

Operations User Manual

www.beward.eu

IP CAMERA N35110



IR LEDs built in
IP66 rated housing
Megapixel CMOS sensor

Table of contents

CHAPTER 1. SAFETY INSTRUCTIONS	3
CHAPTER 2. OVERVIEW	5
2.1. OVERVIEW OF BEWARD N35110	5
2.2. N35110 FEATURES	6
2.3. THE N35110 SPECIFICATIONS	6
2.4. PACKAGE CONTENTS	7
2.5. DEFAULT SETTINGS	7
2.6. PURPOSE OF USER MANUAL	8
2.7. MINIMUM SYSTEM REQUIREMENTS	8
CHAPTER 3. USING THIRD PARTY CLIENTS.....	9
3.1. PLAYING 3GP VIDEO	9
3.2. PLAYING STREAMING VIDEO IN 2.5G NETWORKS OVER WAP	9
3.3. PLAYING STREAMING VIDEO IN 2.5G NETWORKS VIA BROWSER	9
3.4. PLAYING STREAMING VIDEO VIA THIRD PARTY SOFTWARE	9
3.4.1. <i>Playing MPEG-4 Video</i>	10
3.4.2. <i>Playing MJPEG Video</i>	10
3.4.3. <i>Getting a JPEG Image</i>	10
CHAPTER 4. MANAGING THE IP CAMERA VIA INTERNET EXPLORER	11
4.1. INSTALLING ACTIVEX CONTROLS	12
CHAPTER 5. MAIN MENU	16
5.1. [LIVE VIEW] PANE	16
5.1.1. <i>[Snapshot] Button</i>	17
5.1.2. <i>[Fullscreen] Button</i>	17
5.1.3. <i>[Open Digital Zoom] Button</i>	17
5.1.4. <i>Video Control Buttons</i>	18
5.1.5. <i>Audio Control Buttons</i>	18
5.2. SETTING MENU	19
5.3. CLIENT SETTING	20
5.3.1. <i>Mode</i>	21
5.3.2. <i>View Size</i>	21
5.3.3. <i>Protocol</i>	21
5.3.4. <i>Video Buffer</i>	22
5.4. IMAGE SETUP	22
5.4.1. <i>Brightness</i>	23
5.4.2. <i>Contrast</i>	23
5.4.3. <i>Saturation</i>	23
5.4.4. <i>Sharpness</i>	23
5.4.5. <i>Exposure</i>	23
5.4.6. <i>Default</i>	23
CHAPTER 6. SETTING: BASIC MENU	24
6.1. SYSTEM	24
6.1.1. <i>Information</i>	24
6.1.2. <i>Date/Time</i>	25
6.1.3. <i>Initialize</i>	27
6.1.4. <i>Language</i>	28
6.2. CAMERA	29
6.2.1. <i>General</i>	29
6.2.2. <i>H.264</i>	32
6.2.3. <i>MPEG-4</i>	34
6.2.4. <i>MJPEG</i>	36
6.2.5. <i>3GPP</i>	38
6.2.6. <i>Advanced</i>	39
6.2.7. <i>Playback</i>	40
6.3. NETWORK	42
6.3.1. <i>Information</i>	43
6.3.2. <i>PPPoE (Point-to-Point Protocol over Ethernet)</i>	45
6.3.3. <i>DDNS (Dynamic DNS)</i>	46
6.3.4. <i>UPnP (Universal Plug and Play)</i>	47

6.3.5. Bonjour	48
6.3.6. IP notification	49
6.4. SECURITY	51
6.4.1. Account	51
6.4.2. HTTPS.....	53
6.4.3. IP Filter	54
CHAPTER 7. SETTING: ADVANCED.....	56
7.1. FTP CLIENT.....	56
7.1.1. General.....	57
7.1.2. Alarm Sending.....	58
7.1.3. Periodical Sending	60
7.2. SMTP	62
7.2.1. General.....	63
7.2.2. Alarm Sending.....	64
7.2.3. Periodical Sending	67
7.3. NETWORK STORAGE	69
7.3.1. General.....	70
7.3.2. Alarm Sending.....	71
7.3.3. Periodical Recording	74
7.4. HTTP EVENT.....	76
7.4.1. General.....	76
7.4.2. Alarm Sending.....	77
7.5. ALARM OUTPUT	79
7.6. SCHEDULE	81
7.7. ALARM INPUT	82
7.8. ALARM BUFFER.....	83
7.9. MOTION DETECTION.....	84
7.10 AUDIO DETECTION	86
7.11. SYSTEM LOG	87
APPENDIX.....	88
APPENDIX A. BITRATE VALUES.....	88
APPENDIX B. REQUIRED DISK SPACE	92
APPENDIX C. REQUESTS FOR IMAGES FROM IP CAMERA.....	95
APPENDIX D. PORT VALUES.....	97
APPENDIX E. FACTORY DEFAULTS.....	98
APPENDIX F. ACCESSING THE CAMERA OVER THE INTERNET USING DYNDNS SERVICE.....	99
F.1. Overview of Internet Access to Cameras Using DynDNS service	99
F.2. Creating an Account at DynDNS Service	99
F.3. Creating a Domain Name at DynDNS.....	103
F.4. Setting up the Equipment to Work with DynDNS	107
APPENDIX G. GLOSSARY	111

Chapter 1. Safety Instructions

Before using this product

This camera complies with all safety rules. However, improper use of any electric device can be a cause of fire and bring to property damage. Before you start using this camera, please study this user manual carefully.

IMPORTANT!

Use accessories recommended by the manufacturer only. Use of the improper accessories may cause camera's breakdown.

Follow the operating instructions

- Do not use and store this camera in severe environment:
- avoid extremely low or high ambient temperatures (the camera's operating temperature is -40°C to $+50^{\circ}\text{C}$)
- avoid exposure to direct sunlight and do not locate the camera near any heat sources
- avoid exposure to high humidity
- do not locate the camera near any electrical appliances which can be electromagnetic transmitters
- avoid exposure to high vibration

IMPORTANT!

In case of malfunction of the product, please contact your local dealer for technical assistance.

In case of:

- detection of a strange smell or smoke
- penetration of any liquid or foreign objects into the camera
- the camera has been dropped or damaged

Do the following:

- unplug the power cord and disconnect all other cords from the camera
- contact our Service Center. You can find contact information on our website: <http://www.beward.eu/>.

Transportation

Transport the camera carefully, using the original box and protective packing.

Ventilation

To prevent overheating of the device, keep free air circulation in the area where the camera is located.

Cleaning

Use a soft, dry cloth for cleaning camera's external surfaces. It is acceptable to use some detergent for removing persistent dirt, but not the volatile cleaners such as the alcohol-containing solvents, benzene and so on, because of the risk to damage the camera's housing.

Chapter 2. Overview

2.1. Overview of BEWARD N35110

BEWARD N35110 is designed for both indoor and outdoor usage. The camera's housing surely protects it against harsh weather conditions and is IP66 rated, so that the camera can be used in any environmental conditions.

The N35110 features a megapixel CMOS sensor and a mechanical IR cut filter, which ensures clear pictures under low-light conditions. Besides, the camera has built-in IR LEDs, which provide twenty-four-hour surveillance.



Pic. 2.1

BEWARD N35110 comes with everything you need to quickly set up your camera and start using it. The user manuals and the surveillance software in English are included. The N35110 is easy to use and set up.

2.2. N35110 Features

- IP66 rated housing
- Motorized IR cut filter
- 15 meter IR distance
- Optimal solution concerning price/quality
- Recording to network attached storage (NAS)
- Professional surveillance software included (16 channels)
- Simultaneous streaming: H.264/MPEG-4/MJPEG/3GPP
- High-resolution sensor (up to 1280x1024 resolution)
- Two-way audio, support for connecting an external microphone
- Viewing camera images on a mobile phone (including iPhone)
- Built-in multi-zone motion detection
- Support for audio detection (when an external microphone is connected)
- Sending of images and videos via e-mail and to FTP
- PoE IEEE 802.3af Class 0 support

2.3. The N35110 Specifications

- Compact size (80 x Ø102 mm (with sunshield: 116/145 mm), weight is 635 g)
- Sensor: 1/4" 1.3 megapixel progressive scan CMOS
- Built-in lens: M12, f4.0 mm, F1.5 (angle of view: 65° diagonal, 48° horizontal, 40° vertical)
- Motorized IR cut filter
- Sensitivity: 0.5 lux (0 lux if IR LED is on)
- Shutter time: 1 ~ 1/17780 sec
- Illumination: IR LED (850 nm), 21 pcs, 8 mm diameter, up to 15 meters
- S/N ratio: 44 dB
- Resolution: 1280x1024, 1280x720, 640x480, 320x240
- Simultaneous streaming: Motion JPEG, H.264, MPEG-4 part 2 (ISO/IEC 14496-2) Profile: SP, 3GPP
- Frame rate: H.264/MPEG-4/MJPEG: up to 30 frames per second at 640x480, 320x240, up to 15 frames per second at 1280x1024, 1280x720. 3GPP: up to 10 frames per second at 640x480, 320x240
- Digital zoom: 10x

- Two-way audio with support for switching between G.711 μ law, a-law, and AMR compression formats, 3.5 mm jack, output for connection of an external microphone and speakers
- Built-in multi-zone motion detection and audio detection, sensitivity and threshold control
- Up to 5 simultaneous connections
- Continuous, scheduled and motion detection triggered sending of images and video via e-mail and to FTP
- Power: 12 V DC, 0.5 A, 12 W maximum, PoE IEEE 802.3af Class 0
- Operating temperature: -40 to +50°C
- Supported protocols: Bonjour, TCP/IP, DHCP, PPPoE, ARP, ICMP, FTP, SMTP, DDNS, NTP, UPnP, RTSP, RTP, RTCP, HTTP, TCP, UDP, 3GPP/ISMA RTSP
- Support for ONVIF v1.02

2.4. Package Contents

- IP camera N35110 (lens M12, 4.0 mm, F1.5 pre-installed)
- Sunshield
- RJ-45 adapter
- Quick installation guide
- CD with user manuals and software
- Bracket
- Power supply 12 V 1 A DC

2.5. Default Settings

The main default settings are:

- IP address: **192.168.0.99**
- Subnet mask: **255.255.255.0**
- Gateway: **192.168.0.1**
- Username: **admin**
- Password: **admin**
- HTTP port: **80**
- RTSP port: **554**

2.6. Purpose of User Manual

BEWARD N35110 is an outdoor camera that features a web server, a network interface and can be connected to the Ethernet directly.

The camera images can be viewed via a web browser or the free Beward software that comes with this camera. Besides, the live images can be viewed over mobile networks, via stream players, over the Internet remotely, etc.

This User manual provides information on the camera's web interface and how to configure it without using software but with the use of the built-in web server only.

Despite some BEWARD IPS options are not available (see BEWARD IPS Operations User Manual) when you are managing the camera via a web browser or a mobile device, it allows viewing camera images from any location in the world, though. Moreover, you can view it on any device such as a laptop, a cell phone, a PDA, etc. This User manual provides detailed information on managing the N35110 without using any software.

2.7. Minimum System Requirements

Verify that your computer meets the system requirements listed on the camera packaging. If your computer does not meet these requirements, this IP camera may not work correctly.

Item	Requirements
CPU	2.8 GHz Pentium 4 (or equivalent AMD)
Video Card	256 MB (or equivalent integrated video card)
RAM	1 GB
Operating System	Windows 2000, XP, Vista, Windows 7, Mac OS X Leopard
Web Browser	Internet Explorer 8.0 or later

NOTE:

1. If you cannot play records, please install Xvid codec or VLC freeware player (<http://www.videolan.org/vlc/>).
2. For correct program operation, you may need to update some Windows components (.Net Framework, Windows Media Player, Enhance ActiveX Security).

Chapter 3. Using Third Party Clients

The N35110 supports RTSP/RTP streaming.

RTSP (Real Time Transfer Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The protocol is used for establishing and controlling media sessions between end points. Clients of media servers issue VCR-like commands, such as play and pause, to facilitate real-time control of playback of media files from the server (see [paragraph 6.2.1](#) for details).

NOTE:

You can play RTSP stream with any supported video player (Real Player, VLC, Quick Time, etc).

3.1. Playing 3GP Video

You can view camera images on a computer as well as a mobile device such as cell phones, smartphones, PDA, etc (iPhone supported as well). You can configure the stream to be viewed on a mobile device at **SETTING – Basic – Camera – 3GPP**.

If your phone does not support streaming video, type «**rtsp://<IP>:<PORT>/video.3gp**» in the address bar of the streaming player installed in your phone to view the 3GP video. <IP> is the public IP address of your camera, <PORT> is the RTSP port (default value is 554). Example: **rtsp://89.57.167.76:554/video.3gp**.

3.2. Playing Streaming Video in 2.5G Networks over WAP

If your phone is used on a 2.5G network, type «**http://<IP>/mobile.wml**» in the WAP browser's address bar to the images. <IP> is the public IP address of your camera.

3.3. Playing Streaming Video in 2.5G Networks via Browser

If your phone is used on a 2.5G network, type «**http://<IP>/mobile.htm**» in the browser's address bar to view the images. <IP> is the public IP address of your camera.

3.4. Playing Streaming Video via Third Party Software

If your computer is connected to high-speed Internet or you need to view the streaming video in other formats, you can use real time RTSP players such as VLC, Quick Time, Real Player, etc.

NOTE:

The connection speed to the camera depends on the bandwidth.

3.4.1. Playing MPEG-4 Video

Type `rtsp://<IP>:<PORT>/video.mp4`, <IP> is the IP address of your camera, <PORT> is the RTSP port of your camera (default value is 554). Example: `rtsp://89.57.167.76:554/video.mp4`.

3.4.2. Playing MJPEG Video

Type `rtsp://<IP>:<PORT>/video.mjpg`, <IP> is the IP address of your camera, <PORT> is the HTTP port of your camera (default value is 80). Example: `rtsp://89.57.167.76:80/video.mjpg`.

3.4.3. Getting a JPEG Image

Type `http://<IP>:<PORT>/jpg/image.jpg`, <IP> is the IP address of your camera, <PORT> is the HTTP port of your camera (default value is 80).

