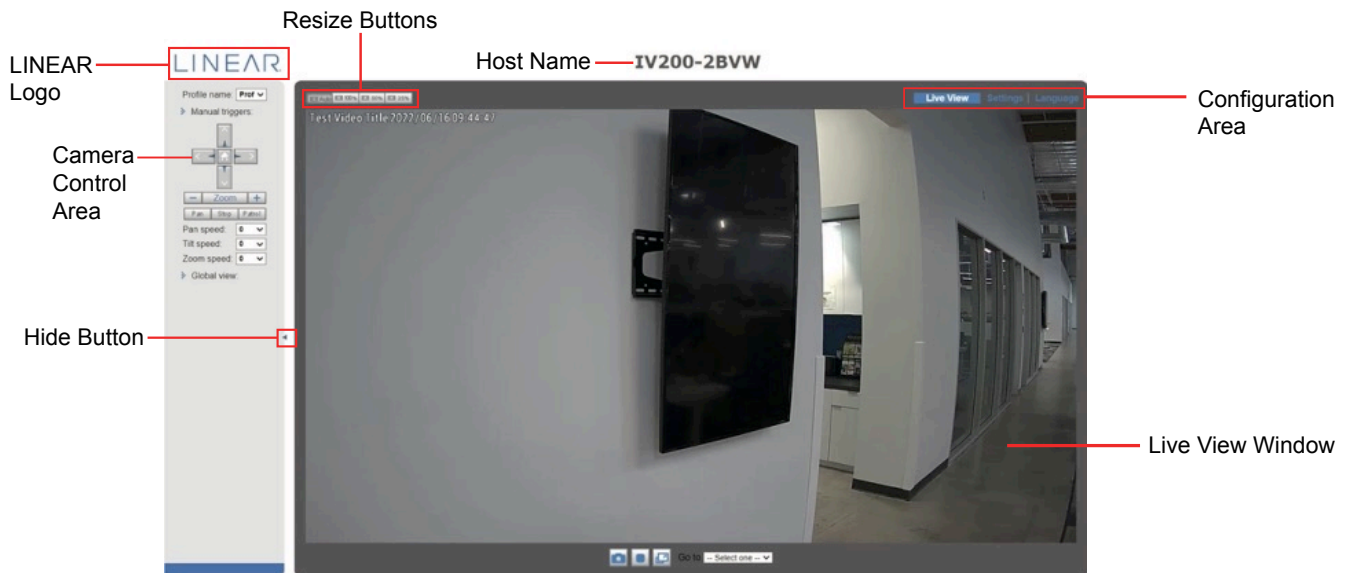
For example:



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

Main Page

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



LINEAR Logo

Click this logo to visit the LINEAR website.

Host Name

The host name can be customized to fit your needs. The name can be changed, especially if there are many cameras in your surveillance deployment. For more information, refer to **System** on page 36.

Camera Control Area

<p>Video Stream</p>	<p>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, refer to page 53 for detailed information.</p>
<p>Manual Trigger</p>	<p>Click to enable/disable an event trigger manually. Configure an event setting on the Application page before you enable this function. A total of 3 event configuration can be configured. If you want to hide this item on the home page, go to Configuration > System > Home page Layout > General settings > Customized button to deselect the “show manual trigger button” checkbox.</p>

Configuration Area

<p>Settings</p>	<p>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 only the administrator can configure the Network Camera. For more information, refer to Configuration on page 35.</p>
<p>Language</p>	<p>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. Note that you can also change a language on the Configuration on page 44.</p>

Hide Button

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

Resize Buttons

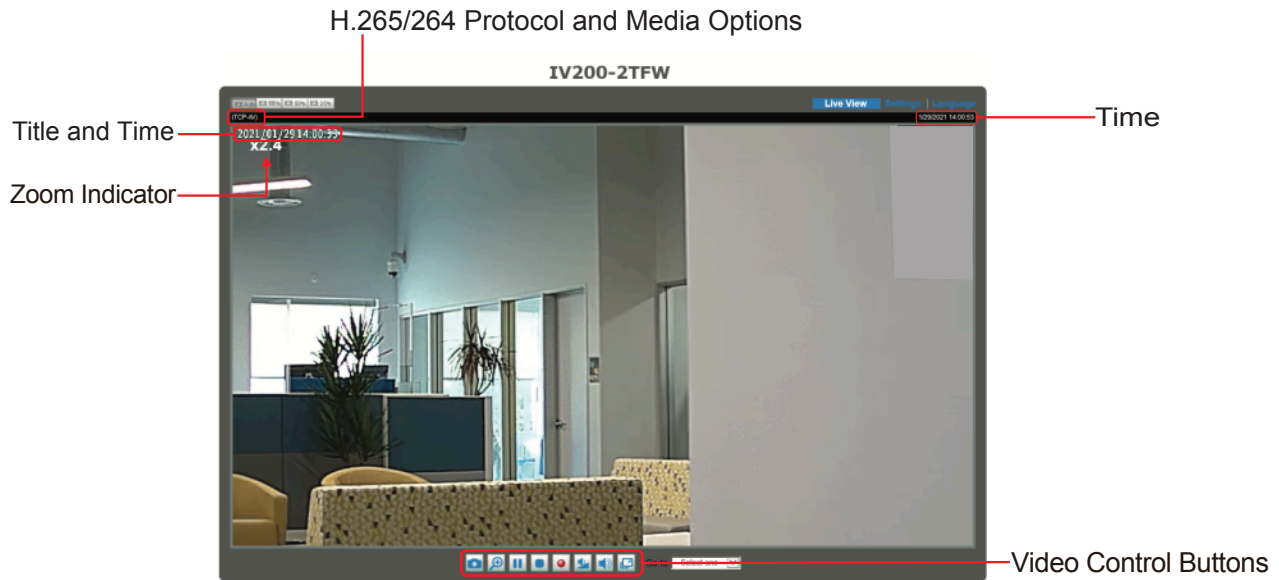


Click the Auto button, the video cell will resize automatically to fit the monitor.

Click 100% is to display the original home page size.

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

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

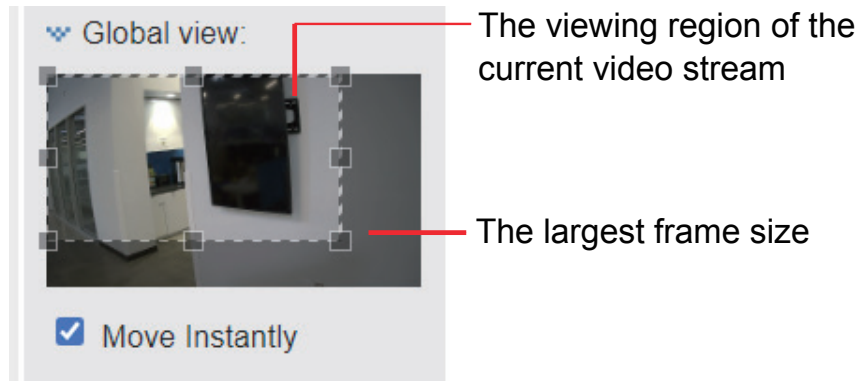




Live Video Window

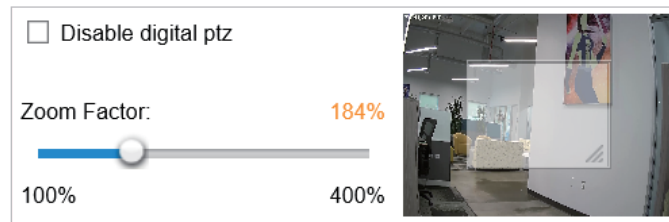
■ The following window is displayed when the video mode is set to H.264 or H.265:








<p>Video Title</p>	<p>The video title can be configured. Refer to Stream Settings on page 44.</p>
<p>H.264 or H. 265 Protocol and Media Options</p>	<p>The transmission protocol and media options for H.264 or H.265 video streaming.</p>
<p>Time</p>	<p>The current time. For further configuration, refer to Camera > Image on page 44.</p>
<p>Title and Time</p>	<p>The video title and time can be stamped on the streaming video. For further configuration, refer to Camera > Image on page 44.</p>

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).
-------------	---





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 (Motorized Lens only)	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.

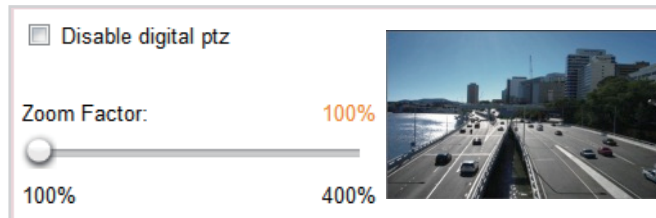





 Pause	Pause the transmission of the streaming media. The button becomes the Resume button  after clicking the Pause button.
 Stop	Stop the transmission of the streaming media. Click the Resume button  to continue transmission.
 Start MP4 Recording	Click this button to record video clips in MP4 file format to your computer. Press the  Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly.
 Full Screen	Click this button to switch to full screen mode. Press the “Esc” key to return 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, refer to Camera > Image on page 44.
Time	Display the current time. For more information, refer to Camera > Image on page 44.
Title and Time	Video title and time can be stamped on the streaming video. For more information, refer to Camera > Image on page 44.
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 (Motorized Lens only)	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.
 Full Screen	Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Settings

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

Provided is 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:

The screenshot displays the LINEAR camera's settings interface. At the top right, there are three buttons: 'Live View', 'Settings', and 'Language', which are highlighted with a red box and labeled 'Navigation Options'. Below these is a breadcrumb trail 'System > General settings'. The main content area is divided into two sections: 'System' and 'System time'. The 'System' section includes a 'Host name' field with the value 'IV200-2TFW' and a checkbox for 'Turn off the LED indicator'. The 'System time' section includes a 'Time zone' dropdown menu set to 'GMT-08:00 Las Vegas, San Francisco, Vancouver', a checked checkbox for 'Enable daylight saving time', and fields for 'Starting time' (2021/03/14 02:00:00) and 'Ending time' (2021/11/07 02:00:00). There are also radio buttons for 'Keep current date and time', 'Synchronize with computer time', 'Manual', and 'Automatic' (selected). Below these are fields for 'NTP server' (169.254.61.222) and 'Updating interval' (One day). A 'Save' button is located at the bottom right of the settings area. On the left side, there is a 'Configuration List' menu with categories: System (General settings, Homepage layout, Client settings, Logs, Parameters, Maintenance), Camera, Network, Security, Events, Recording, and Storage. At the bottom left, the 'Firmware Version' is displayed as 'Version: 0100f'.

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), **Settings** page and multi-language selection.