Example: `rtsp://89.57.167.76:80/jpg/image.jpg`.

NOTE:

You can get 5-6 images per second maximum.

Chapter 4. Managing the IP Camera via Internet Explorer

Step 1: connect your camera according to the User manual.

Step 2: open Internet Explorer, type the camera's IP address in the address bar. The default IP address is **192.168.0.99**.

NOTE:

There are two ways to assign an IP address to this IP camera:

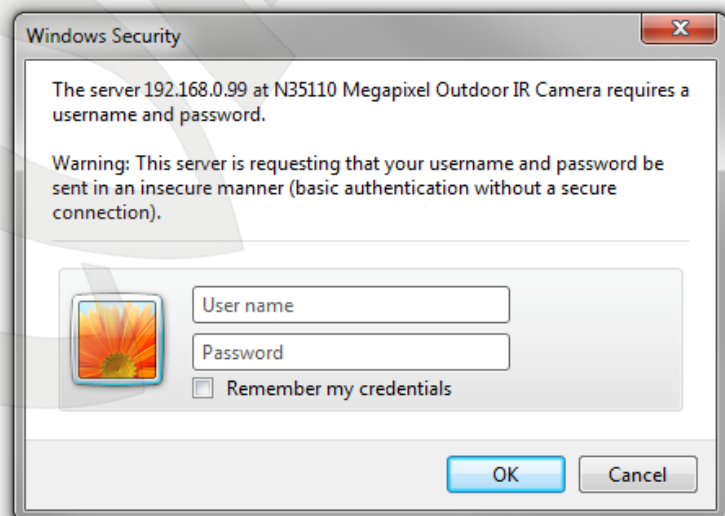
1. An IP address can be obtained automatically from a Dynamic Host Configuration Protocol (DHCP) according to the network parameters.
2. Use a manually specified IP address. See [paragraph 6.3.1](#) for details. Contact your system administrator to avoid IP address conflict.

NOTE:

To view the camera images without showing the control panel, type «<http://<IP>/index2.htm>» in the address bar of the browser. <IP> is the IP address of your camera

Step 3: enter the camera's username and password in the authorization window (*Pic. 4.1*).

The default user name is «**admin**», the default password is «**admin**».



Pic. 4.1

IMPORTANT!

You can change the camera's user name and password at **SETTING – Basic – Security – Account**. If you forgot your user name or password, you can reset your camera to factory settings by holding **[RESET]** button during 10-15 seconds. Hold **[RESET]** button during 5-7 seconds to restart the camera.

By default, Windows prevents ActiveX add-ons from running but some ActiveX add-ons are required to operate this IP camera. Therefore, you need to install the ActiveX add-ons to operate your camera.

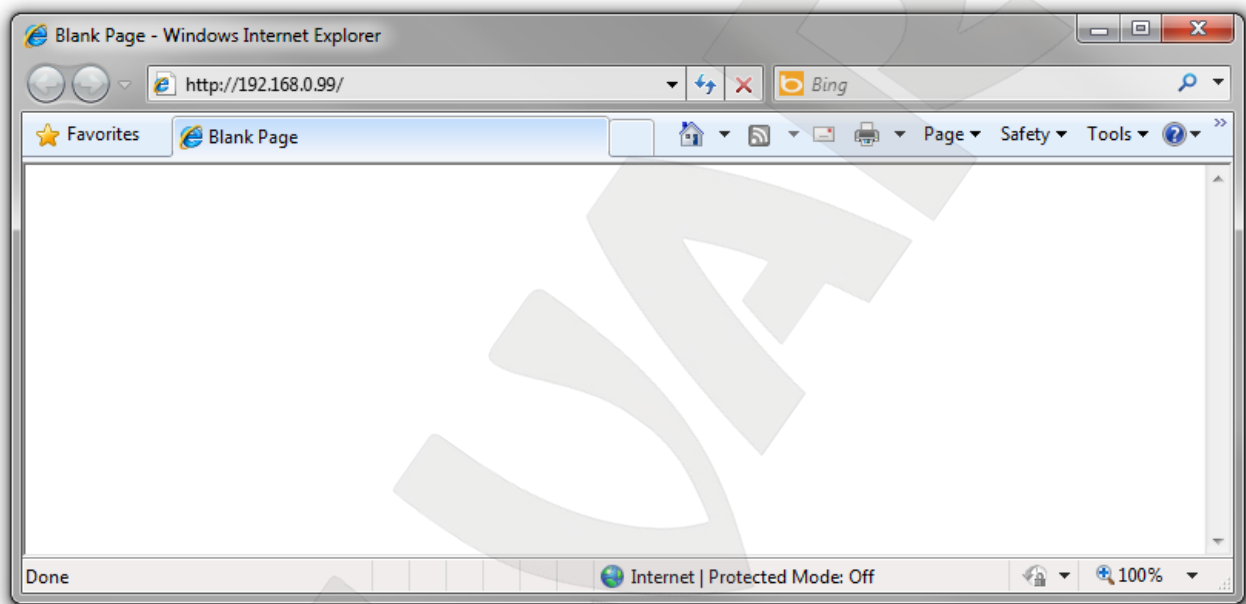
4.1. Installing ActiveX Controls

To view the camera images via Internet Explorer, you need to install the ActiveX controls. To do so, follow these steps:

NOTE:

The installation is shown for Internet Explorer 8.0 and Windows 7.

Step 1: open Internet Explorer, type the IP address of your camera in the address bar (*Pic. 4.2*). Press **Enter** or click the **Go To** button.



Pic. 4.2

IMPORTANT:

The camera's default IP address is **192.168.0.99**. If the camera was assigned an IP address by a DHCP server on the local network, use BEWARD IP Installer to find your camera on the network. If you use multiple IP cameras, you need to change their default IP addresses so that each camera will have a unique IP address.

NOTE:

To connect to the camera, you need to get your computer and your camera to the same subnet.

Step 2: you will see an authorization window where you should enter the camera's username and password (*Pic. 4.3*)

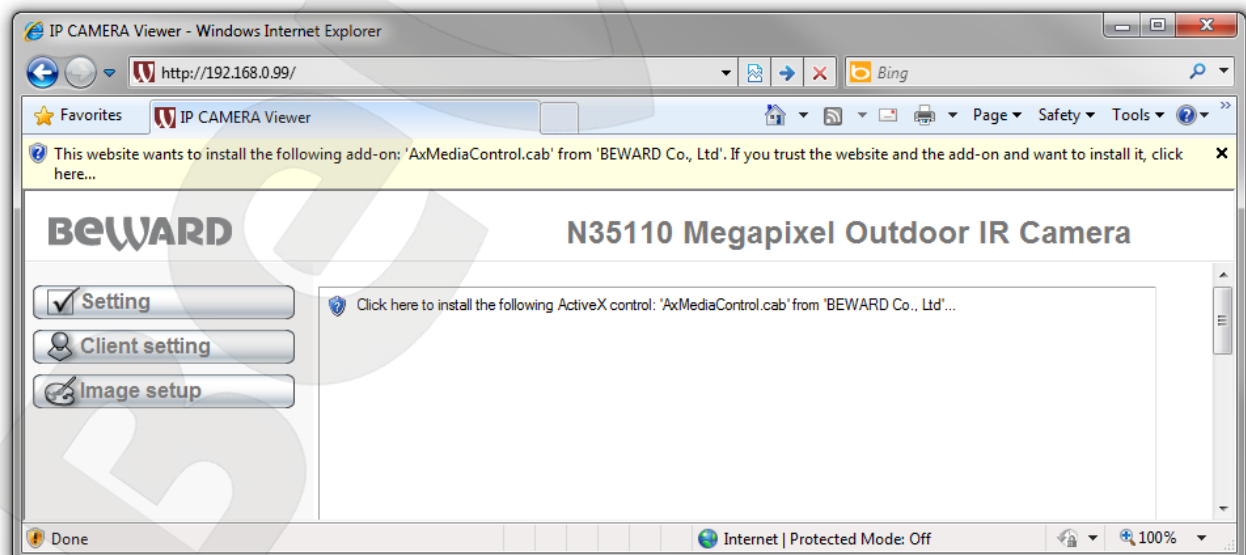


Pic. 4.3

IMPORTANT:

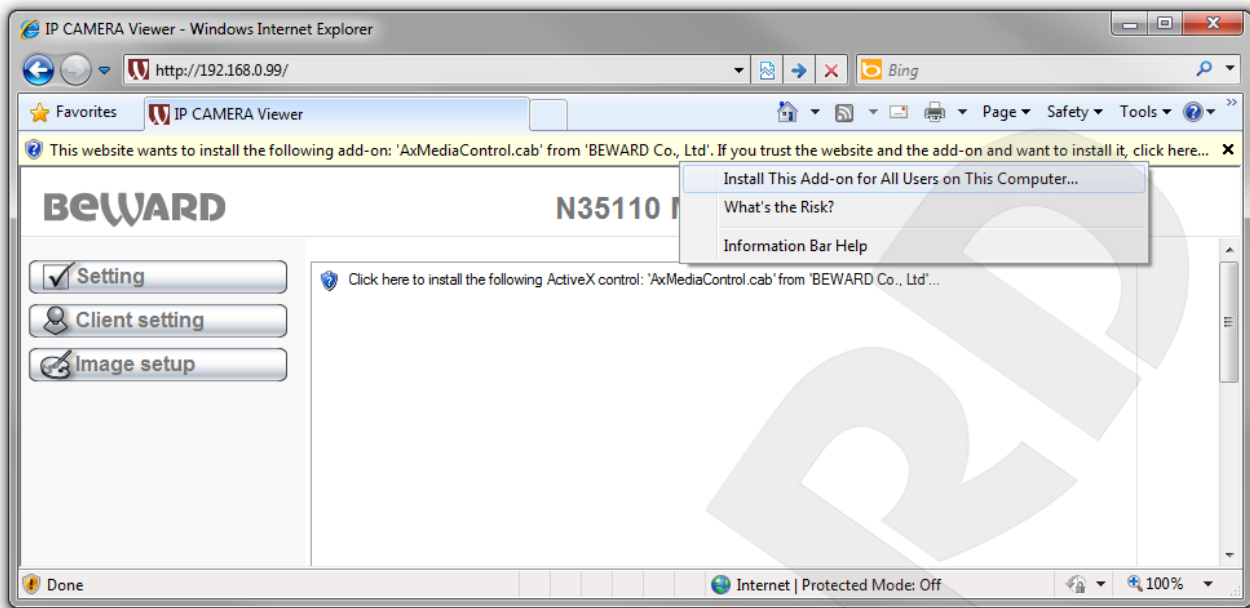
The default user name is **admin**, the default password is **admin**.

Step 3: after successful authorization you will be prompted to install an ActiveX add-on. You will see a system notification under the address bar: **“This website wants to install the following add-on: “AxMediaControl.cab” from “BEWARD Co., Ltd.”. If you trust the website and the add-on and want to install it, click here...”** (Pic. 4.4).



Pic. 4.4

Step 4: click right mouse button on this notification. In the drop-down menu select **“Install This Add-on for All Users on This Computer...”** or click on the area **“Click here to install the following ActiveX control: “AxMediaControl.cab” from “BEWARD Co., Ltd.”...”** (Pic. 4.5).

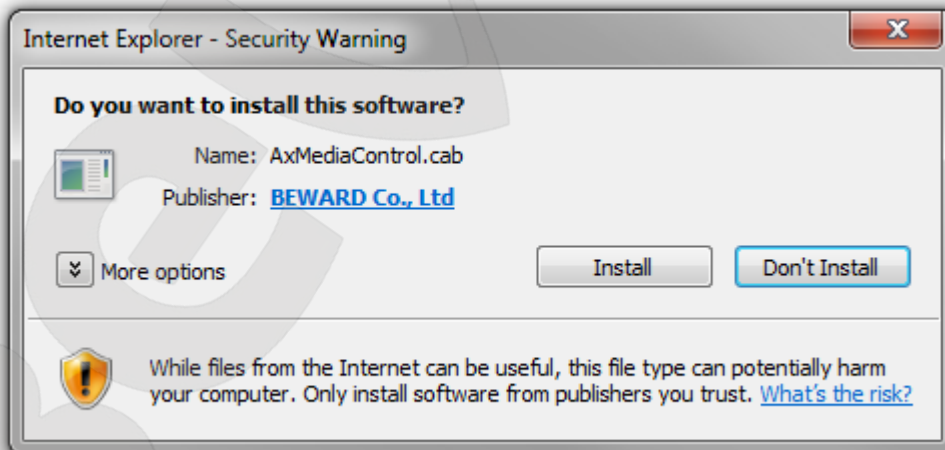


Pic. 4.5

NOTE:

Titles of system menu and notifications may differ from the titles of system menu and notifications that appear in other versions of Windows and Internet Explorer.

Step 5: by default, Internet Explorer prevents ActiveX add-ons from installation, click **[Install]** to continue. (Pic. 4.6)

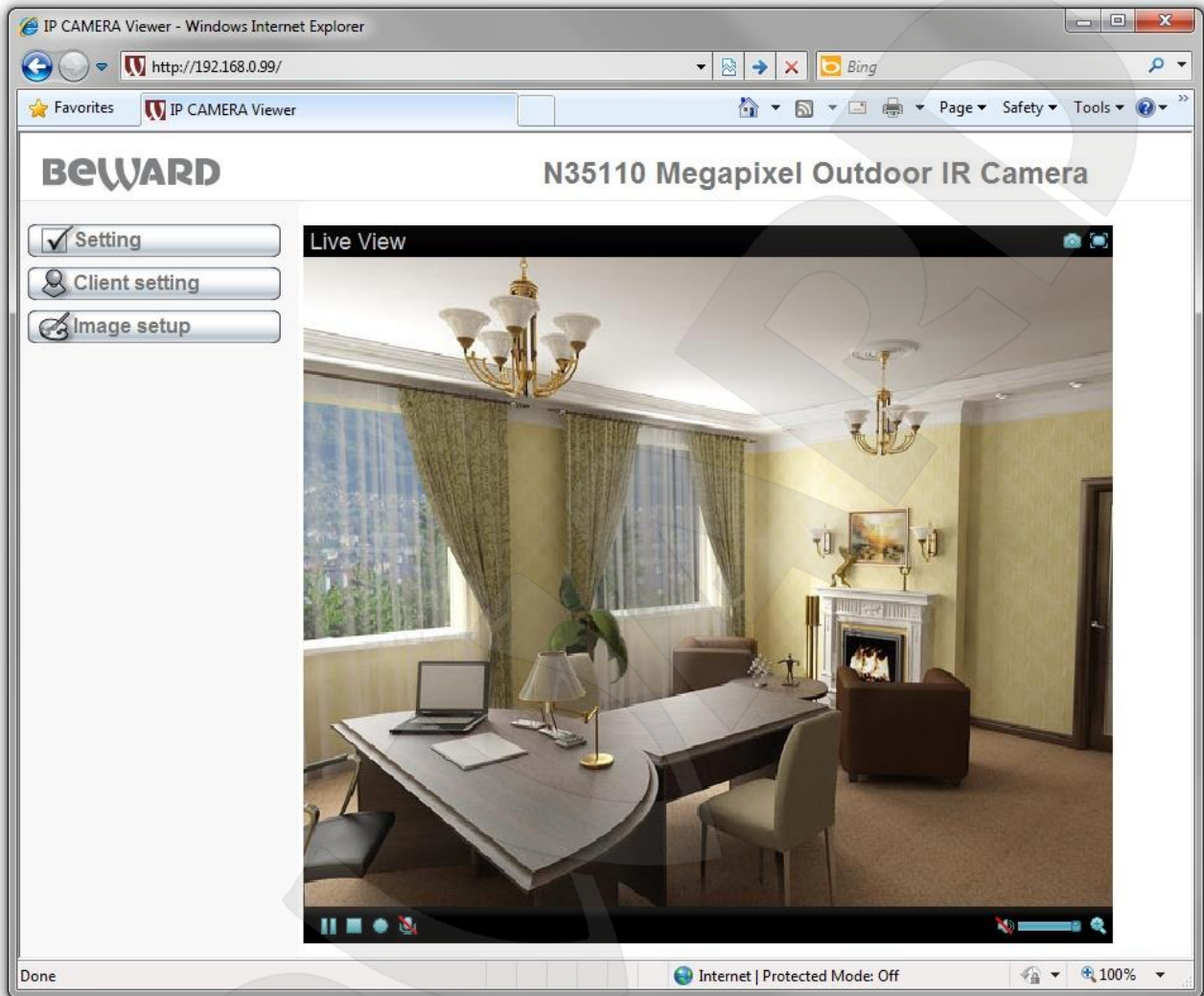


Pic. 4.6

NOTE:

When installing ActiveX controls for Windows 7 with enabled User Account Control (UAC), it prevents them from installation and generates a warning message. Click yes in the appeared window.

Step 6: if everything was done correctly, you should get the camera images via your browser. The settings bar is on the left side, the camera images are on the right side (Pic. 4.7). Detailed information is discussed later in this Manual.



Pic. 4.7

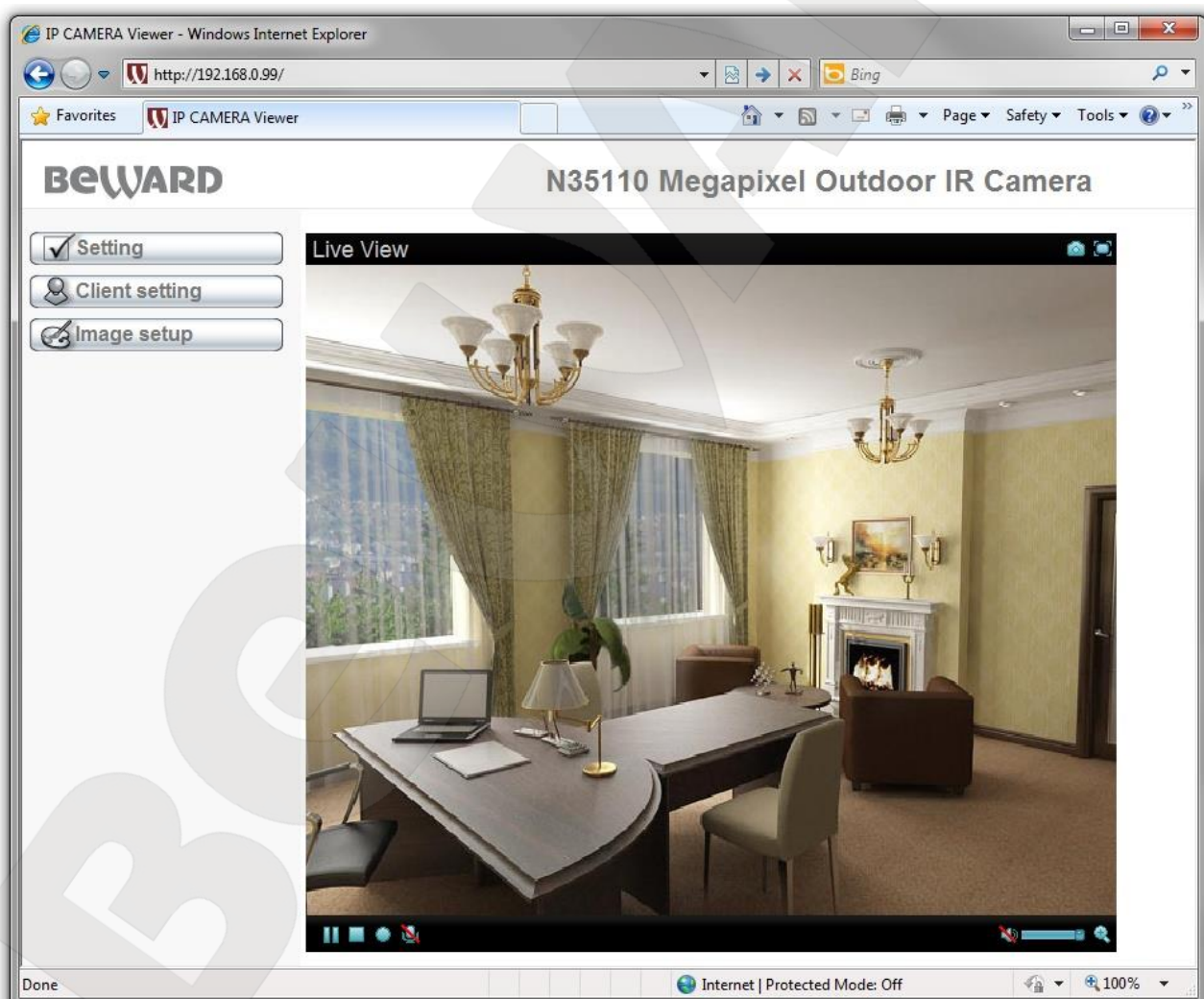
Chapter 5. Main Menu

The main menu consists of two panes. The left pane contains **[Setting]**, **[Client setting]**, and **[Image setup]** menus (Pic. 5.1).

The right pane contains the “**Live view**” window, which displays real-time camera images. Also, this pane contains the following buttons: **[Snapshot]**, **[Fullscreen]**, **[Open digital zoom]**, **[Start record]**, **[Microphone]**, **[Pause]**, **[Play/Stop]**, and **[Volume]** (Pic. 5.1). These functions are discussed later in this Manual.

NOTE:

The example in the picture below is shown for «**MPEG-4**» and «**MJPEG**» image. When viewing a «**JPEG**» image, there are no control buttons. You can only rewind a clip frame-by-frame.




Pic. 5.1

5.1. [Live View] Pane

This pane displays real-time camera images and allows you to manage them.

5.1.1. [Snapshot] Button


This button captures and saves a snapshot image of the current video image from your camera to your computer's hard drive. To do so, click the icon  and specify the path where you want to save the snapshot.

NOTE:





When specifying the path, check the permissions on the folder where you want to save the snapshot. If you do not have the permissions, you cannot save snapshots there.

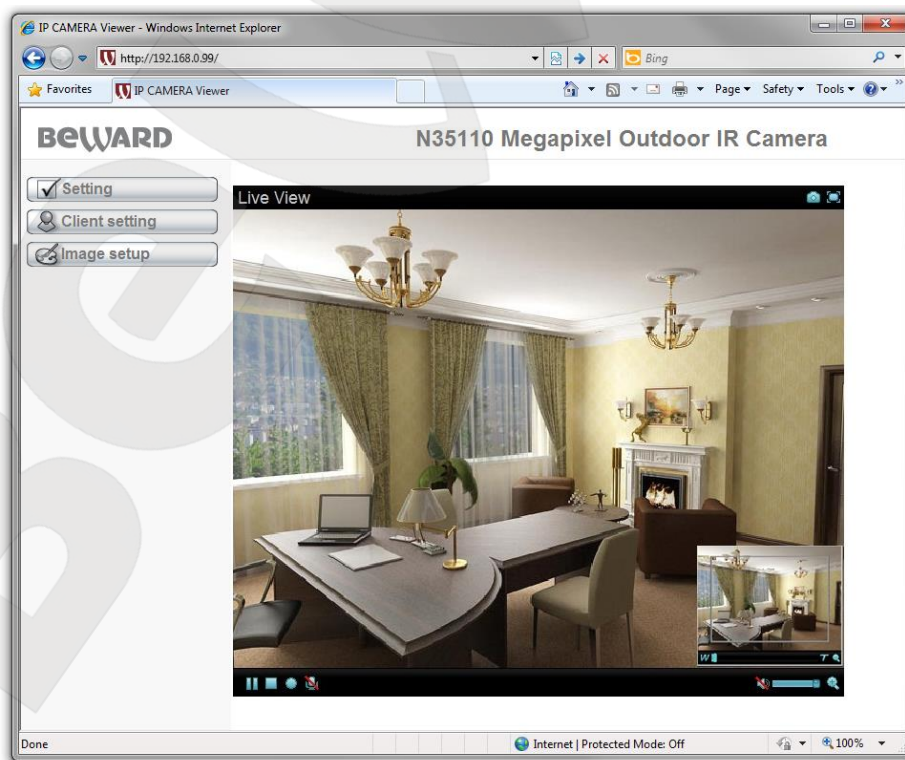
In Windows 7, you need to start Internet Explorer as an administrator to save records on your local HDD.

5.1.2. [Fullscreen] Button

Click the  button to hide the controls and stretch the image to fill the screen. Press **[ESC]** or double-click left mouse button to exit full screen mode.

5.1.3. [Open Digital Zoom] Button

Click the  button to magnify a specific area of the image. Drag the slider towards the magnification level that you want  (W is wide (no magnification)/T is tele (maximum magnification). Move this  frame to the desired area. Click the  button to exit the digital zoom mode and save the selected magnification (*Pic. 5.2*).








Pic. 5.2

NOTE:

The image zoom is applied only for the current images in the browser. Such parameters are saved in the browser's temporary folder. The next time you open the browser, the magnification level of the image will be set to the value that was set when you previously closed the browser (if the option for saving settings is enabled in the browser). If the image is viewed through software, the magnification settings will not be applied.

5.1.4. Video Control Buttons

Icon	Function
	[Pause] : click this button to temporarily pause the playback.
	[Play] : click this button to resume the playback.
	[Stop] : click this button to stop the playback.
	[Start record] : click this button to specify the path for saving the files and after that start recording the video.
	[Stop record] : click this button to stop recording the video.

IMPORTANT:



To playback the recorded video, use the integrated player at **SETTING – Camera – Playback**, otherwise you may need to install third-party software, e.g. VLC media player. Its official website is <http://www.videolan.org/vlc/>.




NOTE:

When specifying the path, check the permissions on the folder where you want to save the snapshot. If you do not have the permissions, you cannot save snapshots there.

In Windows 7, you need to start Internet Explorer as an administrator to save records on your local HDD.

5.1.5. Audio Control Buttons

Icon	Function	Comments
	[Sound enabled]	Transmits sound from the camera's microphone (Audio In) to the speakers connected to your computer (if the microphone is connected to the correct jack).
	[Sound disabled]	Stops transmitting sound from the camera's microphone to the speakers connected to your computer.

	[Mic is on]	Transmits sounds from the microphone connected to your computer to the speakers connected to your camera (Audio Out).
	[Mic is off]	Stops transmitting sounds from the microphone connected to your computer to the speakers connected to your camera.
	[Volume level]	Move this slider to the desired level to adjust the volume at which sound is transmitted from the camera (if the microphone is connected to the correct jack).

5.2. Setting Menu

This menu provides options for configuring the IP camera (Pic. 5.3). The menu is divided into two sections, the **[Basic]** (Pic. 5.4) and the **[Advanced]** (Pic. 5.5), which are both provide options for adjusting and configuring the IP camera.