System > General settings

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

System

Host name	Enter a desired name for the Network Camera. This can be a descriptive name such as where the camera is located i.e. "Front Lobby".
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

Host name:

Turn off the LED indicator

System time

System time

Time zone:

Enable daylight saving time

Starting time:

Ending time:

Keep current date and time

Synchronize with computer time

Manual

Automatic

NTP server:

Updating interval:

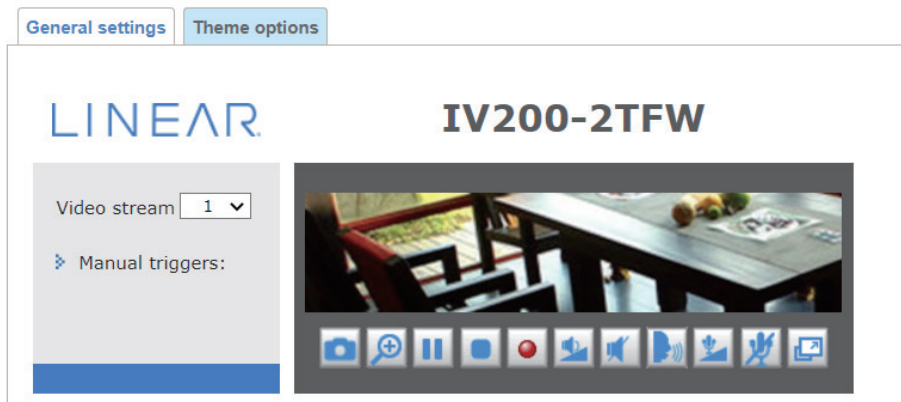
Time zone	Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, refer to System > Maintenance > Import/ Export files on page 41 for details.
Keep current date and time	Select this option to preserve the current date and time of the Network Camera. The Network 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.
<u>NTP server</u>	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.
<u>Update interval</u>	Select to update the time using the NTP server on an hourly, daily, weekly or monthly basis.

System > Home page layout

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

General settings

This column shows the settings of your home page 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 home page using the default settings:



Logo graph

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

Logo graph

Default
 Custom

LINEAR

Logo link:

Customized button

Show manual trigger button

Save

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 home page, uncheck this item. This item is checked by default.

Customized button

Show manual trigger button

Save

Theme Options

Here you can change the color of your home page 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.

The screenshot shows the 'Theme options' configuration interface. At the top, there are two tabs: 'General settings' and 'Theme options'. The main area is divided into a preview and a configuration panel. The preview shows a video player with the 'LINEAR' logo on the left and a video stream titled 'IV200-2TFW' on the right. Below the video is a control area with various icons. The configuration panel has two columns: 'Themes' and 'Color'. The 'Themes' column has three preset patterns and a 'Custom' option. The 'Color' column has seven color selection fields. A 'Save' button is located at the bottom right of the configuration panel.

Labels pointing to specific elements in the screenshot:

- Font Color (points to the 'Video stream' dropdown menu)
- Font Color of the Video Title (points to the 'IV200-2TFW' title)
- Color Background (points to the video player area)
- Frame Color (points to the border of the video player)
- Preset Patterns (points to the three theme options in the 'Themes' section)
- Save (points to the 'Save' button)

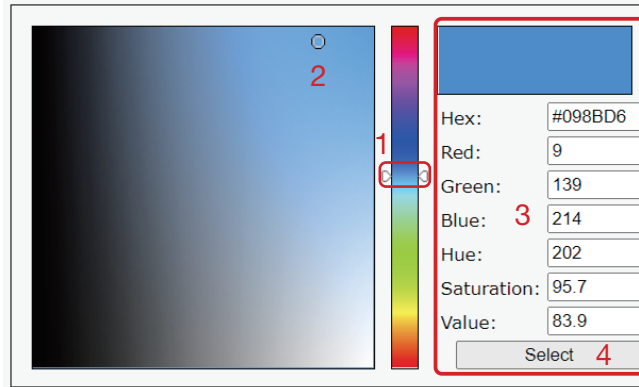
- Follow the steps below to set up the customized home page:
 1. Click **Custom** on the left column.
 2. Click the field where you want to change the color on the right column.

This close-up shows the 'Custom' theme selection and the 'Color' configuration panel. The 'Custom' option is selected in the 'Themes' section. The 'Color' section has seven color selection fields. The 'Font color of video title' field is highlighted with a red box and labeled 'Color Selector'.

Labels pointing to specific elements in the close-up:

- Custom Pattern (points to the 'Custom' radio button)
- Color Selector (points to the '#098BD6' color field)

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:

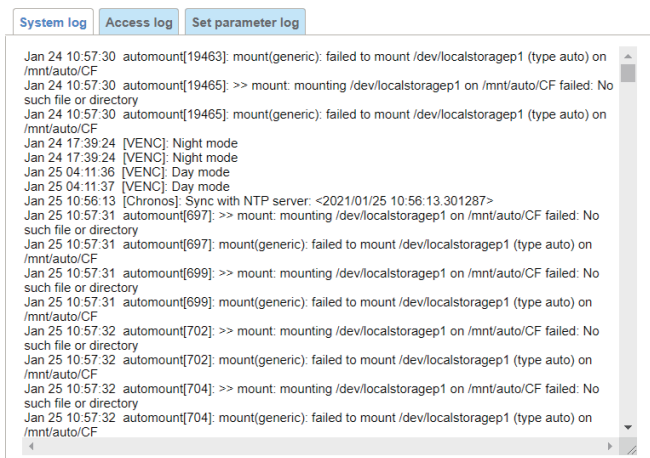
Follow the steps below to set up the remote log:

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

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera.

System log

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



Access log

System log **Access log** Set parameter log

```
Oct 29 09:13:05 [Authorization Center]: IP(192.168.1.1) tried to login(WSS) with username(admin), but login failed
Oct 29 09:13:06 [Authorization Center]: IP(192.168.1.1) tried to login(WSS) with username(admin), but login failed
Oct 29 09:13:07 [Authorization Center]: IP(169.254.50.150) tried to login(WSS) with username(admin), but login failed
```

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

System > Parameters

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

Parameters

```
system_hostname='IV200-2TFW'
system_ledoff='0'
system_lowlight='1'
system_date='2021/02/01'
system_time='14:05:18'
system_datetime=''
system_ntp='169.254.61.222'
system_daylight_enable='1'
system_daylight_auto_begintime='2021/03/14 02:00:00'
system_daylight_auto_endtime='2021/11/07 02:00:00'
system_daylight_timezones='0'
system_updateinterval='86400'
system_info_modelname='IV200-2TFW'
system_info_extendedmodelname='IV200-2TFW'
system_info_serialnumber='F0D14F810060'
system_info_firmwareversion='IT9360-NORK-0100f'
system_info_language_count='4'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4=''
system_info_language_i5=''
system_info_language_i6=''
system_info_language_i7=''
system_info_language_i8=''
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
system_info_language_i13=''
```

System > Maintenance

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

General settings > Upgrade firmware

Upgrade firmware

Firmware file:

Choose File No file chosen

Upgrade

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

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

The following message is displayed when the upgrade has succeeded.

Reboot system now!!
This connection will close.

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

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

General settings > Reboot

Reboot

Reboot

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

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



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

General settings > Restore

Restore

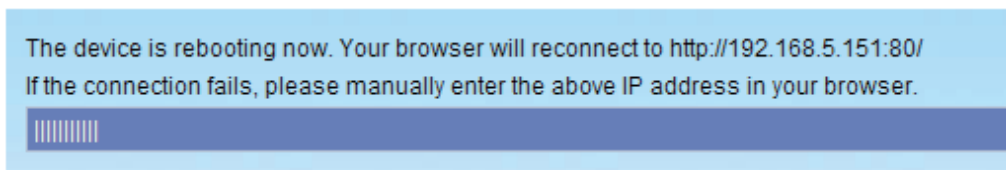
Restore all settings to factory default except settings in

Network
 Daylight saving time
 Custom language

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

Network	Select this option to retain the Network Type settings (refer to Network Type on page 15).
Daylight Saving Time	Select this option to retain the Daylight Saving Time settings (refer to Import/Export files below on this page).
Custom Language	Select this option to retain the Custom Language settings.
Focus position	Retain the lens focus position using the previously saved position parameters.

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



Import/Export files

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

Follow the steps below to export:

General settings | **Import/Export files**

Export files

Export language file:

Export configuration file:

Export server status report:

Upload files

Update custom language file: No ...sen

Upload configuration file: No ...sen

In the Export files column, click on the **Export** button to export the following:

- Language:** Will export an XML file for the current configured language.
- Export Configuration file:** Will export an encrypted configuration file that can be used to configure additional cameras or used as backup file.
- Export Server Status Report:** Will export a compressed server report file.

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



Export language file	Click to export language strings. LINEAR provides nine languages: <i>English, Deutsch, Español, Français, Italiano</i> , 日本語, <i>Português</i> , 簡體中文 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. 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 and kernel message.

Tips:

- If a firmware upgrade is accidentally disrupted (for example, a power outage), there is a last resort method to restore normal operation. Refer to the following options to restore the camera:

Applicable scenario:

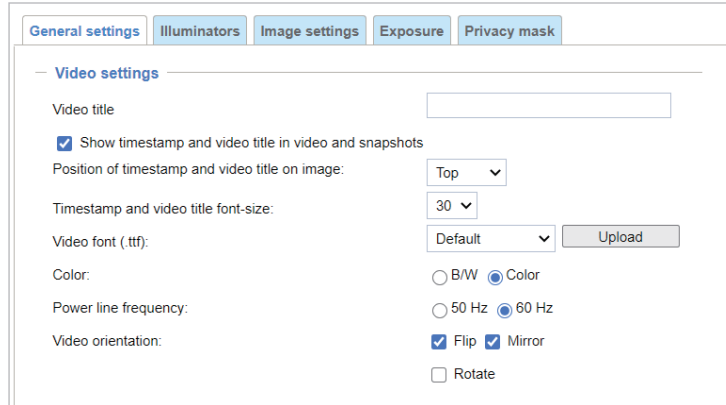
- a. Power disconnected during firmware upgrade.
- b. Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

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.

Camera > Image

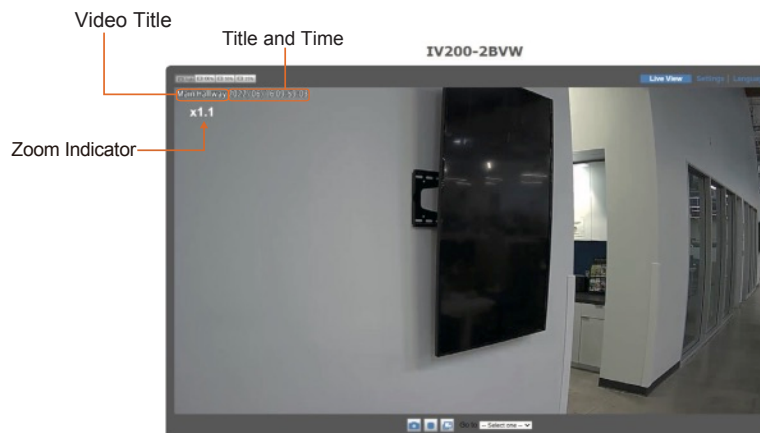
This section explains how to configure the image settings of the Network Camera. It is composed of the following columns: General settings, Illuminators, Image settings, Exposure, Focus, and Privacy mask. The Focus window is available only for models that come with motorized lens.