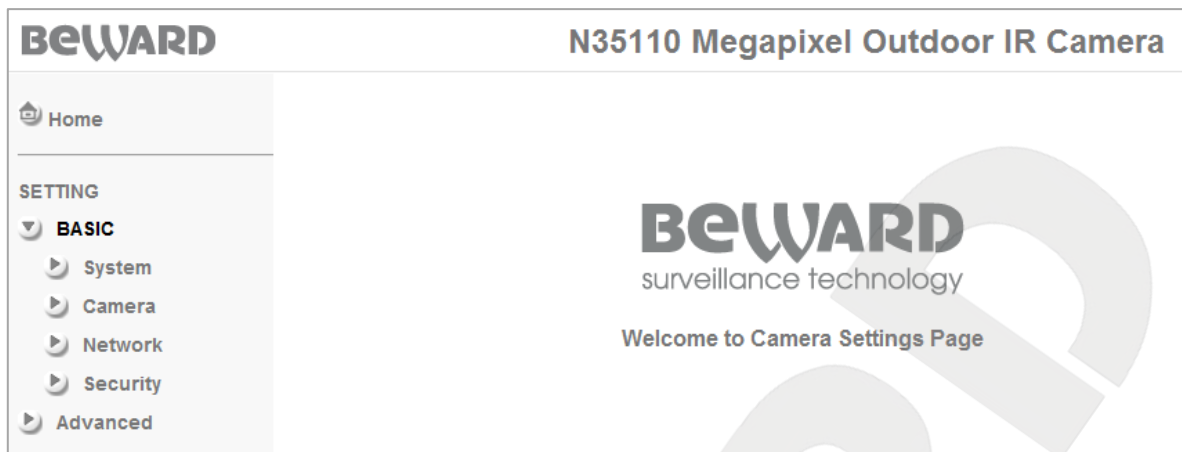


Pic. 5.3

IMPORTANT:

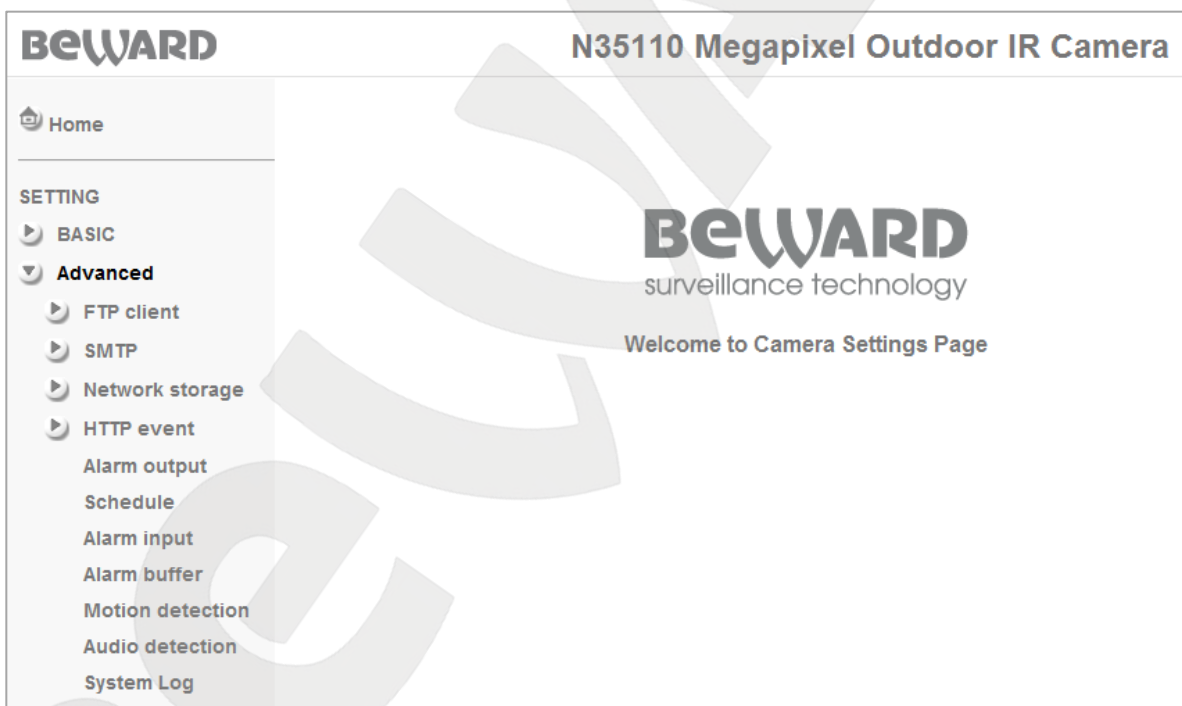
This menu is available only for administrators.

The **[Basic]** menu is divided into the following sections: **[System]**, **[Camera]**, **[Network]**, and **[Security]** (Pic. 5.4). Detailed information is discussed later in this Manual.



Pic. 5.4

The **[Advanced]** menu is divided into the following sections: **[FTP client]**, **[SMTP]**, **[Network storage]**, **[HTTP event]**, **[Alarm output]**, **[Schedule]**, **[Alarm input]**, **[Alarm buffer]**, **[Motion detection]**, **[Audio detection]**, and **[System log]** (Pic. 5.5). Detailed information is discussed later in this Manual.



Pic. 5.5

5.3. Client Setting

This menu provides options for adjusting the camera image. These settings are applied only to the image viewed via the browser and do not change the camera settings. This menu is divided into the following sections: **[Mode]**, **[View size]**, **[Protocol]**, and **[Video buffer]** (Pic. 5.6).



Pic. 5.6

5.3.1. Mode

You can select a compression type from the list of available compressions: H.264, MPEG-4, Motion JPEG and JPEG (sends individual JPEG images sequentially).

NOTE:

Displaying of some menu items depends on selected compression. Detailed information is discussed later in this Manual.

5.3.2. View Size

You can adjust the image resolution in proportion to its current size: 1X, 1/2X, 1/4X. The number of displayed image size proportions and the proportions themselves may vary and depend on the resolution that a user selected in the **[Camera]** menu. The 1X, 1/2X, 1/4X proportions are available when 1280x1024 or 1280x720 resolution is selected; the 1X, 1/2X proportions are available when 640x480 resolution is selected; the 1X, 2X proportions are available when 320x240 resolution is selected. This item is available for all compressions.

5.3.3. Protocol

You can select any of the available protocols: HTTP, TCP, UDP, or Multicast. This item is available for **[H.264]**, **[MPEG-4]**, or **[MJPEG]** mode.

HTTP: select this item for video streaming via HTTP.

TCP: select this item for video streaming via TCP, RTSP is used as a control protocol.

UDP: select this item for video streaming via UDP, RTSP is used as a control protocol.

Multicast: select this item to stream video to multiple users at once. It reduces bandwidth usage by delivering a single stream of information to multiple network recipients.

IMPORTANT:

[Multicast] mode is available only for [H.264], [MPEG-4], and [MPEG-4].

When selecting any of the available transport protocols, it automatically assigns the following data ports: HTTP – 80, TCP – 554. If UDP is selected, it uses the strictly defined range of port numbers. The port number is assigned when the camera establishes a connection with a client.

NOTE:

«HTTP» protocol is for networks where the port number restriction is used. When such a security policy is applied, all nonstandard ports are blocked but port 80 is commonly open (443, 554, etc) and is used by this connection type.

IMPORTANT:

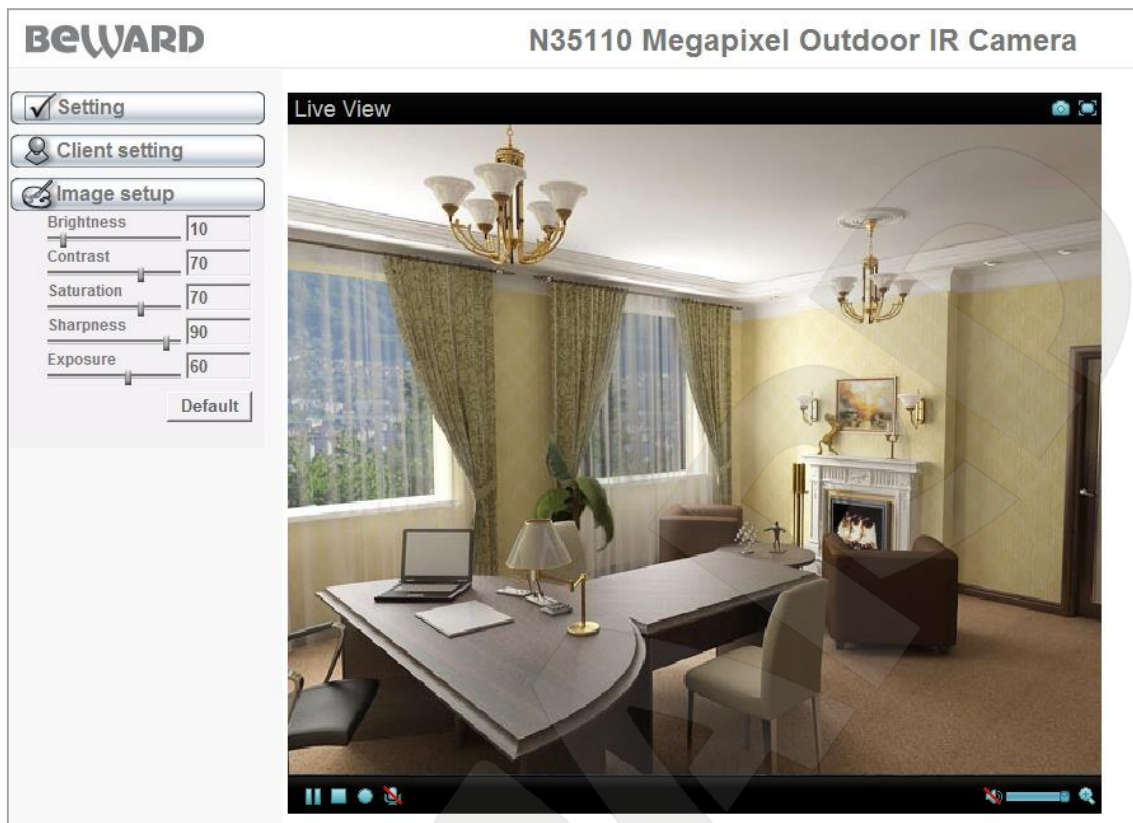
When the [Multicast] mode is selected, the number of simultaneous users for viewing the image is not limited. To enable this mode for a specific image compression, go to **SETTING – Basic – Camera** and go to the menu related to the required image compression (H.264, MPEG4, or MJPEG). When using the other modes, the maximum number of simultaneous connections is 5 (depends on network port use)

5.3.4. Video Buffer

You can enable or disable the video buffer function. When this function is enabled, it makes the video stream from the IP camera smoother when the connection is unstable but may cause lags up to several seconds.

5.4. Image Setup

This menu provides options for adjusting [Brightness], [Contrast], [Saturation], and [Hue] (Pic. 5.7).



Pic. 5.7

5.4.1. Brightness

You can increase or decrease the image brightness.

5.4.2. Contrast

You can increase or decrease the image contrast.

5.4.3. Saturation

You can increase or decrease the image saturation. If the saturation is set to its minimum, the image will be black and white.

5.4.4. Sharpness

You can increase or decrease the image sharpness.

5.4.5. Exposure

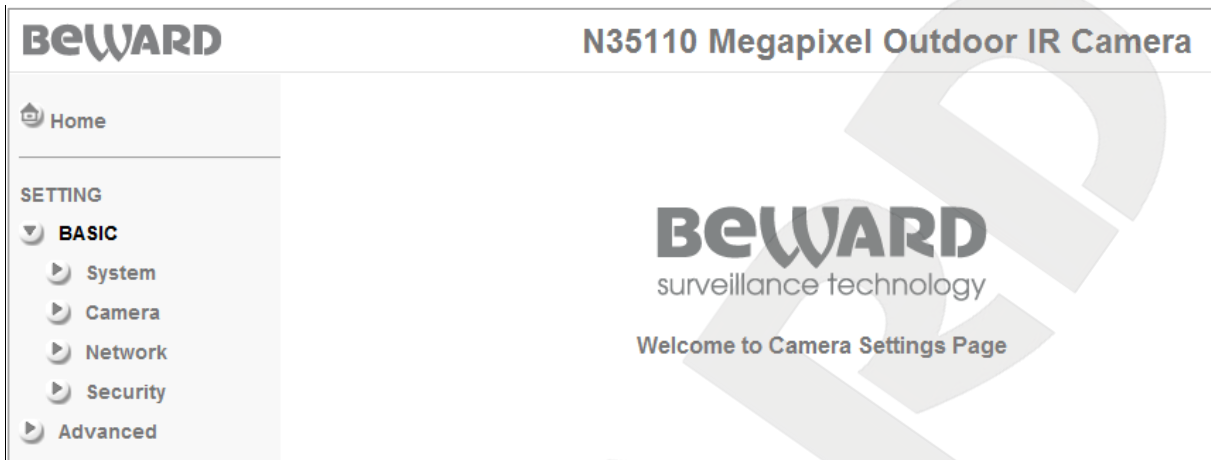
You can adjust the electronic shutter.

5.4.6. Default

Click this button to restore the following items to their default settings: brightness, contrast, saturation, and hue. If the image still has color distortion, adjust the hue manually.

Chapter 6. SETTING: Basic Menu

This menu is divided into the following sections: **[System]**, **[Camera]**, **[Network]**, and **[Security]** (*Pic. 6.1*).



Pic. 6.1

6.1. System

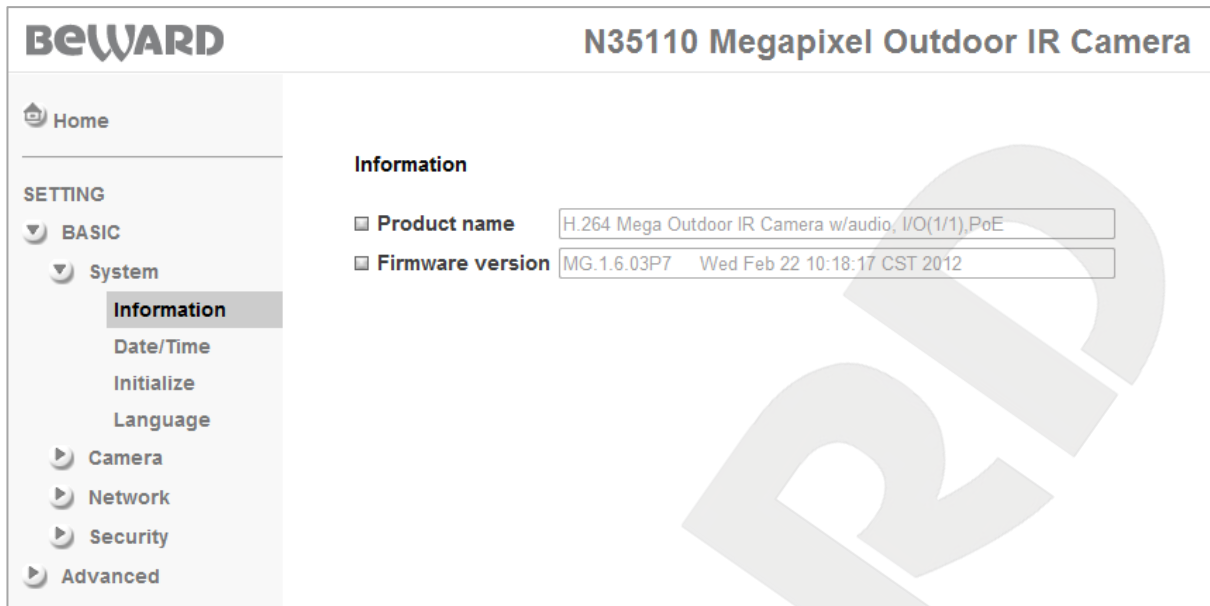
This menu is divided into the following sections: **[Information]**, **[Date/Time]**, **[Initialize]**, and **[Language]** (*Pic. 6.2*).