General settings

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 (<u>Motorized Lens only</u>).
Position of timestamp and video title on image	Click Browse... and specify your own custom language file to upload.
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 stream

Video title



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.
----------------------	--

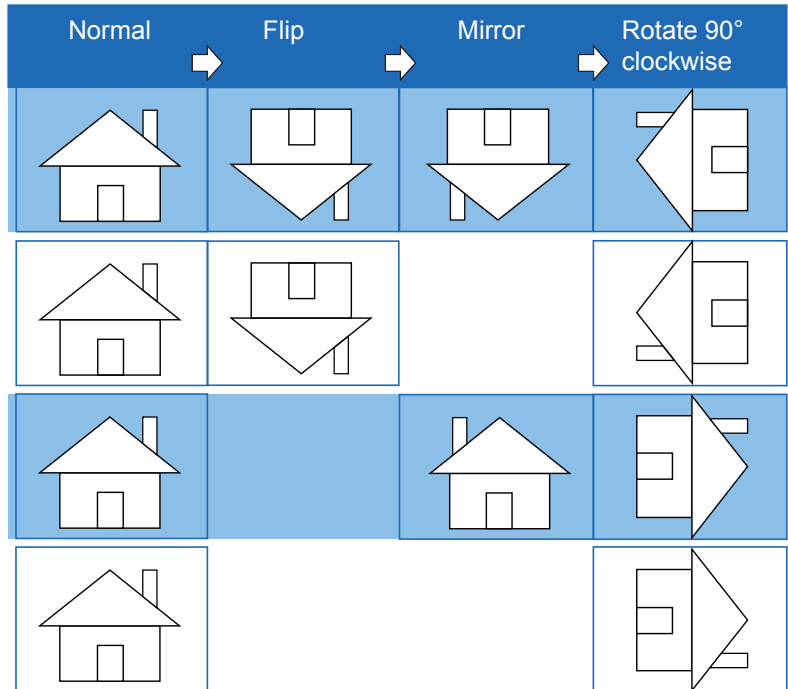
Video orientation Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Note that if you have preset locations, those 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:

Sensitivity of IR cut filter:

Select auto mode will disable profile of exposure settings.

Switch to B/W in night mode

Select this to enable the Network Camera to automatically switch to Black/White during night mode.

IR cut filter

With a removable IR-cut filter, this Network Camera can automatically remove the filter to let Infrared light pass into the sensor during low light conditions.

- **Auto mode:** (The **Day/Night Exposure Profile** will not be available if Auto mode is selected). The Network Camera automatically removes the filter by judging the level of ambient light.
- **Day mode:** In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.
- **Night mode:** In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.
- **Schedule mode:** 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.

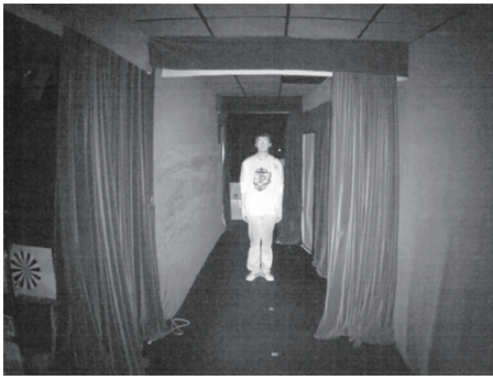
Illuminators

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.

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

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 51.

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

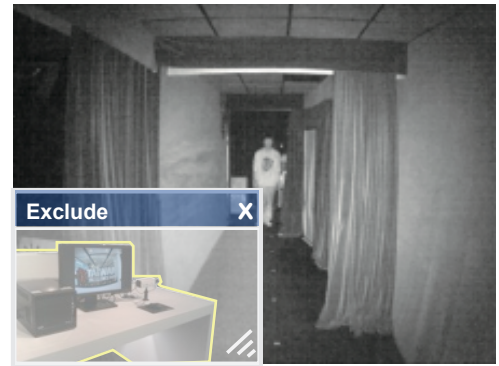
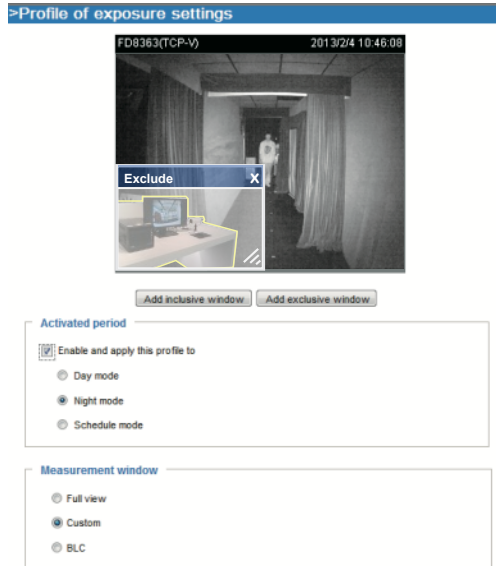


Image settings

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



Sensor Setting 2:
For special situations. To enable, go to *General Settings* > *Day/ Night settings* > *IR cut filter* and select **Day mode**, **Night mode** or **Schedule mode**.

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

Noise reduction

The noise reduction feature reduces 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 all changes made to image settings are 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. Manually enter a range of time if you choose the Schedule mode. Then click **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.
To enable, go to General Settings > Day/Night settings > IR cut filter and select **Day** mode, **Night** mode or **Schedule** mode.

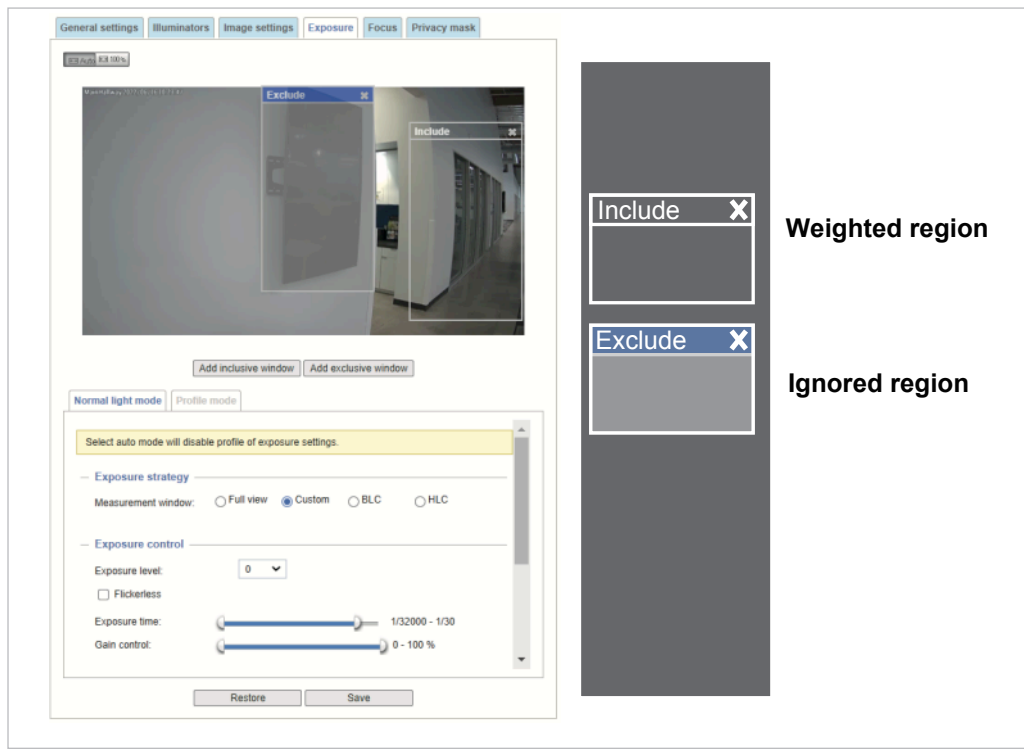
Sensor Setting 1:
For normal situations

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. Refer to the next page for detailed illustration.

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.



- **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.
- **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 lights 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:

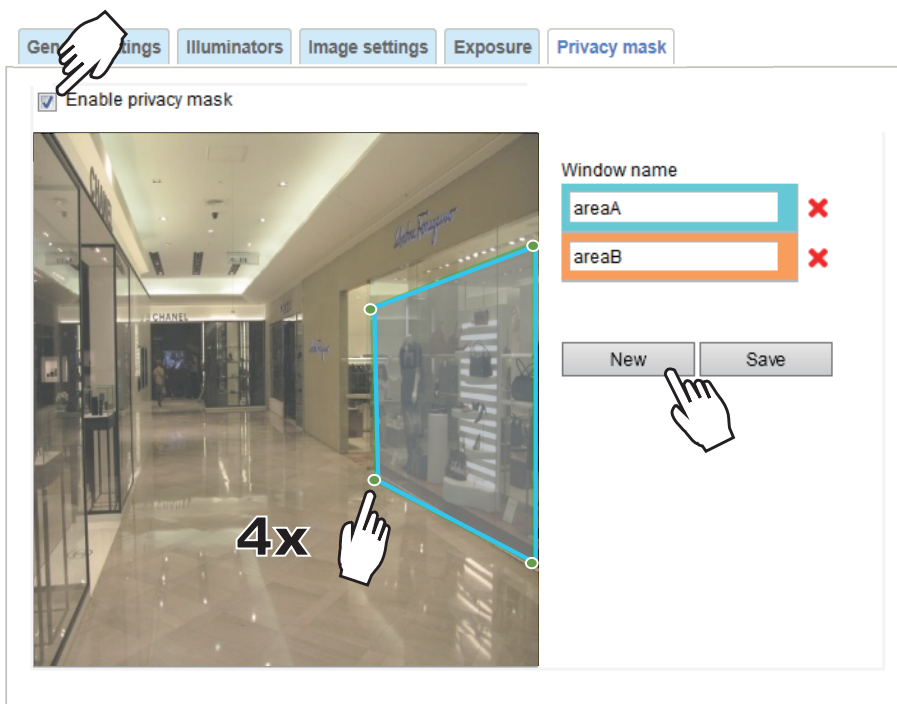
This refers to the Wide Dynamic Range function that enables the camera to capture details in a high contrast environment. Use the checkbox to enable the function, and use the slide bar to select the strength of the WDR Pro functionality (depending on the lighting condition at the installation site). 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 (for example, 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.

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



NOTE:

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

Stream settings

Stream

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

Save

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.

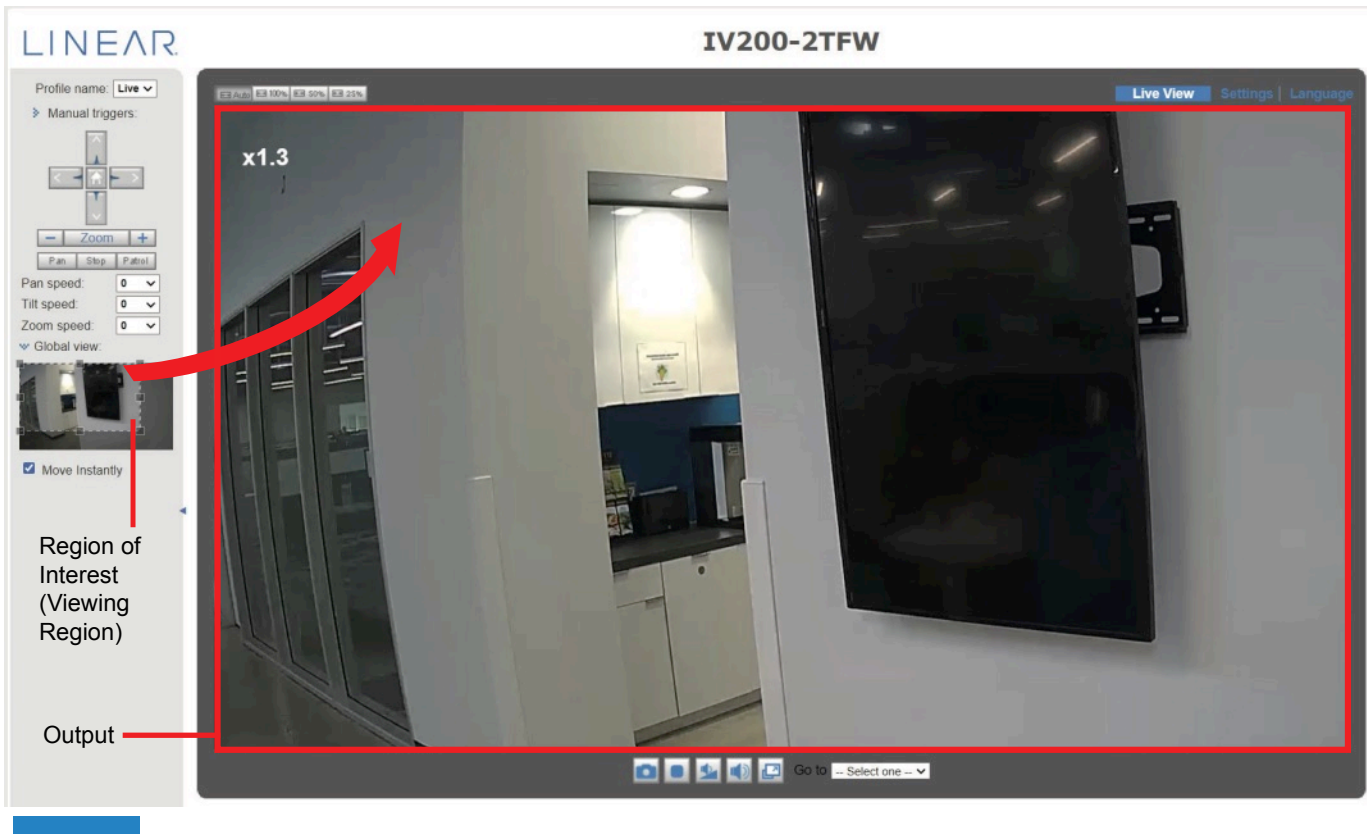
Click **Viewing Window** to open the viewing region settings page. On this page, you can configure the **Region of Interest** and the **Output Frame Size** for a video stream. For example, you can crop only a portion of the image that is of your interest, and thus save the bandwidth needed to transmit the video stream. As the picture shown below, the area of your interest in an office should be the people. The ceiling above is of little value for the purpose of surveillance.





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.



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

The screenshot shows a 'Stream' configuration window with three sections for 'Video settings for stream 1', 'Video settings for stream 2', and 'Video settings for stream 3'. Stream 1 and Stream 2 are expanded, showing H.265 settings. Stream 3 is collapsed. A 'Save' button is at the bottom right.

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:

This is a close-up of the 'Video settings for stream' window. The 'H.265' radio button is selected and highlighted with a red box. The settings shown are: Resolution: 1424x1080, Maximum frame rate: 30 fps, Intra frame period: 1 S. Under 'Smart stream III', 'Dynamic intra frame period' is checked, 'Smart FPS' is unchecked, and 'Smart codec' is checked. The 'Mode' is set to 'Auto tracking'. Under 'Bit rate control', 'Fixed quality' is selected with a quality of 'Good'.

■ Resolution

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 IB9365 supports a frame rate of up to 60fps.

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

■ Intra frame period

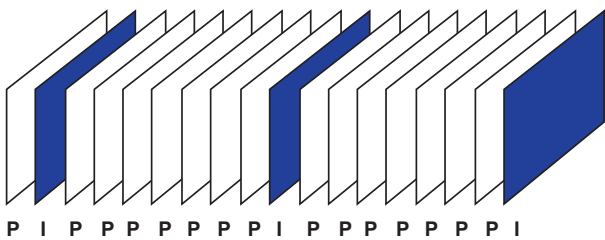
Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds,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

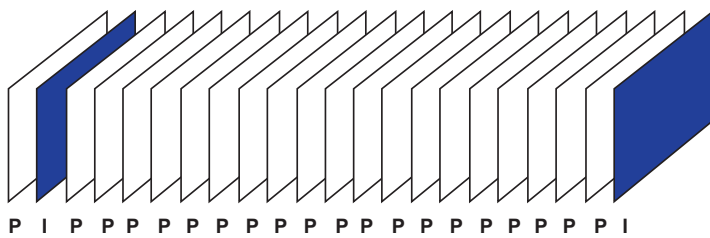
The encoding parameters are summarized and illustrated below. The **I-frames** are completely self-referential and they are largest in size. The **P-frames** are predicted frames. The encoder refers to the previous I- or P-frames for redundant image information.



H.264/265 Frame Types

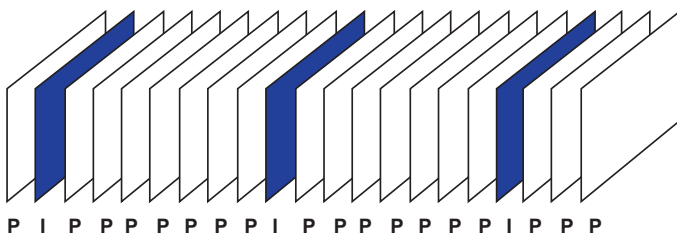
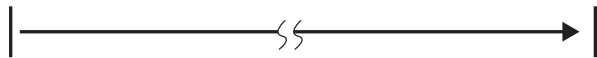
By dynamically prolonging the intervals for I-frames insertion to up to 10 seconds, the bit rates required for streaming a video can be tremendously reduced. When streaming a video of a static scene, the Dynamic Intra frame feature can save up to 53% of bandwidth. The amount of bandwidth thus saved is 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, therefore 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. During the no-traffic period of time, it can reduce down to 500kb/s.



Dynamic Intra Frame w/ static scenes

Static scene



Dynamic Intra Frame w/ activities in scenes

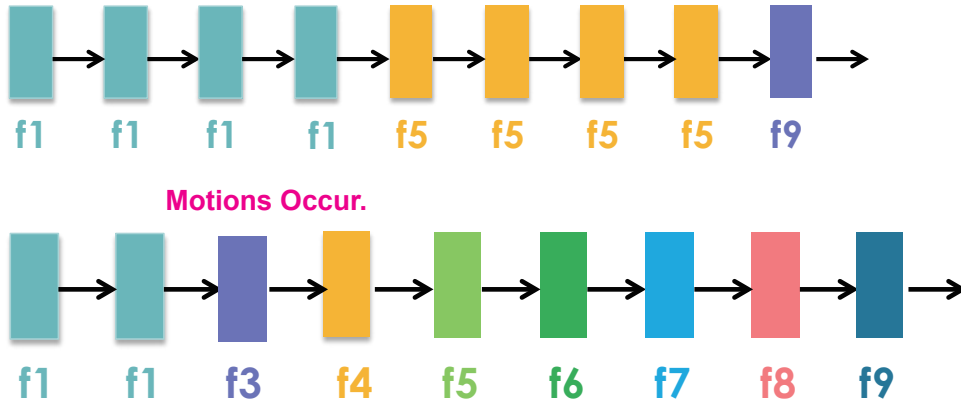
Activities



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.

- **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.

Smart stream II

Dynamic intra frame period ([Help](#))

smart_codec:

Mode: Manual

[Manual window setting](#)

Quality priority: ([Help](#))

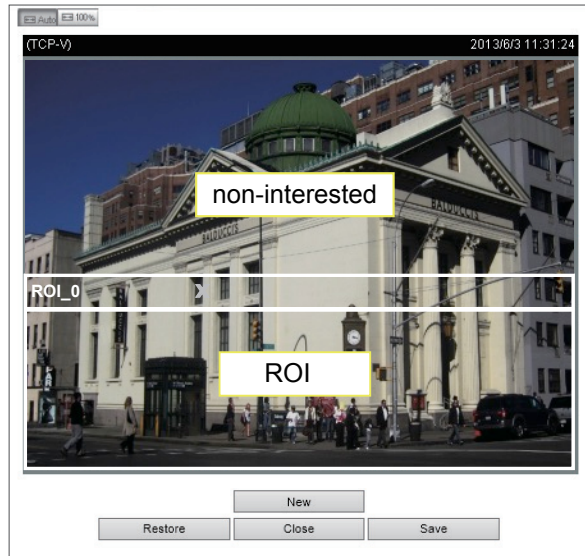
The user can adjust the quality balance between ROI (Region of Interest) and non-ROI area. Moving the selector to the right side gives more quality priority on ROI area, whereas moving the selector to the left side gives more quality priority on non-ROI area.

Example:

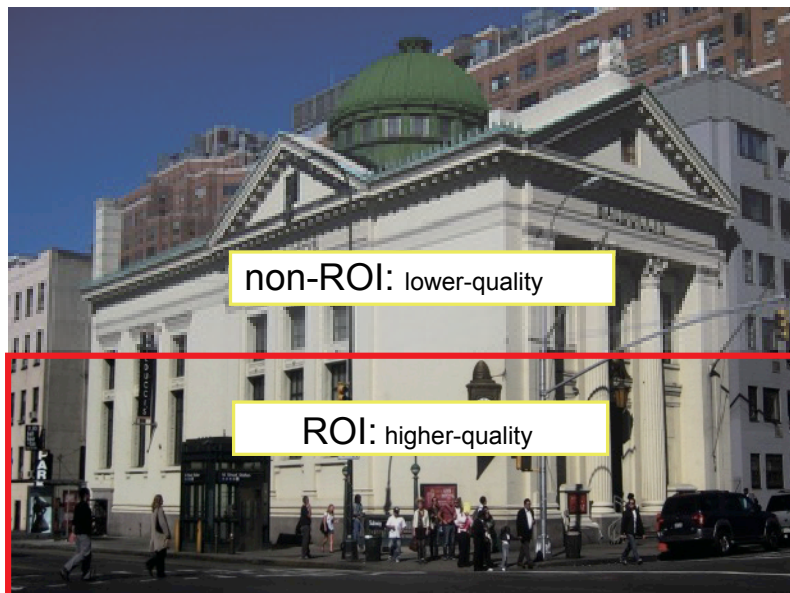
Select an operation mode if Smart codec is preferred.

- **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:** 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:

The screenshot shows a configuration window for MJPEG mode. At the top, the 'JPEG' radio button is selected and highlighted with a red rectangular box. Below it, the 'Resolution' is set to '1424x1080' in a dropdown menu. The 'Maximum frame rate' is set to '10 fps' in another dropdown menu. Under the 'Bit rate control' section, the 'Fixed quality' radio button is selected. The 'Quality' is set to 'Good' in a dropdown menu, and the 'Maximum bit rate' is set to '80 Mbps' in a final dropdown menu.

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

Security > Users

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

Account management

The administrator account name is “admin”, which is permanent and can not be deleted. If you want to add more accounts in the Account management window, apply the password for the “admin” 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. Viewers can only access the main page for live viewing.