Pic. 6.2

6.1.1. Information

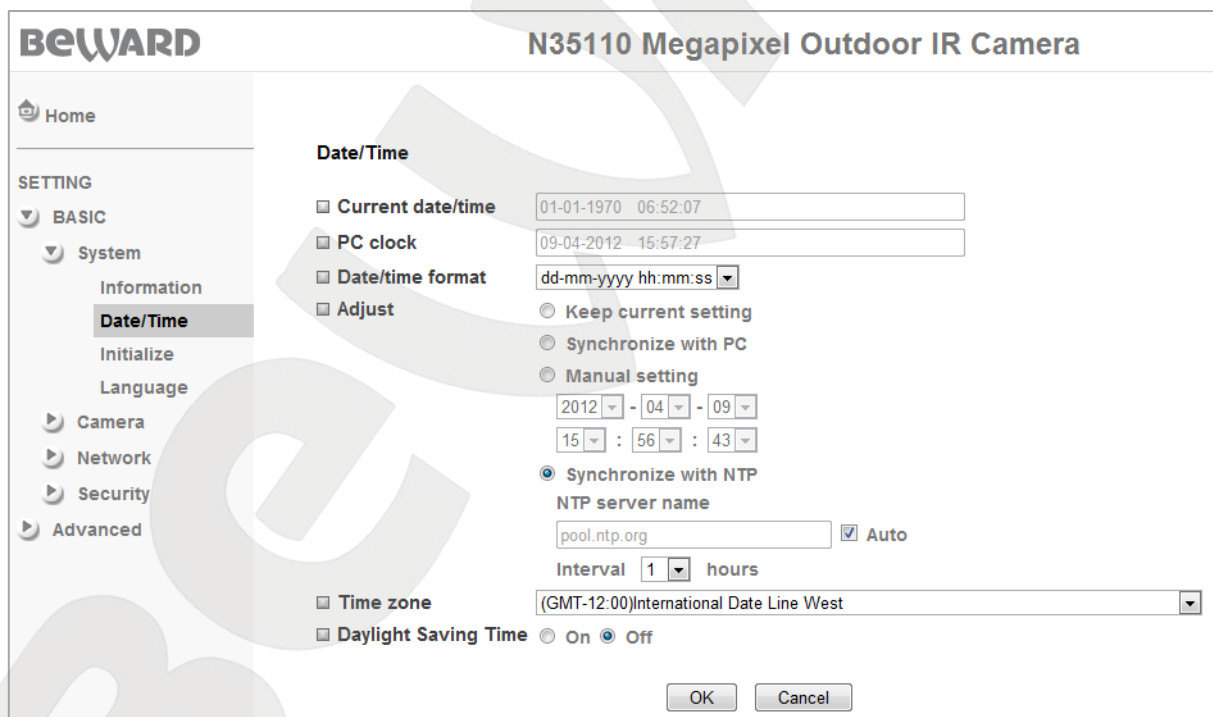
This section provides the camera's name and firmware version (*Pic. 6.3*).



Pic. 6.3

6.1.2. Date/Time

This menu provides options for setting the camera's date and time (Pic. 6.4).



Pic. 6.4

Current date/time: displays the current date and time of the camera.

IMPORTANT:

After you reboot the camera, its date and time will be reset to their default values: **1970-01-01 00:00:00**. It is recommended to use the **[Synchronize with NTP]** option to set the correct date and time.

PC clock: displays date and time of the computer that is used for connection to the camera (client computer).

Date/Time format: select a date/time format.

Adjust: select how to set the camera's date and time.

- **Keep current setting:** keeps the current date and time as they are.
- **Synchronize with PC:** sets the same date and time as on the computer that is used for connection to the camera.
- **Manual setting:** select this mode to adjust the camera's date and time manually.
- **Synchronize with NTP:** synchronizes your camera's date and time with an NTP server (Network Time Protocol) located in the Internet (e.g. time.windows.com, time.nist.gov, etc). Select an NTP server name and a time update interval (by default, camera's date and time are typically updated once an hour).

NOTE:

By default, the camera time is synchronized with the following NTP server: pool.ntp.org.

IMPORTANT:

To synchronize the camera time, an NTP server must be accessible on the local network or over the Internet. The camera must be connected to the Internet to synchronize the time with an Internet time server.

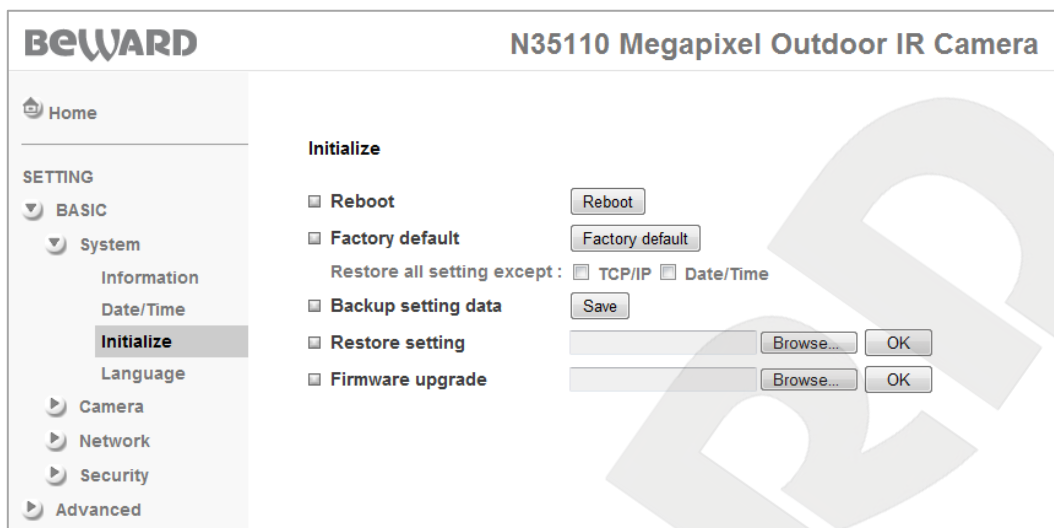
Time Zone: choose the time zone in which the camera is located. The correct time zone is important for the synchronization with an NTP server.

Daylight Saving Time: this item allows your camera's internal clock to be automatically adjusted when daylight saving time changes. This parameter is important for the correct synchronization with an NTP server. You can specify the start time and the end time so that the camera's internal clock could be adjusted by date or by week number (*Pic. 6.5*).

Daylight Saving Time
 On Off
 By date By week number
 Start time: January | First | Mon | 01 | 00 : 00
 By date By week number
 End time: January | First | Mon | 01 | 00 : 00

Pic. 6.5

6.1.3. Initialize



Pic. 6.6

[Reboot]: click this button to reboot the camera. The camera takes 1-2 minutes to reboot. If you click the **[Reboot]** button, the confirmation dialog box appears. The user will be prompted to continue or cancel the reboot. Click **[OK]** to continue or click **[Cancel]** to cancel the reboot.

[Factory Default]: click this button to reset the camera to factory defaults. After that, the camera will reboot. All settings including the IP address, the user name, and the password will return to their defaults. Do not power off the camera until the reboot is completed!

If you click the **[Factory Default]** button, the confirmation dialog box appears. The user will be prompted to continue or cancel the reset to factory defaults. Click **[OK]** to continue or click **[Cancel]** to cancel.

NOTE:

See the [Appendix E](#) for information on camera's default values.

Backup setting data: you can save the camera settings to a file. Click **[Save]** and specify the path where you want to save the settings and enter the file name.

NOTE:

When specifying the path, check the permissions on a folder where you want to save a snapshot. If you do not have the permissions, you cannot save snapshots there.

In Windows 7, you need to start Internet Explorer as an administrator to save records on your local HDD.

Restore setting: you can restore previously saved settings. Click **[Browse]** to select the backup file. In the appeared window, select the required file by clicking your left mouse button on the name of the file and click **[Open]**. Click **[OK]** to start restoring the settings. When the restoration is completed, the camera automatically restarts to apply the settings.

Firmware upgrade: this item allows you to update the camera firmware. Click **[Browse]** or specify the path of the firmware manually. In the appeared window select the required file by clicking your left mouse button on the name of the file and click **[Open]**. Click **[OK]** to start updating the firmware.

NOTE:

When the firmware is updated, all settings may automatically restore to their defaults. Before you start updating the firmware, it is recommended to perform a backup of camera settings.

When the update is completed, the camera automatically reboots.

IMPORTANT:

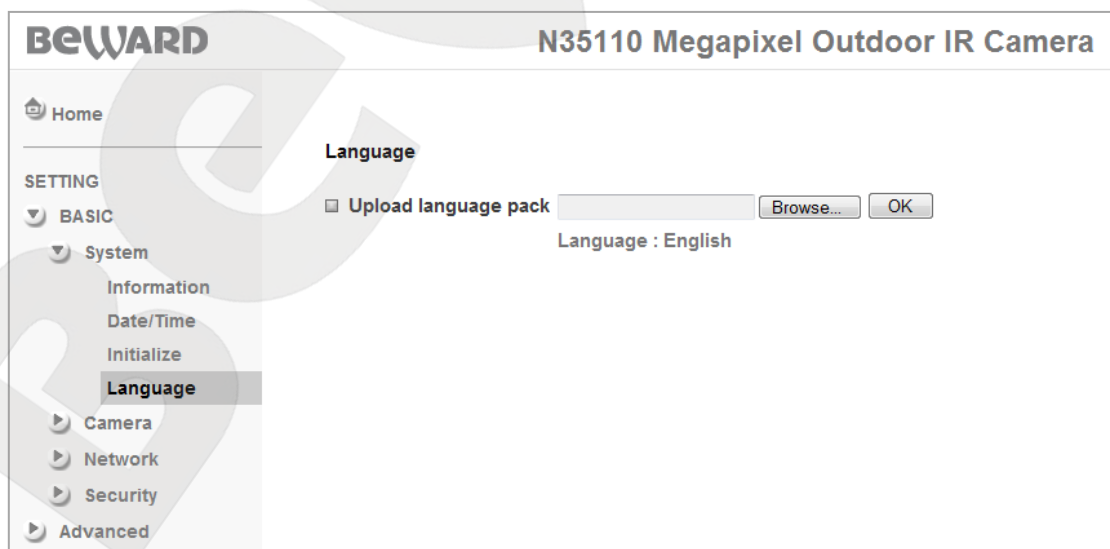
When the update is completed, it is recommended to reset camera settings to their factory defaults.

IMPORTANT:

Be careful when you update camera firmware. Make sure that you use only the firmware designed for your IP camera. Using the wrong firmware file may cause your camera to become inoperable. The manufacturer is not liable for the incorrect firmware update. Do not disconnect your camera until the update is completed.

6.1.4. Language

Upload Language Pack: you can upload a language module to change the camera's web interface language. Click the **[Browse]** button. In the appeared window, left-click the language file and click **[Open]**. Click **[OK]** to change the web interface language (Pic 6.7).



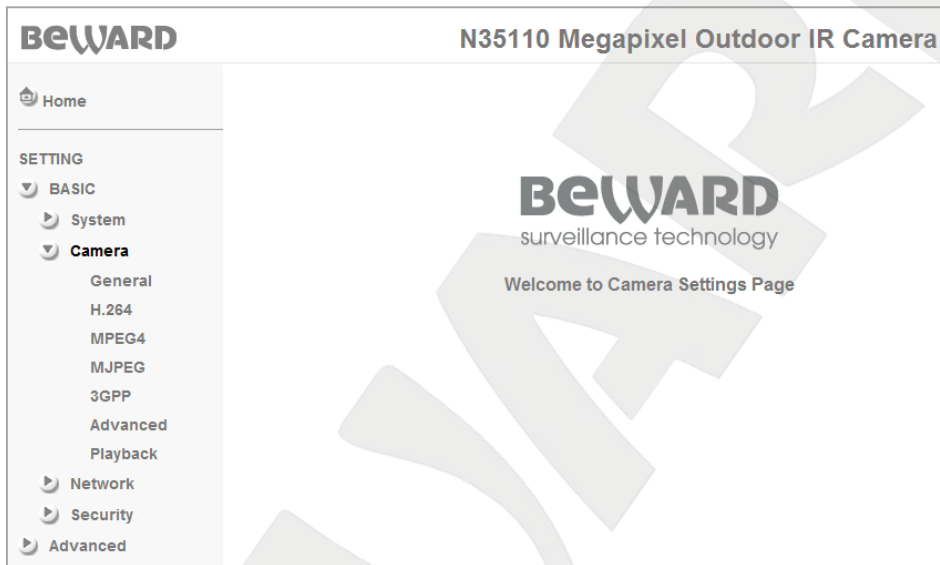
Pic. 6.7

IMPORTANT:

Be careful when you upload a language pack. Make sure that you use a language pack that is compatible with your IP camera. Using an incompatible language pack may cause your camera to become inoperable. The manufacturer is not liable for failure caused by uploading an incompatible language pack.

6.2. Camera

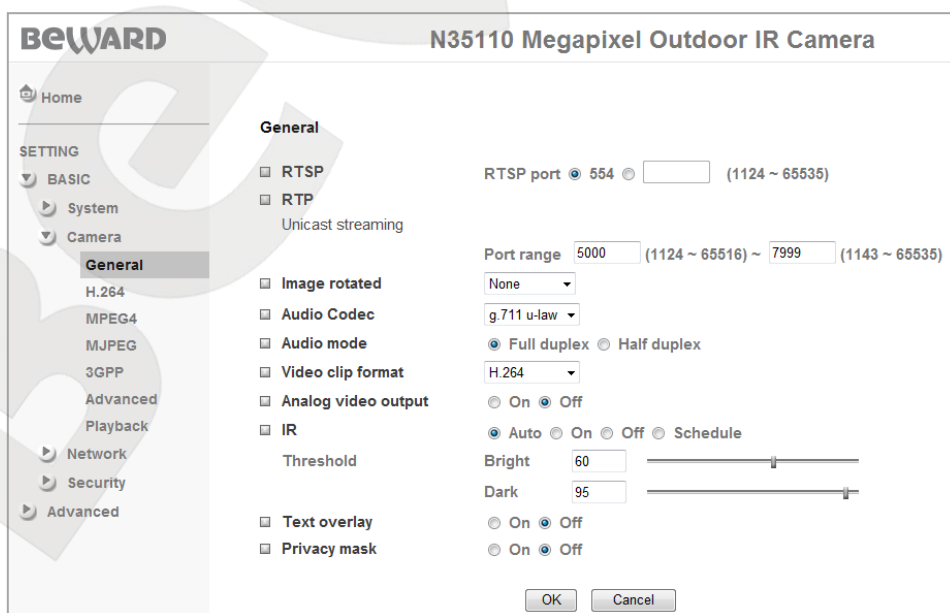
The [Camera] menu is divided into the following sections: [General], [H.264], [MPEG-4], [MJPEG], [3GPP], [Advanced], and [Playback] (Pic. 6.8).



Pic. 6.8

6.2.1. General

This menu provides options for adjusting the camera's image and other functions (Pic. 6.9).



Pic. 6.9

RTSP: this menu item provides options for configuring the RTSP port (the default value is 554). This is a standard reserved port and it is not recommended to change its value. However, you can set the value of the port between the values of 1124 and 65535.

RTP: specify a port range to transfer data between the camera and a client (clients). The port number is assigned automatically when the connection is established. The port number is assigned only during stream transmission. You can set the value of the port between the values of 1124 and 65535.

Image rotated: this menu provides options to rotate image from the camera. The following options are available: **«None»** - the image is not rotated; **«Mirror»** - the image is mirrored around the vertical axis; **«Flip»** - the image rotated 180°; **«Mirror» + «Flip»** - the image is mirrored and rotated 180°.

Audio codec: this mode allows you to select one of the following audio compression formats or to disable audio transmission:

- **g.711 μ -law:** select this option to set audio compression based on this standard.
- **g.711 α -law:** select this option to set audio compression based on this standard.
- **AMR Audio:** select this option to set audio compression based on this standard.

If AMR mode is selected, the following options for **Bit rate** are available: 4.75, 5.15, 5.9, 6.7, 7.4, 7.95, 10.2, 12.2 kbps. The wider the bandwidth, the higher the quality of audio transmission.

- **Off:** select this option to disable audio transmission.

Audio mode: this item allows you to set an audio transmission mode: two-way (full duplex) or one-way (half-duplex).

NOTE:

When **[Half-duplex]** is selected, you can either transmit sound through a microphone connected to your computer to speakers connected to your camera or through a microphone connected to your camera to speakers connected to your computer.

Video clip format: this item allows you to select format for video that is recorded using camera's web interface. You can select H.264 or MPEG4.

Analog video output: this item allows you to enable or disable camera's analog video output.

- **On:** the output is enabled.
- **Off:** the output is disabled.

NOTE:

The **[Analog video output]** is available only for H.264.

IR: allows you to set IR LED mode. **[On]** means that the IR LED is always turned on. **[Off]** means that the IR LED is always turned off. **[Auto]** means that the IR LED automatically turns on or off according to the illumination level. You can adjust the threshold by moving the **[Bright]** and **[Dark]** slider bars. **[Schedule]** means that the IR LED turns on or off according to the schedule. Click the **[Schedule]** button to specify the schedule or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for detailed information.

NOTE:

If the **[Auto]** mode is selected, response time of the IR LED is about 10 seconds.

Text overlay: you can enter any text (for example, device name) and/or date and time. You can change the **[Text color]** and **[Background color]**.

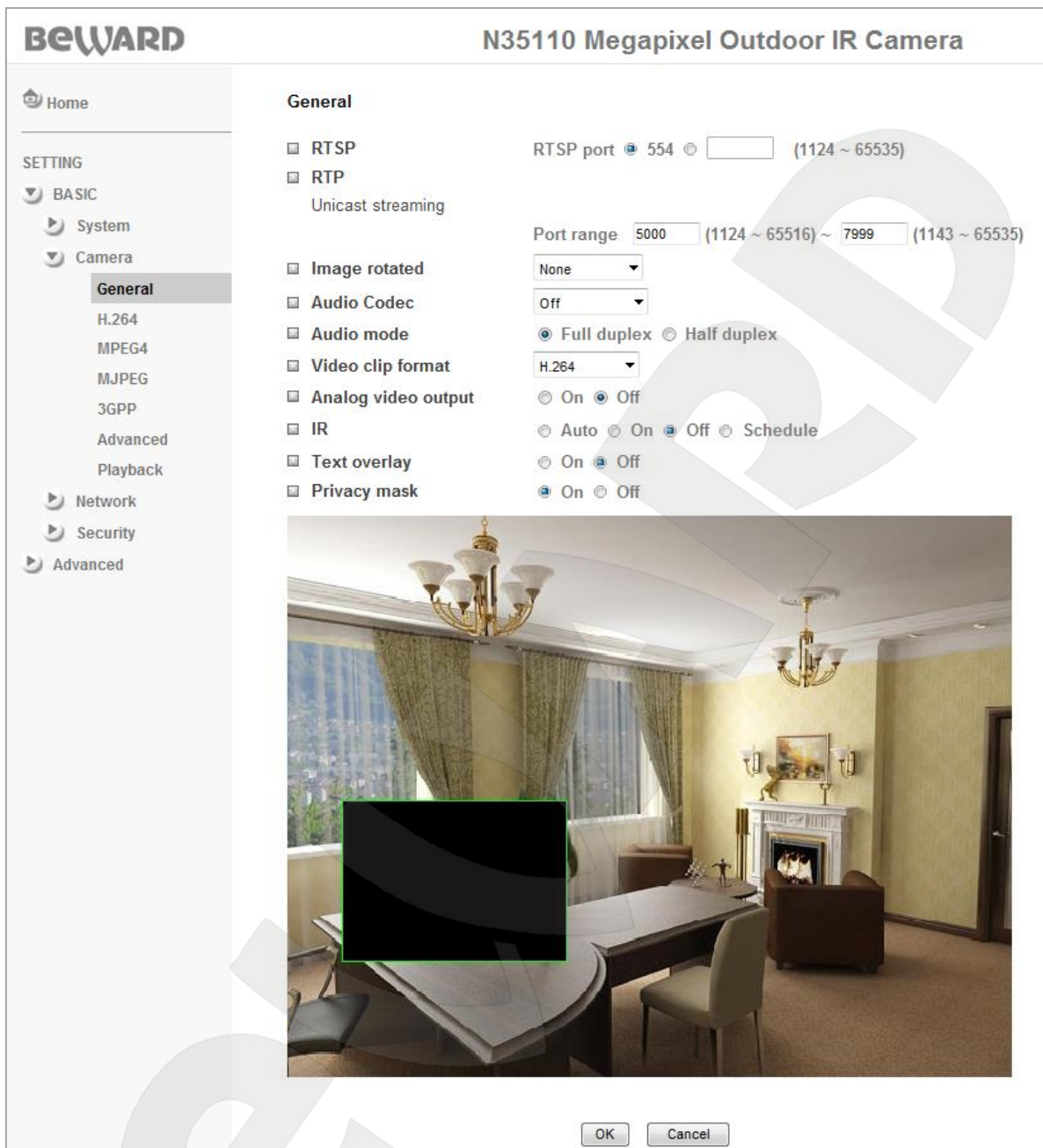
Pic. 6.10

NOTE:

The **[Alias]** field may contain only numbers or uppercase letters (A-Z), 6 characters maximum.

Privacy mask: you can set up a privacy mask to hide a part of the monitored area and therefore an area applied with a privacy mask will not be recorded. This is useful when there are areas in the camera view that must not be recorded. For example, a door security lock or a safe. Therefore to prevent an area from viewing, apply a privacy mask on it (Pic. 6.11).

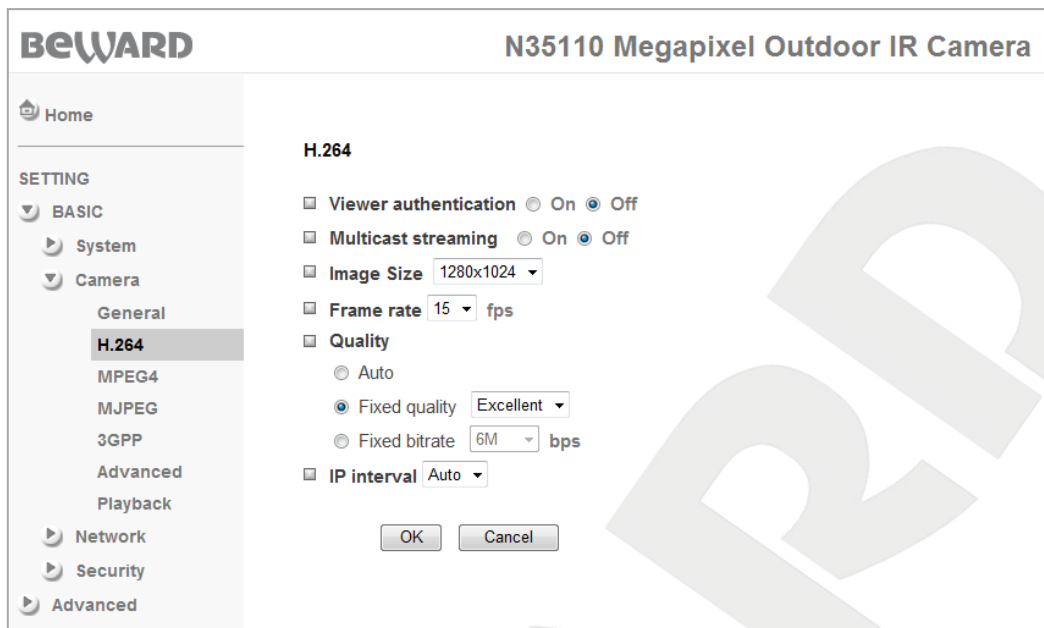
If you want to change the size, drag the right bottom corner of the frame. Also, you can adjust the size anytime by dragging any of its corners or move the privacy mask to the required position (Pic. 6.11).



Pic. 6.11

6.2.2. H.264

This menu provides options for streaming H.264 video (*Puc. 6.12*).



Pic. 6.12

Viewer authentication: if this option is enabled, a user will be required to enter a user name and a password to view video through third-party software such as Quick Time.

Multicast streaming: enable or disable multicast streaming. When this function is enabled, the following menu items appear: **[Multicast address]**, **[Video port]**, **[Audio port]**, **[Time-To-Live]** (Pic. 6.13).



Pic. 6.13

IMPORTANT:

To use multicast streaming, your network router must support it.

Multicast address: enter the multicast IP address. The default value is 228.0.0.1.

Video port: enter the port on which the camera sends a multicast video stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Audio port: enter the port on which the camera sends a multicast audio stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Time-To-Live: adjust the multicast packet time to live. The default value is 15.

NOTE:

TTL is a mechanism that limits the lifespan of data in a computer or network.

Image size: select the desired resolution: 1280x1024, 1280x720, 640x480 or 320x240.

Frame rate: select the desired frame rate per second. Depending on selected resolution, the following values are supported: 2, 3, 4, 5, 7, 10, 15, 20, 25 and 30 frames per second. For 1280x1024 or 1280x720 resolution, the following frame rate values are supported: 2, 3, 4, 5, 7, 10, and 15. For 640x480 or 320x240 resolution, the following frame rate values are supported: 2, 3, 4, 5, 7, 10, 15, 20, 25, and 30.

NOTE:

To use a frame rate value higher than 15, set a resolution not higher than 640x480 for H.264/MPEG-4/MJPEG streams.

Quality: choose an option for the video quality of the video stream from the camera.

- **Auto:** the camera automatically adjusts the image quality and the frame rate according to available bandwidth. In low-bandwidth conditions, the camera automatically reduces video streaming rate and leaves the frame rate unchanged.
- **Fixed quality:** set the video quality to: **[Excellent]**, **[Detailed]**, **[Good]**, **[Standard]**, and **[Medium]**.
- **Fixed bitrate:** set the video bitrate to a fixed value: 64, 128, 256, 384, 512, 768 kbps and 1, 1.5, 2, 3, 4, 5, 6 Mbps.

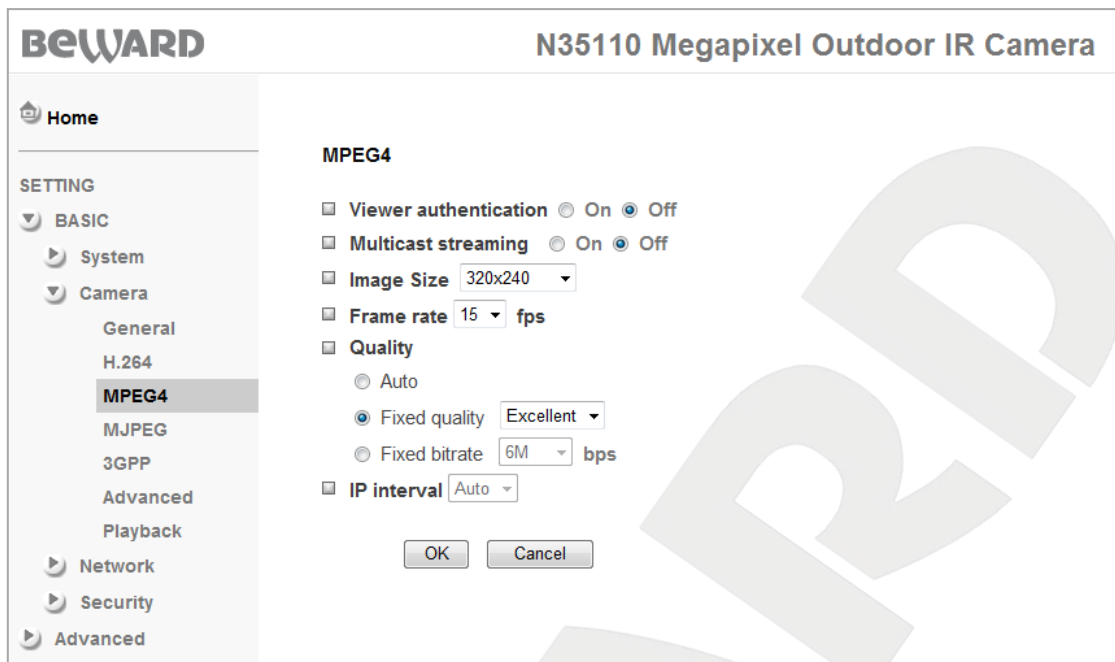
IP interval: a numerical relation between i-frames and p-frames. The following values are available: 1, 5, 10, 15, 30, 60, 120 and Auto. The less the value, the better the image quality and the more bandwidth is required for video streaming. It determines, how many p-frames should be sent before another i-frame (or a key frame) is sent.