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

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

Security > HTTPS (Hypertext Transfer Protocol over SSL)

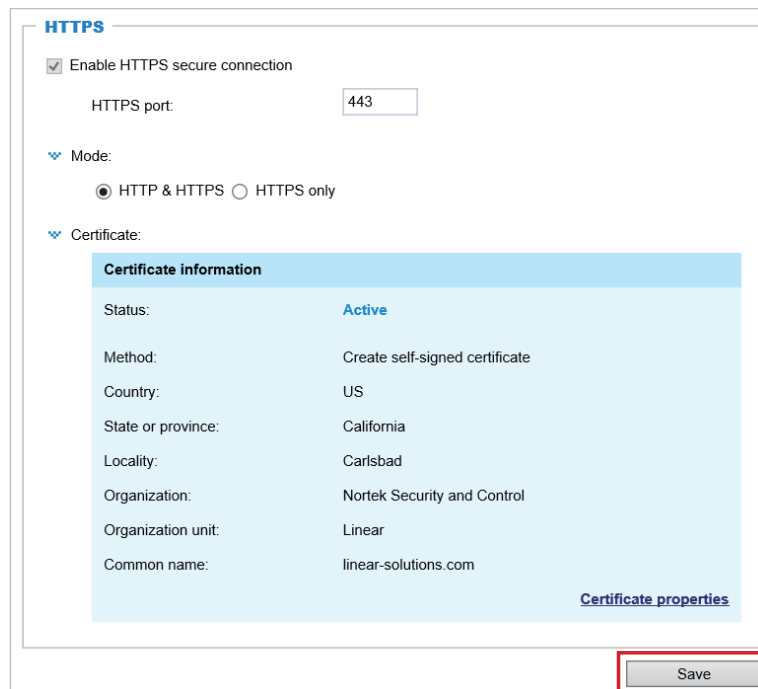
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

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

Create self-signed certificate

1. First, select Enable HTTPS secure connection, then select a mode: “HTTP & HTTPS” or “HTTPS only”.
2. Under Method, select “Create self-signed certificate” from the pull-down menu.
3. Click **Create certificate** to generate a certificate.
4. The Certificate Information will automatically be displayed as shown below. You can click Certificate properties to view detailed information about the certificate.

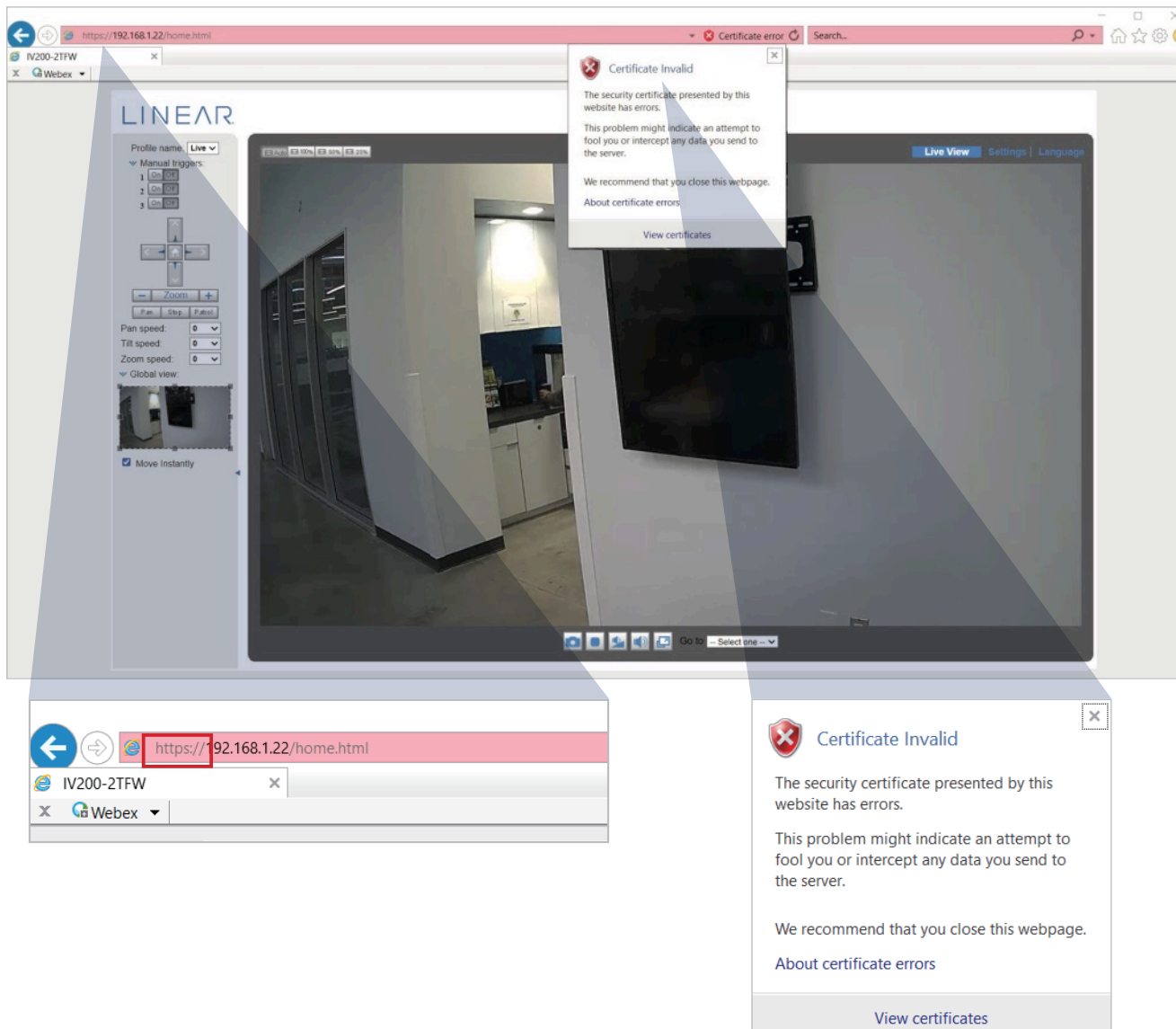


The screenshot displays the HTTPS configuration page. At the top, there is a section titled "HTTPS" with a sub-section "Certificate:" expanded. The "Enable HTTPS secure connection" checkbox is checked. The "HTTPS port" is set to 443. The "Mode" is set to "HTTP & HTTPS". The "Certificate:" section shows a table of certificate information:

Certificate information	
Status:	Active
Method:	Create self-signed certificate
Country:	US
State or province:	California
Locality:	Carlsbad
Organization:	Nortek Security and Control
Organization unit:	Linear
Common name:	linear-solutions.com

At the bottom right of the certificate information table, there is a link labeled "Certificate properties". Below the entire configuration area, there is a "Save" button highlighted with a red 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 may appear. Click **OK** or **Yes** to enable HTTPS.



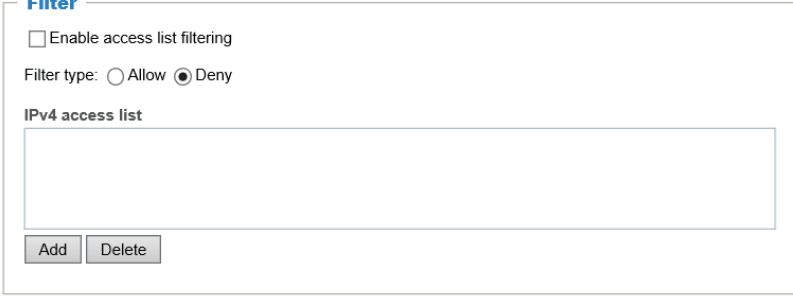
Security > Access List

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

Filter

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

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



The screenshot shows a configuration window titled "Filter". It contains the following elements:

- A checkbox labeled "Enable access list filtering" which is currently unchecked.
- A "Filter type" section with two radio buttons: "Allow" (unchecked) and "Deny" (checked).
- A section titled "IPv4 access list" containing a large, empty rectangular text area for listing IP addresses.
- At the bottom of the list area, there are two buttons: "Add" and "Delete".

Then you can **Add** a rule to the following Access List. Note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, refer to **Network > General settings** on page 15 for detailed information.

Click **Add** to create a new rule. There are three types of rules:

Single: This rule allows the user to add a single IP address to the Allowed/Denied list.

For example:

Filter address

Rule:

IP address:

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

For example:

Filter address

Rule:

Network address / Network mask: /

IP address range 192.168.2.x will be blocked.

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

Filter address

Rule:

Network address / Network mask: /

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.

Note: This rule only applies to IPv4 addresses.

For example:

Filter address

Rule:

IP address - IP address: -

Administrator IP address

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

Administrator IP address

Always allow the IP address to access this device:

Security > IEEE 802.1X

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

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

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



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

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

Follow the steps below to enable 802.1x settings:

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

IEEE 802.1x

Enable IEEE 802.1x

EAP method: EAP-PEAP ▼

Identity:

Password:

CA certificate:

Status: no file

IEEE 802.1x

Enable IEEE 802.1x

EAP method: EAP-TLS ▾

Identity:

Private key password:

CA certificate: Browse... Upload

Status: no file Remove

Client certificate: Browse... Upload

Status: no file Remove

Client private key: Browse... Upload

Status: no file Remove

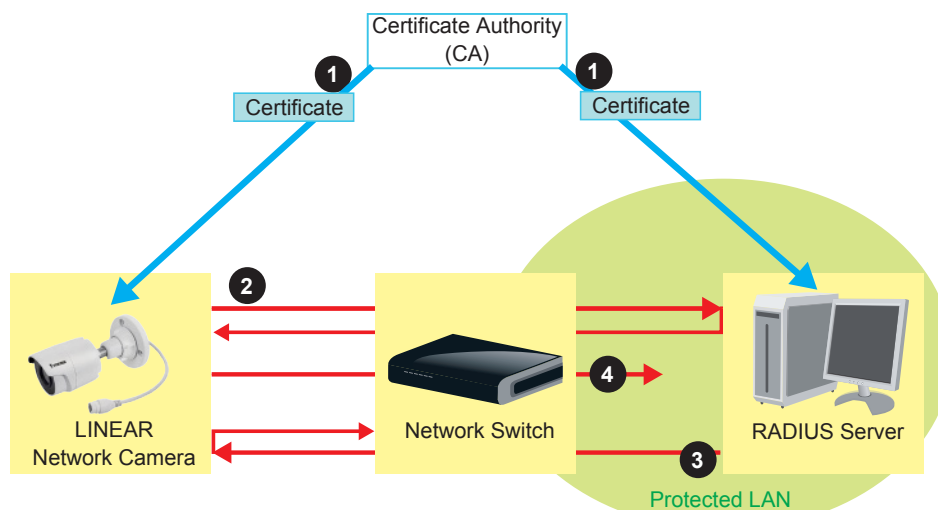
Save

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

 **NOTE:**

► *The authentication process for 802.1x:*

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



Events > Event settings

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

Events

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
Detector	OFF	V	V	V	V	V	V	V	00:00~24:00	Detector	Delete

[Add](#) [Help](#)

Event trigger → **Action (What to do)**

Ex.
Motion Detector, Periodically,
Digital input, System boot

Media (What to send)

Ex.
Snapshot, Video clip, System log,
Digital output

Server (Where to send)

Ex.
Email, FTP, HTTP server,
Network storage

Event

To configure an event with reactive measures such as recording video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window. Here you can arrange three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

Events

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
Detector	OFF	V	V	V	V	V	V	V	00:00~24:00	Detector	Delete

[Add](#) [Help](#)

Event name:

Enable this event

Priority: [Normal](#)

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

Event schedule

1. Schedule

2. Trigger

3. Action

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

[Save event](#) [Close](#)

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

1. Schedule

Specify the period of time during which the event trigger will take effect. Select the days of the week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, you may prefer an event to be triggered only during the off-office hours.

2. Trigger

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

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

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

Periodically

Trigger every other minute(s)

- **System boot:** This option triggers the Network Camera when the power to the Network Camera is disconnected and re-connected.

- **Recording notify:** This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite older data.

- **Audio Detector:** This option makes use of the built-in audio detection mechanism as a trigger source. Once Audio Detector is configured, select click **Normal** or **Profile** (or both).

Audio Detector

Normal: Trigger event when detected audio rises above alarm level

Profile: Trigger event when detected audio rises above alarm level

Note: Please configure Audio Detector first

To enable this function, you need to first configure **Audio Detection**.

Click **Enable audio detection**, then move the slider to an appropriate Alarm level.

Click **Profile** (next page).

Audio Detector

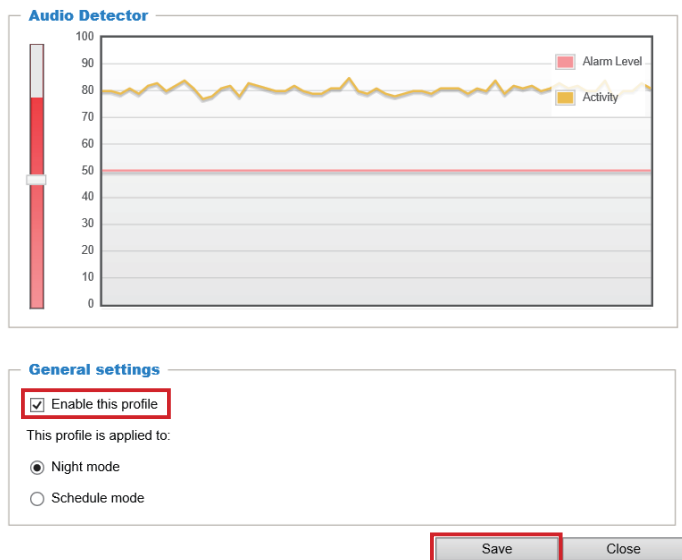
Enable audio detection

Profile

Save

Click **Enable this profile**, then select **Night mode** or **Schedule mode**.

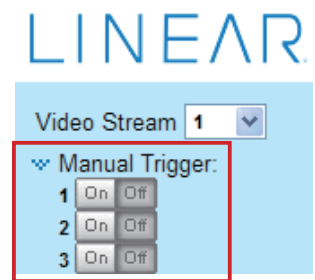
Click **Save**, then click **Close**.



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

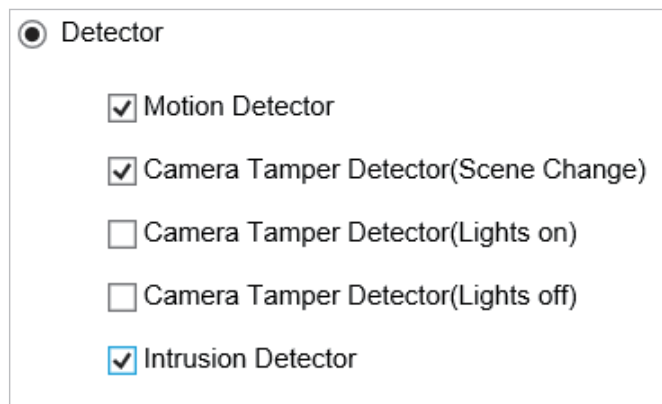
Manual triggers

1 2 3



- **Detector:** This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the **Tampering Detection** option first. Refer to page 86 for detailed information.

Click one or more detectors to configure.



3. Action

Define the actions to be performed by the Network Camera when a trigger is activated.

Action

Server	Media	Extra parameter
<input type="checkbox"/> SD	-----None-----	SD test
Add server	Add media	

Add server

It is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. Click **Add server** to open the server setting window. You can specify where the notification messages are sent to when a trigger is activated. A total of 5 server settings can be configured.

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

[Add server](#) [Add media](#)

Server name:

Server type

Email

Sender email address:

Recipient email address:

Server address:

User name:

Password:

Server port:

This server requires a secure connection

FTP

HTTP

Network storage

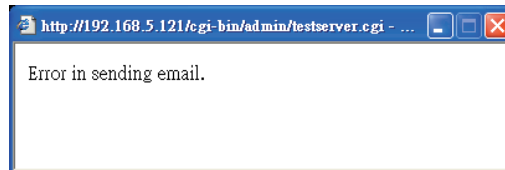
Server type - Email

Select to send the media files via email when a trigger is activated.

- **Server name:** Enter a name for the server setting.
- **Sender email address:** Enter the email address of the sender.
- **Recipient email address:** Enter the email address of the recipient.
- **Server address:** Enter the domain name or IP address of the email server.
- **User name:** Enter the user name of the email account if necessary.
- **Password:** Enter the password of the email account if necessary.
- **Server port:** The default mail server port is set to 25. You can also manually set another port.

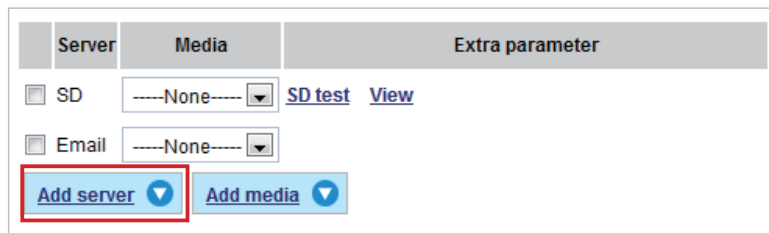
If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL)**.

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



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

Note that after you configure the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.



Server type - FTP

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

Server name:

Server type

Email

FTP

Server address:

Server port:

User name:

Password:

FTP folder name:

Passive mode

HTTP

Network storage

- **Server name:** Enter a name for the server setting.
- **Server address:** Enter the domain name or IP address of the FTP server.
- **Server port:** By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- **User name:** Enter the login name of the FTP account.
- **Password:** Enter the password of the FTP account.
- **FTP folder name:** Enter the folder where the media files will be placed. If the folder name does not exist, the Network Camera will automatically create one on the FTP server.

- **Passive mode:** Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall. The firmware default has the Passive mode checkbox selected.

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

ftp transmission successfully.

ftp transmission failed.

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

Server type - HTTP

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

The screenshot shows a configuration window for an HTTP server. At the top, there is a text input field labeled 'Server name' containing the text 'Email'. Below this is the 'Server type' section, which contains four radio button options: 'Email', 'FTP', 'HTTP' (which is selected), and 'Network storage'. Under the 'HTTP' option, there are three input fields: 'URL' containing 'http://', 'User name' (empty), and 'Password' (empty). At the bottom of the window, there are three buttons: 'Test', 'Save server', and 'Close'.

- **Server name:** Enter a name for the server setting.
- **URL:** Enter the URL of the HTTP server.
- **User name:** Enter the user name if necessary.
- **Password:** Enter the password if necessary.

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

HTTP Transmission successfully. Thanks

HTTP Transmission failed.

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

Network storage:

Select to send the media files to a networked storage when a trigger is activated. Refer to **NAS management** on page 89 for details. Note that only one NAS server can be configured.

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

Action

Backup media if the network is disconnected

Server	Media	Extra parameter
<input type="checkbox"/> SD	-----None-----	SD test View
<input type="checkbox"/> Email	-----None-----	
<input type="checkbox"/> FTP	-----None-----	
<input type="checkbox"/> HTTP	-----None-----	
<input type="checkbox"/> NAS	-----None-----	<input type="checkbox"/> Create folders by date time and hour automatically View

- **SD Test:** Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, format it before use. Refer to page 79 for detailed information.
- **View:** Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button for an SD card, a Local storage page will prompt so that you can manage the recorded files on SD card. For more information about **Local storage**, refer to page 92. If you click the View button for a Network storage, a file directory window will prompt for you to view recorded data on Network storage. For detailed illustration, refer to the next page.
- **Create folders by date, time and hour automatically:** If you select this item, the system will automatically create folders by the date when video footages are stored onto the networked storage.

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

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	20190120	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	20190121	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	20190122	

The format is: YYYYMMDD
Click to open the directory

Click to delete all recorded data

Click to delete selected items

Click [20190120](#) to open the directory:

The format is: HH (24r)

Click to open the file list for that hour

< [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) >

	file name	size	date	time
<input type="checkbox"/>	Recording1 58.mp4	2526004	2019/01/20	07:58:28
<input type="checkbox"/>	Recording1 59.mp4	2563536	2019/01/20	07:59:28

Delete Delete all Back

Click to delete selected items

Click to go back to the previous level of the directory

Click to delete all recorded data

< [07](#) [08](#) [09](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) >

	file name	size	date	time
<input type="checkbox"/>	Recording1 58.mp4	2526004	2019/01/20	07:58:28
<input type="checkbox"/>	Recording1 59.mp4	2563536	2019/01/20	07:59:28

Delete Delete all Back

The format is: File name prefix + Minute (mm)

You can set up the file name prefix on Add media page. Refer to next page for detailed information.

Add media

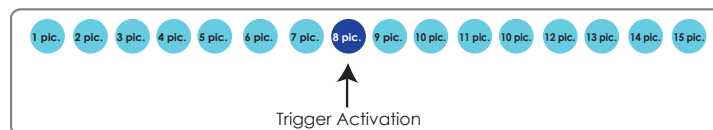
Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: **Snapshot**, **Video Clip** and **System log**. Select the item to display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

Media type - Snapshot

Select to send snapshots when a trigger is activated.

- **Media name:** Enter a name for the media setting.
- **Source:** Select to take snapshots from any of the video streams.
- **Send pre-event images:** The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.
- **Send post-event images:** Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

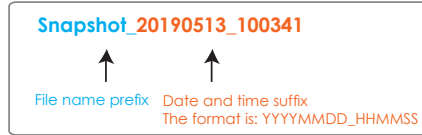
For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images can be generated after a trigger is activated.



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

- Add date and time suffix to the file name. Select this option to add a date/time suffix to the file name.

For example:



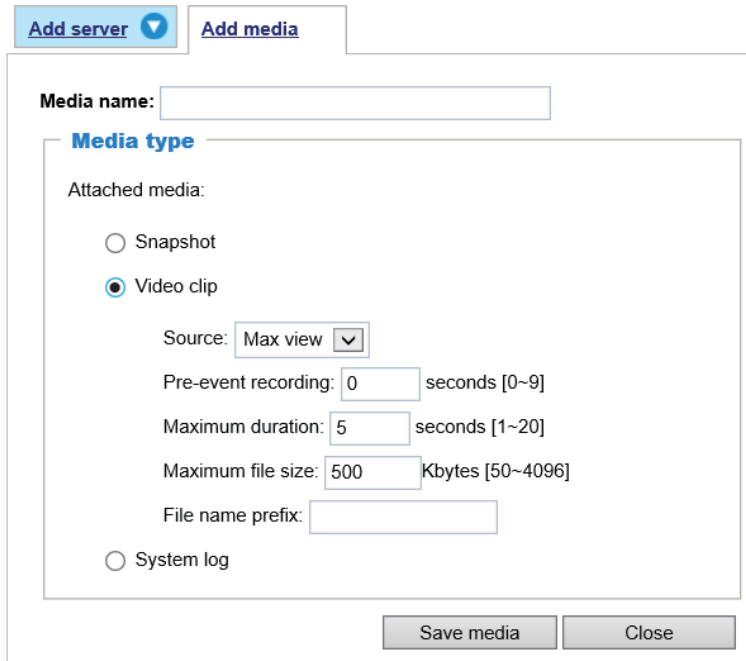
Click **Save media** to enable the settings.

Note that after you set up the first media server, a new column for media server will automatically display on the Media list. If you wish to add more media options, click **Add media**.

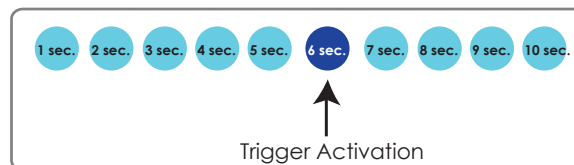
Media type - Video clip

Select to send video clips when a trigger is activated.