NOTE:

If H.264 is selected in **SETTING – Basic – Camera – General**, the **[IP interval]** becomes unavailable and the numerical relation between i-frames and p-frames sets to **[Auto]** (the camera automatically sets the value).

6.2.3. MPEG-4

This menu provides options for streaming MPEG-4 video (*Pic. 6.14*).



Pic. 6.14

Viewer authentication: if this option is enabled, a user will be required to enter a user name and a password to view video through third-party software such as Quick Time.

Multicast streaming: enable or disable multicast streaming. When this function is enabled, the following menu items appear: **[Multicast address]**, **[Video port]**, **[Audio port]**, **[Time-To-Live]** (Pic. 6.15).

Pic. 6.15

Multicast address: enter the multicast IP address. The default value is 228.0.0.1.

Video port: enter the port on which the camera sends a multicast video stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Audio port: enter the port on which the camera sends a multicast audio stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Time-To-Live: adjust the multicast packet time to live. The default value is 15.

NOTE:

TTL is a mechanism that limits the lifespan of data in a computer or network.

Image size: select the desired resolution: 1280x1024, 1280x720, 640x480 or 320x240.

Frame rate: select the desired frame rate per second. Depending on selected resolution, the following values are supported: 2, 3, 4, 5, 7, 10, 15, 20, 25 and 30 frames per second For 1280x1024 or 1280x720 resolution, the following frame rate values are supported: 2, 3, 4, 5, 7, 10, and 15. For 640x480 or 320x240 resolution, the following frame rate values are supported: 2, 3, 4, 5, 7, 10, 15, 20, 25, and 30.

NOTE:

To use a frame rate value higher than 15, set a resolution not higher than 640x480 for H.264/MPEG-4/MJPEG streams.

Quality: choose an option for the video quality of the video stream from the camera.

- **Auto:** the camera automatically adjusts the image quality and the frame rate according to available bandwidth. In low-bandwidth conditions, the camera automatically reduces video streaming rate and leaves the frame rate unchanged.
- **Fixed quality:** set the video quality to: **[Excellent]**, **[Detailed]**, **[Good]**, **[Standard]**, and **[Medium]**.
- **Fixed bitrate:** set the video bitrate to a fixed value: 64, 128, 256, 384, 512, 768 kbps and 1, 1.5, 2, 3, 4, 5, 6 Mbps.

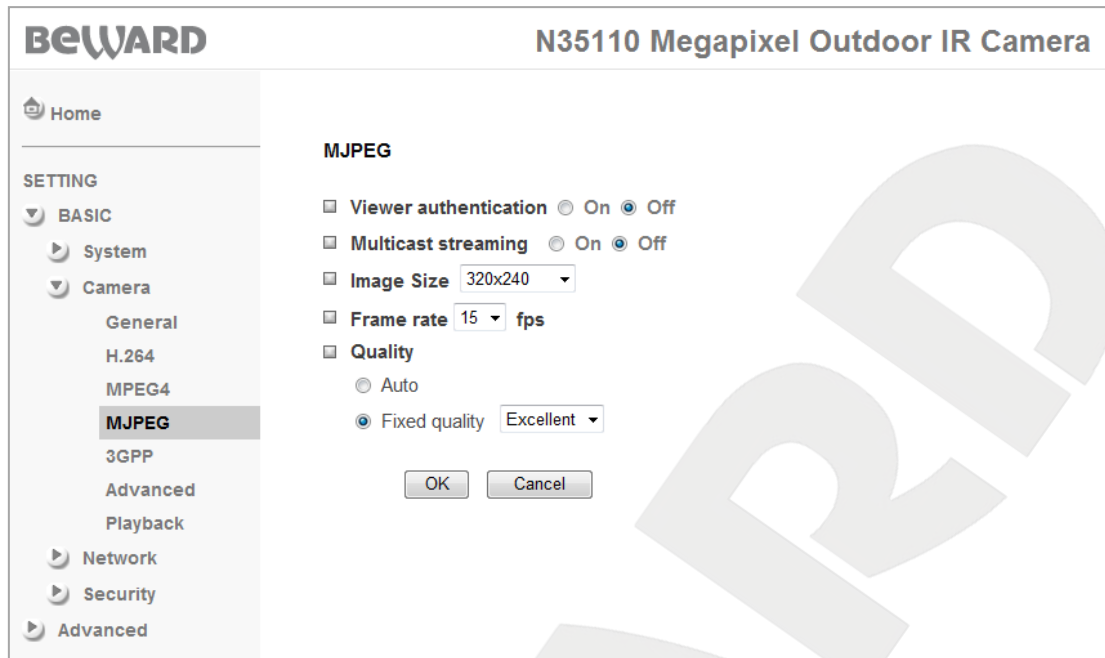
IP interval: a numerical relation between i-frames and p-frames. The following values are available: 5, 10, 15, 30, 60, 120 and Auto. The less the value, the better the image quality and the more bandwidth is required for video streaming. It determines, how many p-frames should be sent before another i-frame (or a key frame) is sent.

NOTE:

If MPEG-4 is selected in **SETTING – Basic – Camera – General**, the **[IP interval]** becomes unavailable and the numerical relation between i-frames and p-frames sets to **[Auto]** (the camera automatically sets the value).

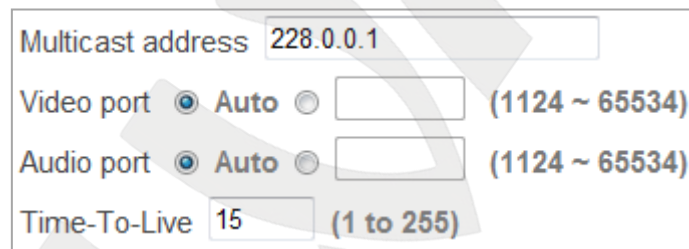
6.2.4. MJPEG

This menu provides options for streaming MJPEG video (*Pic. 6.16*).



Pic. 6.16

Viewer authentication: if this option is enabled, a user will be required to enter a user name and a password to view video through third-party software such as Quick Time.



Pic. 6.17

Multicast streaming: enable or disable multicast streaming. When this function is enabled, the following menu items appear: **[Multicast address]**, **[Video port]**, **[Audio port]**, **[Time-To-Live]** (Pic. 6.17).

Multicast address: enter the multicast IP address. The default value is 228.0.0.1.

Video port: enter the port on which the camera sends a multicast video stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Audio port: enter the port on which the camera sends a multicast audio stream. The port can be automatically assigned or you can manually set the value of the port between the values of 1124 and 65534.

Time-To-Live: adjust the multicast packet time to live. The default value is 15.

NOTE:

TTL is a mechanism that limits the lifespan of data in a computer or network.

Image size: select the desired resolution: 1280x1024, 1280x720, 640x480 or 320x240.

Frame rate: select the desired frame rate per second. Depending on selected resolution, the following values are supported: 1, 2, 3, 4, 5, 7, 10, 15, 20, 25 and 30 frames per second. For 1280x1024 or 1280x720 resolution, the following frame rate values are supported: 1, 2, 3, 4, 5, 7, 10, and 15. For 640x480 or 320x240 resolution, the following frame rate values are supported: 1, 2, 3, 4, 5, 7, 10, 15, 20, 25, and 30.

NOTE:

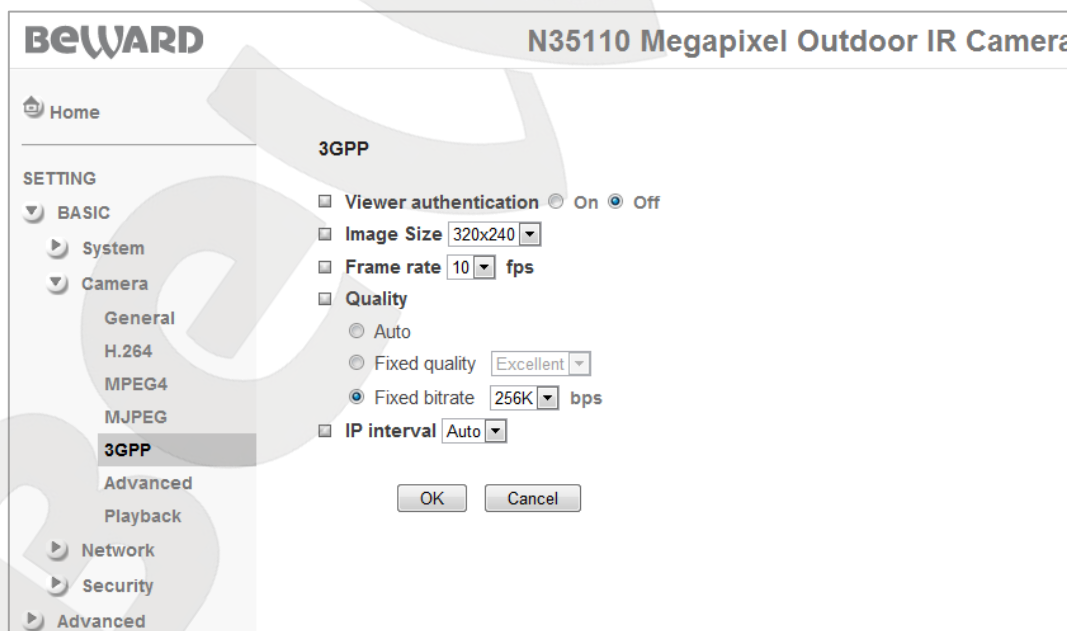
To use a frame rate value higher than 15, set a resolution not higher than 640x480 for H.264/MPEG-4/MJPEG streams.

Quality: choose an option for the video quality of the video stream from the camera.

- **Auto:** the camera automatically adjusts the image quality and the frame rate according to available bandwidth. In low-bandwidth conditions, the camera automatically reduces video streaming rate and leaves the frame rate unchanged.
- **Fixed quality:** set the video quality to: **[Excellent]**, **[Detailed]**, **[Good]**, **[Standard]**, and **[Medium]**.

6.2.5. 3GPP

This menu provides options for streaming 3GPP video to a cell phone (*Pic. 6.18*).



Pic. 6.18

Viewer authentication: if this option is enabled, a user will be required to enter a user name and a password to view video through third-party software such as Quick Time.

Image size: select the desired resolution: 160x120 or 320x240.

Frame rate: select the desired frame rate per second: 5 or 10 fps.

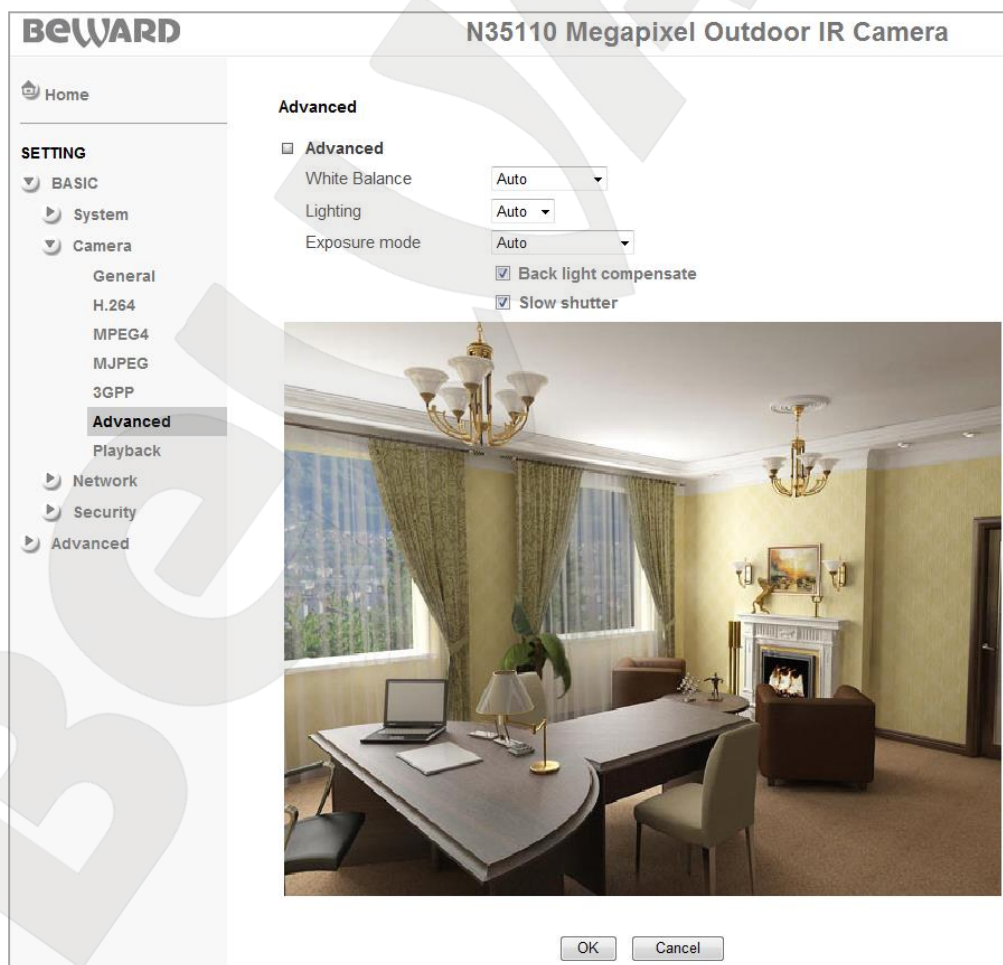
Quality: choose an option for the video quality of the video stream from the camera.