- **Media name:** Enter a name for the media setting.
- **Source:** Select a video stream as the source of video clip.
- **Pre-event recording:** The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

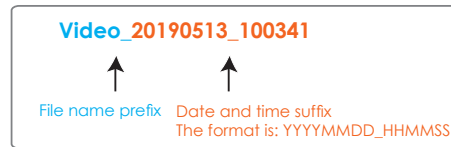


- **Maximum duration:** Specify the maximum recording duration in seconds. The duration can be up to 10 seconds. For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



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

For example:



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

Media type - System log

Select to send a system log when a trigger is activated.

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

Action

Backup media if the network is disconnected

Server	Media	Extra parameter
<input type="checkbox"/> SD	----None----	SD test View
<input type="checkbox"/> mail	----None----	

mail dropdown menu options: None, email, log, snapshot

Save event Close

In the Event settings column, the Servers and Medias you configured will be listed. Make sure the Event -> Status is indicated as **ON**, in order to enable the event triggering action.

When completed, click the **Save event** button to enable the settings and click **Close** to exit the Event Settings page. The new Event / Server settings / Media will appear in the event drop-down list on the Event setting page.

See the example of the Event setting page below:

Event

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
event1	ON	V	V	V	V	V	V	V	00:00~24:00	seq	<input type="button" value="Delete"/>

[Help](#)

Server settings

Name	Type	Address/Location	
HTTP	http	http://192.168.5.10	<input type="button" value="Delete"/>

Media

Available memory space: 13000KB

Name	Type	
Snapshot	snapshot	<input type="button" value="Delete"/>
Video clip	videoclip	<input type="button" value="Delete"/>
System log	systemlog	<input type="button" value="Delete"/>

Customized script

Name	Date	Time
------	------	------

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

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

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that you can only delete a server setting when it is not applied in an existing event setting.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that you can only delete a media setting when it is not applied in an existing event setting.

Events > General

General settings that affect object detection can be adjusted on this page.

The screenshot shows the LINEAR web interface for 'Events > General' settings. The interface includes a sidebar with navigation options: System, Camera, Network, Security, Events, Recording, and Storage. The main content area is divided into sections: 'Sensitivity' with a slider set to 'Default', 'Objects' size calibration' with a video feed and a red bounding box around an object, and a table for object size parameters. The 'Draw Object Size' section has radio buttons for 'Minimum' (selected) and 'Maximum'. The 'Ignore Area' section has a toggle switch set to 'OFF'. The 'Camera View' and 'Scene Type' sections are partially visible at the bottom.

Width Min	Height Min	Width Max	Height Max
30	70	100	100

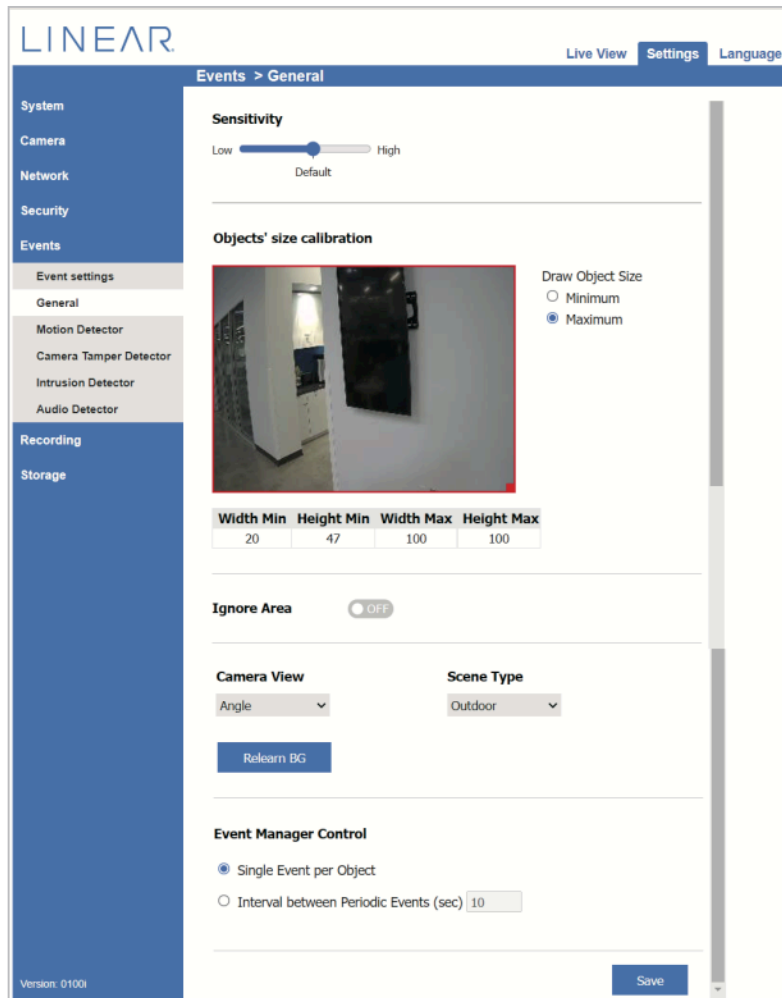
The following parameters are available for Engine setting (tuning) from web-based User Interface within the **Events/General** tab.

- A. **Sensitivity:** The higher the sensitivity threshold value the more motion / movements will be detected.
- B. **Object size calibration:** In order to avoid merging of several objects into one or splitting of an object into multiple bounding boxes, user should set minimal and maximal object size appropriately.

To set minimal / maximal object size, user should do the following:

1. Select "**Draw Object Size -> Minimum or Maximum**" and modify the red rectangle until it fits the smallest (the farthest) object in the scene. Note, that the rectangle size should be a bit smaller than the object. Then, select the "Maximal" radio button and modify the red rectangle to be a bit bigger than the largest object in the scene (the closest object to the camera).

Numbers in the table refer to object width / height as a percentage of the frame width / height respectively.



- C. **Ignore area:** In case user does not want to track all regions of the image, (i.e., if there are any moving objects or reflections), unwanted regions of the image can be masked out, so that they would not be tracked.
- D. **Camera view:** Camera positioning angle is very critical for getting good data for video analytics. Care should be taken to avoid the following: a) object size being too large, as such an object may occupy a large part of the scene, and b) occlusions.

Typically, cameras can be installed with one of the three views:

1. *Overhead or Top-Down* view (Vertical ceiling mount),
2. *Perspective or Angled* view (Wall or Corner mount looking down),
3. *Horizontal or Side View* (Horizontal wall mount at lower height).

The Top-Down view is generally good for counting, detecting direction of movement, etc.

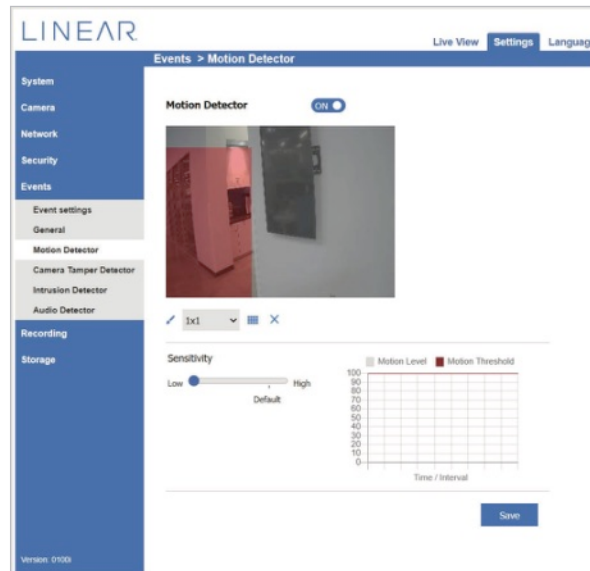
The second option (at angle looking down) is good for detecting intrusions.

The third option (side view) should only be used for face detection. It is not recommended for other analytics since objects can be hidden from view due to occlusions.

- D. **Scene Type:** although the IV Engine is designed to be used for both indoor and outdoor scenes, we recommend that the place of installation (indoor/outdoor).
- E. **Event Manager Control:** regulates frequency of events. User can choose between two options: getting Single event per object or defining an Interval between periodic events.

Events > Motion Detector

The following page contains Motion Detection settings.



- **Enable:** switch to enable *Motion Detection*.
- **Sensitivity:** regulates *Motion Detection* sensitivity (a trade-off between true detections and false alarms).
- **Brush size:** User may set the brush size to 1x1 or 3X3 depending on user needs.

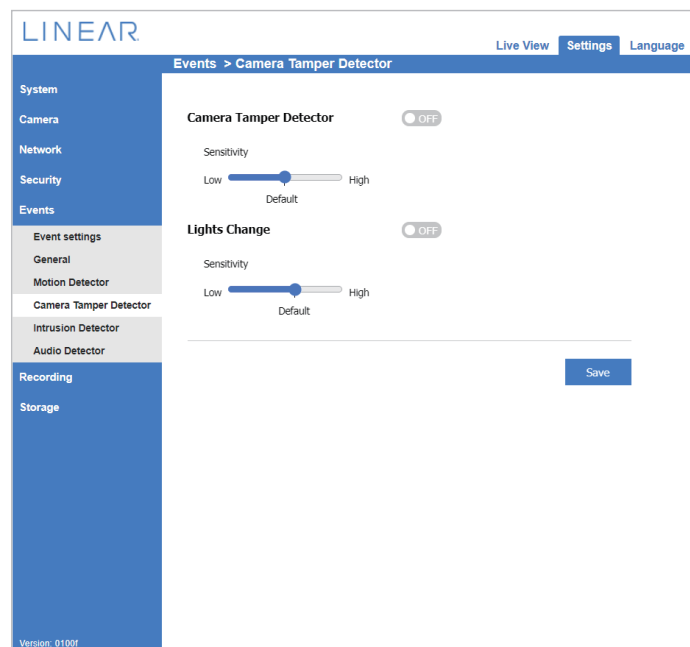
To select an area for *Motion Detector*, click and drag on the image to paint the scene. The area highlighted in red will be the intrusion area. Click and drag on the red area to de-select that section of the grid.

Events > Camera Tamper Detector

Camera Tamper detector notifies whether a camera has been tampered. Camera blocking, de-focusing, power/video loss and drastic changes in camera angle will trigger the CameraTamper event.

Light Change feature sends notifications in case if any light changes are detected.

User may set the sensitivity parameters for both detectors to regulate the trade-off between false alarms and true detections.

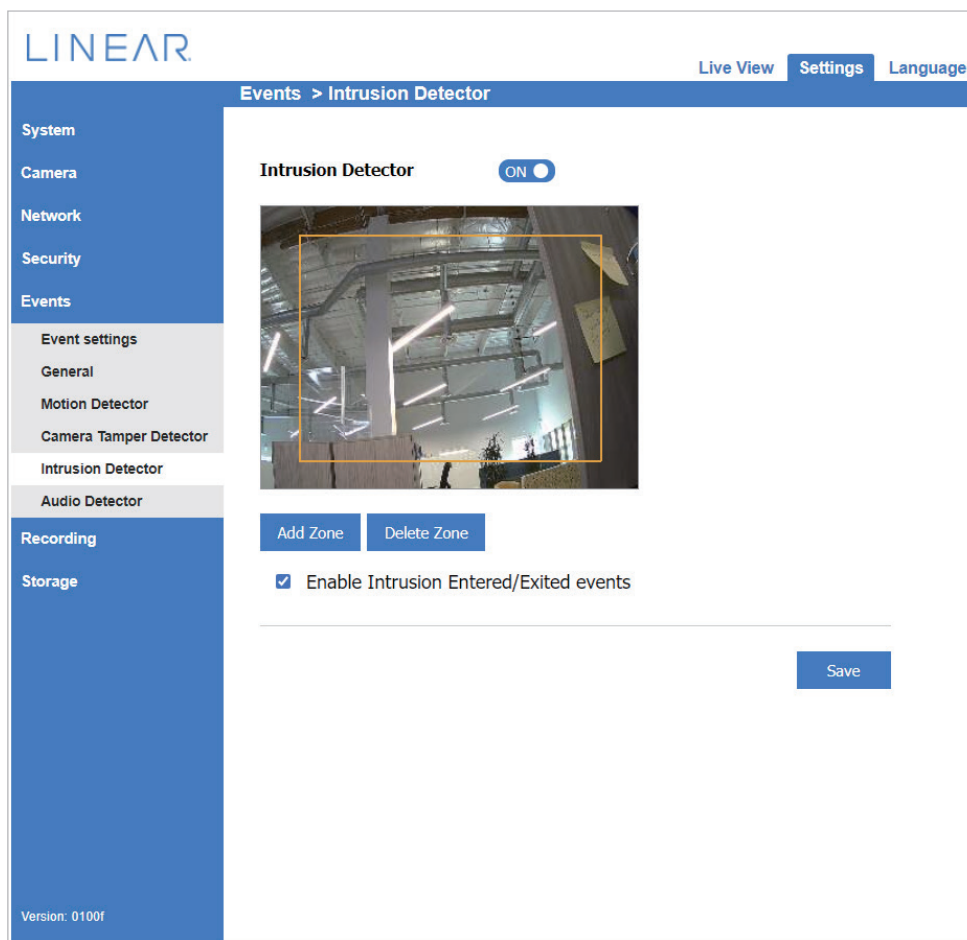


Events > Intrusion Detector

The following page contains Intrusion Detector settings.

- **Enable:** switch to enable the Intrusion detection.
- **Add/Delete Zone:** User can add, delete and modify intrusion zones.
- **Enable Intrusion Entered/Exited events:** user can enable this property to start getting IntrusionEntered / IntrusionExited events.

To modify an area for **Intrusion Detector**, click and drag an angle of the figure. The area within the figure will be the intrusion area.



Recording > Recording settings

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

Recording Settings

Insert your SD card and click here to test

Recording settings

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

[SD test](#)

Note: Before setup recording, you may setup network storage via [NAS server](#) page



NOTE:

- ▶ Remember to format your SD card via the camera's web console (in the Local storage. SD card management page) when using it for the first time.

Recording Settings

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

Recording name:

Enable this recording

With adaptive recording ([Help](#))

Priority:

Source:

1. Trigger

Trigger

Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

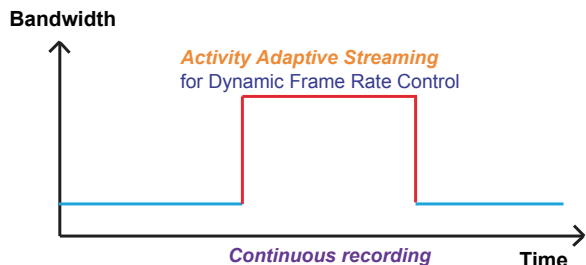
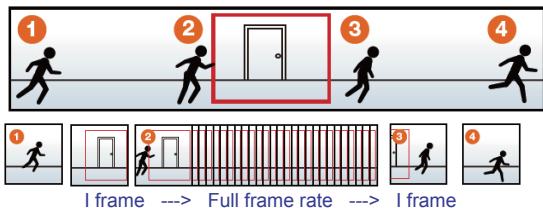
Network fail

2. Destination

Note: To enable recording notification please configure [Events](#) first

- **Recording name:** Enter a name for the recording setting.
- **Enable this recording:** Select this option to enable video recording.
- **With adaptive recording:** Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've configured on the Video quality page. Refer to page 56 for more information.

If you enable adaptive recording on a camera, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidths and storage space.



NOTE:

- ▶ To enable adaptive recording, make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.
- ▶ When there is no alarm trigger:
 - JPEG mode: record 1 frame per second.
 - H.264 mode: record the I frame only.
- ▶ When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.

The alarm trigger includes: motion detection and DI detection. Refer to **Event Settings** on page 70.

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

NOTE:

- ▶ To enable recording notification configure **Event settings** first. Refer to page 70.

Follow the steps below to set up the recording.

1. Trigger

Select a trigger source.

Trigger

Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From to [hh:mm]

Network fail

- **Schedule:** The server will start to record files on the local storage or network storage (NAS).
- **Network fail:** In the event of a network failure, the camera will start to record files on the local storage (SD card).

2. Destination

You can select the SD card or network storage (NAS) for the recorded video files. If you have not configured a NAS server, see details in the following:

NAS management

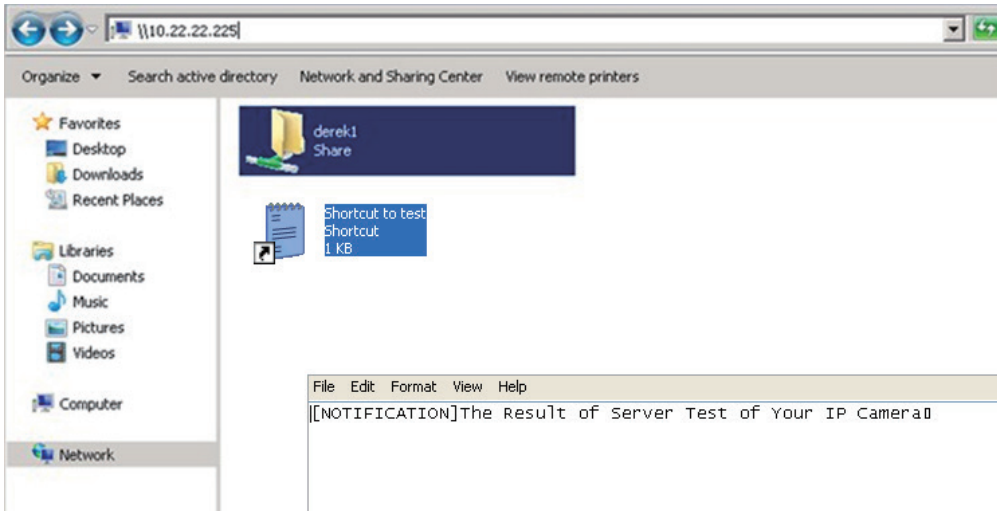
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for your server.

For example:

2. Click **Test** to check the setting. The result will be shown in a pop-up window.

If successful, you will receive a test.txt file on the network storage server.



- 3. Enter a server name.
- 4. Click **Save** to complete the settings, and click **Close** to exit the page.

- **Capacity:** You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording. The reserved space is a small amount of space used only for the transaction stage when the capacity is about to be used up or recycled.
- **Enable cyclic recording:** If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MegaBytes.
- **Recording file management:** You can manually assign the Maximum duration and the Maximum file size for each recording footage. You may need to stitch individual files together under some circumstances. You may also designate a file name prefix by filling in the responsive text field.
- **File name prefix:** Enter the text that will be appended to the front of the file name.

If you want to enable recording notification, click **Event** to configure event triggering settings.

Refer to **Event > Event settings** on page 70 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.

Recording settings												
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
recording	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	NAS	<input type="button" value="Delete"/>
<input type="button" value="Add"/>		SD test										

- Click [recording \(Name\)](#): Opens the Recording Settings page to modify.
- Click [ON \(Status\)](#): The Status will become [OFF](#) and stop recording.
- Click [NAS \(Destination\)](#): Opens the file list of recordings as shown below. For more information about folder naming rules, refer to page 77 for details.

<input type="checkbox"/>	<input type="checkbox"/>	20190210
<input type="checkbox"/>	<input type="checkbox"/>	20190211
<input type="checkbox"/>	<input type="checkbox"/>	20190212
<input type="button" value="Delete"/>		<input type="button" value="Delete all"/>

Local storage > SD card management



NOTE:

- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera file system takes up several megabytes of memory space. The storage space cannot be used for recording.
- Using an SD card that already contains data recorded by another device should not be used in this camera.
- Do not modify or change the folder names in the SD card. That may result in camera malfunctions.

This section explains how to manage the local storage on the Network Camera, view SD card status and implement SD card control.

Storage > Storage Management

This column shows the status and reserved space of your SD card. Remember to format the SD card when using for the first time.

SD card status

SD card status: Detached — **no SD card**

File system: none

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

SD card status

SD card status: Detached

File system: none

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

SD card format

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

SD card format

Ext4

FAT32

Format

SD card control

SD card control

Minimum reserved storage space: %

Enable cyclic storage

Enable automatic disk cleanup

- **Enable cyclic storage:** Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- **Enable automatic disk cleanup:** Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

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

- **File attributes:** Select one or more items as your search criteria.

Search

Device target

All devices
 SD
 NAS

Trigger type

Backup
 System boot
 Motion
 Network fail
 Recording notify
 Periodically
 SD card life expectancy
 Camera Tamper Detector
 Detector
 Manual triggers
 Audio Detector

Media type

Video clip
 Snapshot
 Text

Time

Search for last minute(s) hours days weeks


From: :

to: :

- **Trigger time:** Manually enter the time range you want to search for contents created at a specific point in time.

Click **Search**, and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger type, Media type, Trigger type and Locked. Click  to sort the search results in either direction.

Numbers of entries displayed on one page

Search results

<input type="checkbox"/>	<input type="checkbox"/>	Name	Trigger type	Starting time	Ending time
<input type="checkbox"/>	<input type="checkbox"/>	to SD	Periodically	Today at 3:45 PM	Today at 3:58 PM
<input type="checkbox"/>	<input type="checkbox"/>	to SD	Periodically	Today at 3:58 PM	--
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:45 PM	Today at 3:45 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:49 PM	Today at 3:49 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:49 PM	Today at 3:49 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:50 PM	Today at 3:50 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:50 PM	Today at 3:50 PM

Click to open a live view

/ 3

- **Play:** Click on a search result which will highlight the selected item. A Play window will appear on top for immediate review of the selected file.

For example:



- **Download:** Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.
- **JPEGs to AVI:** This functions only applies to “JPEG” format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.
- **Lock/Unlock:** Select the checkbox in front of a desired search result, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections.

For example:

Search results

<input type="checkbox"/>	<input type="checkbox"/>	Name	Trigger type	Starting time	Ending time
<input type="checkbox"/>	<input type="checkbox"/>	to SD	Periodically	Today at 3:45 PM	Today at 3:58 PM
<input type="checkbox"/>	<input type="checkbox"/>	to SD	Periodically	Today at 3:58 PM	--
<input checked="" type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:45 PM	Today at 3:45 PM
<input checked="" type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:49 PM	Today at 3:49 PM
<input checked="" type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:49 PM	Today at 3:49 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:50 PM	Today at 3:50 PM
<input type="checkbox"/>	<input type="checkbox"/>	test	Motion	Today at 3:50 PM	Today at 3:50 PM

10 [dropdown] [Navigation icons] 1 / 3 [Navigation icons]

[Download] [Lock/Unlock] [JPEGs to AVI] [Remove]

Click to switch pages

- **Remove:** Select the desired search results, then click this button to delete the files.

Electromagnetic Compatibility (EMC)

FCC Statement

This device complies with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Liability

Nortek Security & Control LLC cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Nortek Security & Control LLC makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.



USA & Canada Toll Free: 800-421-1587 or call 760-438-7000 | www.linear-solutions.com