- **Auto:** the camera automatically adjusts the image quality and the frame rate according to available bandwidth. In low-bandwidth conditions, the camera automatically reduces video streaming rate and leaves the frame rate unchanged.
- **Fixed quality:** set the video quality to: **[Excellent]**, **[Detailed]**, **[Good]**, **[Standard]**, and **[Medium]**.
- **Fixed bitrate:** set the video bitrate to a fixed value: 16, 32, 48, 64, 128, 256 kbps.

IP interval: a numerical relation between i-frames and p-frames. The following values are available: 5, 10, 15, 30 and Auto. The less the value, the better the image quality and the more bandwidth is required for video streaming. It determines, how many p-frames should be sent before another i-frame (or key frame) is sent.

6.2.6. Advanced

This menu provides options for configuring the advanced parameters of the image and the sensor (*Pic. 6.19*).



Pic. 6.19

White balance: adjust white balance of the image. The following modes are available: **[Auto]**; **[Fluorescent]**; **[Incandescent]**; **[Sunny]**; or **[Cloudy]**.

Lighting: select lightning conditions at the camera location: **50 Hz**, **60 Hz**, or **Auto**.

Exposure mode: select a shutter speed. The following modes are available:

Auto: when this mode is selected, the shutter speed is adjusted automatically.

High speed mode: the shutter speed is adjusted automatically, but the minimum shutter speed is 1/120 s.

NOTE:

When the high-speed shutter mode is selected, the shutter speed is set to 1/120 s or higher depending on the lightning conditions. This mode is good for capturing fast-moving objects, for example, auto racing, sports, etc.

When **[Auto]** or **[High speed mode]** mode is selected, the following options are available:

- **Back light compensate (BLC):** check this box to enable backlight compensation.
- **Slow shutter:** limit the shutter speed between the values of 1/5 to 1/120 s.

NOTE:

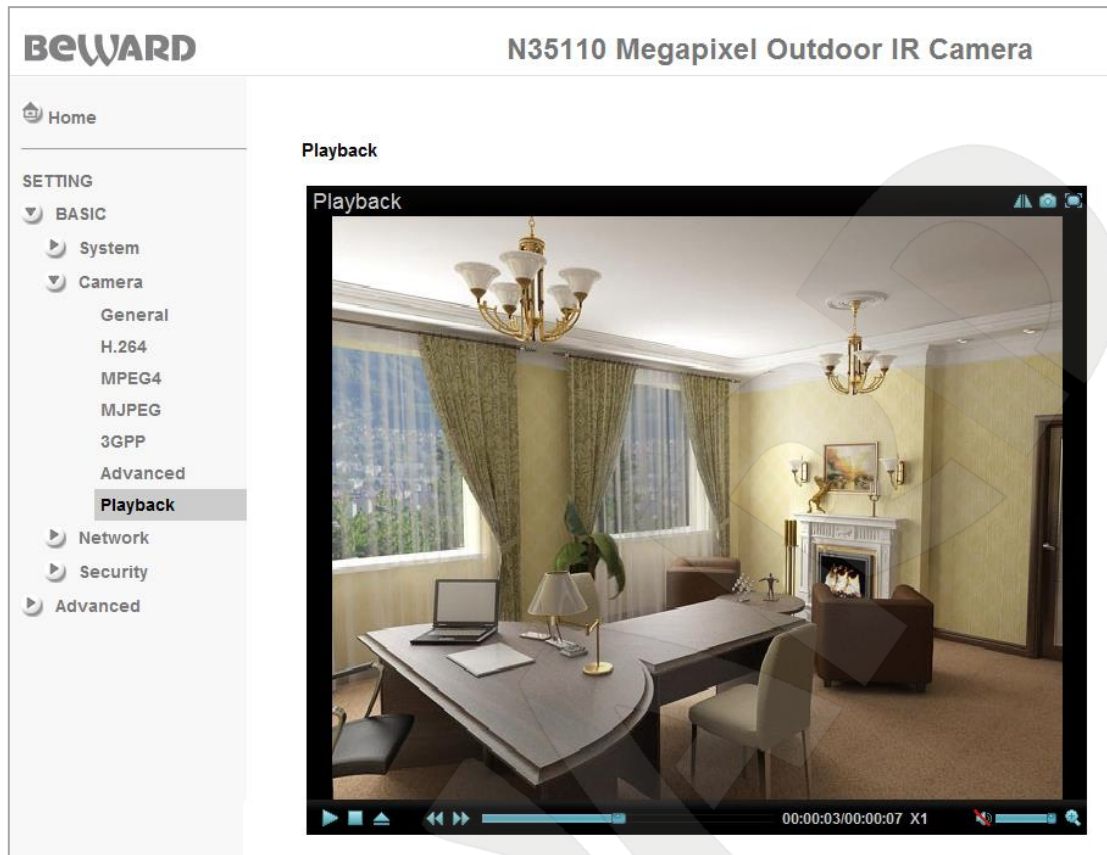
The slow shutter mode is useful when the camera is installed in environments with low lighting.

Manual: adjust the shutter speed manually. When this mode is selected, the following options are available:

- **Shutter speed:** the following values are available: 1/4, 1/5, 1/10, 1/25, 1/50, 1/100 s.
- **Gain:** set the gain from 0 to 9 in increments of 1. The higher the value, the brighter the image but the more noise in the image under low-light conditions.

6.2.7. Playback





This menu allows you to playback the video that was recorded via the web interface of the camera or the video that was recorded to network attached storage and then exported to a computer (*Pic. 6.20*).





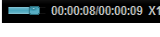




Pic. 6.20

Click the **[Open files]** button to open a video file recorded by clicking the **[Record]** button in the web interface.

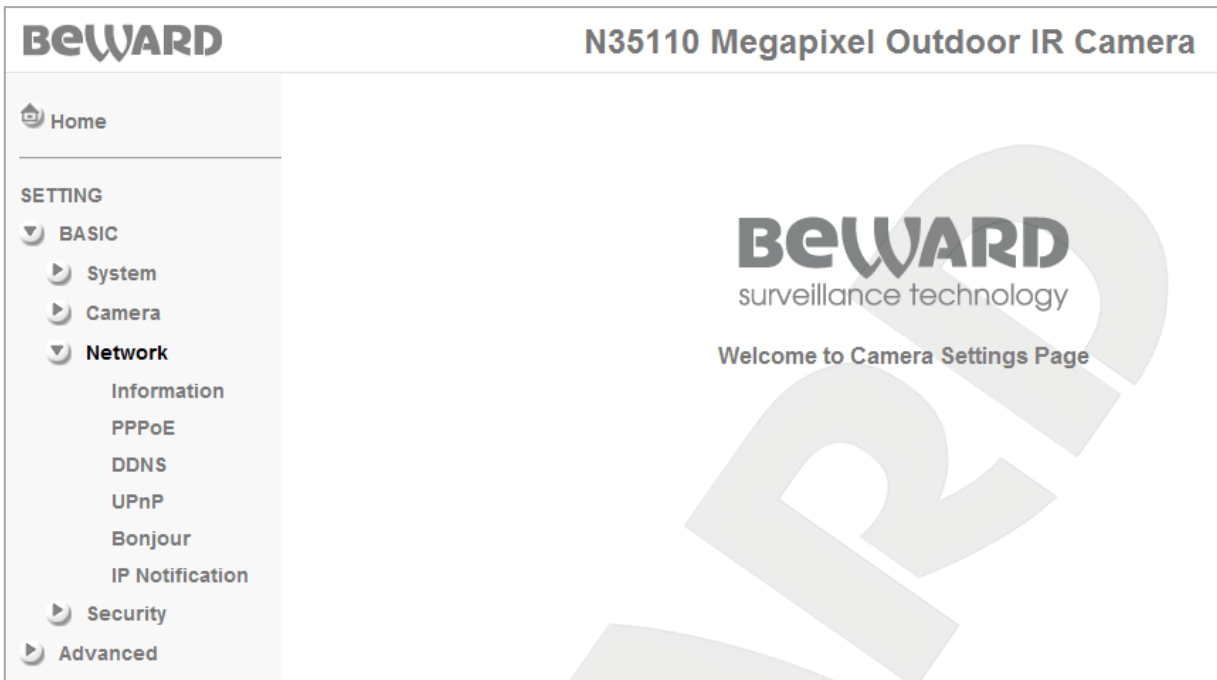
The playback control buttons are shown in the table below:

Icon	Function	Purpose
	[Mirror/Flip]	Rotate/mirror image.
	[Snapshot]	Click this button to capture and save a snapshot image. The snapshot format depends on the resolution of the recorded file.
	[Fullscreen]	Stretches the image to fill the screen.
	[Play/Pause]	Plays the selected file. If a file is currently being played, the [Play] button becomes the [Pause] button.

	[Stop]	Stops playing the selected file. If you click the [Play] button after you clicked the [Stop] button, the file starts playing from the beginning.
	[Open files]	Opens recorded files.
	[Increase speed]	Fast-forwards the video that you are playing. Double-click this button to change the playback rate to x2, x4. Click the «Decrease speed» to slow the playback rate.
	[Decrease speed]	Slows the playback rate. Double-click this button to change the playback rate to x1/2, x1/4. Click the «Increase speed» to fast forward the playback rate.
	[Timeline]	Displays the total playback time and the current playback position.
	[Volume]	Adjusts the volume of the recorded file.
	[Open digital zoom]	Enlarges the video image.

6.3. Network

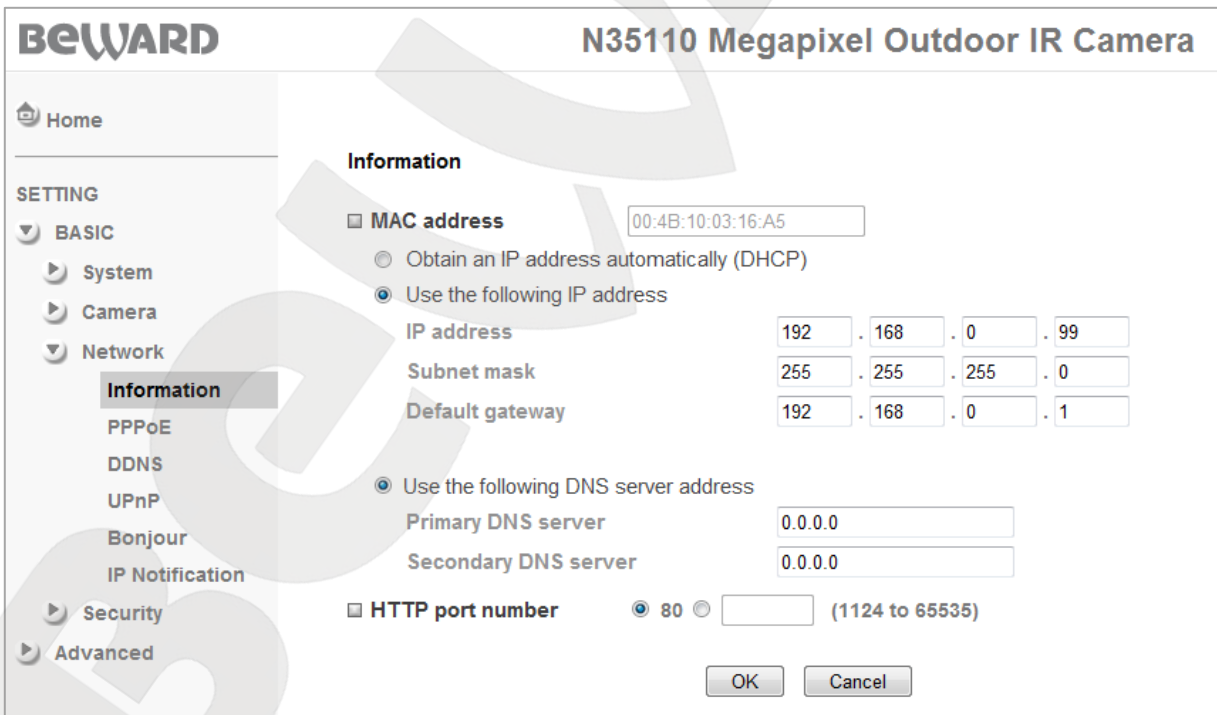
The **[Network]** menu is divided into the following sections: **[Information]**, **[PPPoE]**, **[DDNS]**, **[UPnP]**, **[Bonjour]**, and **[IP Notification]** (*Pic. 6.21*). Each of these sections is discussed later in this manual.



Pic. 6.21

6.3.1. Information

This menu provides options for configuring the network connection (Pic. 6.22).



Pic. 6.22

MAC address: current MAC address of the IP camera. It cannot be changed and is provided for informational purposes only.

Obtain an IP address automatically (DHCP): if your network includes a DHCP server, select this option to obtain an IP address automatically from a DHCP server on your network. After you select this option, the “**Obtain DNS server address automatically**” option will appear.

Obtain DNS server address automatically: select this option to obtain DNS server address automatically.

NOTE:

The [**Obtain DNS server address automatically**] option will appear only after the [**Obtain an IP address automatically (DHCP)**] option is selected.

Use the following IP address: select this option to manually enter the IP address. After you select this option, the following items will appear:

- **IP address:** enter the IP address for the IP camera. The default IP address is 192.168.0.99.
- **Subnet mask:** enter the subnet mask for the IP camera. The default subnet mask is 255.255.255.0.
- **Default gateway:** enter the gateway for the IP camera. The default gateway is 192.168.0.1.

Use the following DNS server address: select this option to manually enter the DNS server addresses. This option will appear both when the option for “**Use the following IP address**” is selected and when it is obtained automatically from a DHCP server.

- **Primary DNS server:** enter the IP address of the primary DNS server.
- **Secondary DNS server:** if required, enter the IP address of a secondary DNS server.

HTTP port number: the default port is 80. You can enter a port number from 1124 through 65535.

NOTE:

If you use an HTTP port number other than 80, you must specify the port number in the URL for the IP camera to access it. For example, if the IP address of the IP camera is 192.168.1.100 and the HTTP port is 8081, enter the following URL in the address bar of your browser to access the camera:
`http://192.168.1.100:8081.`

IMPORTANT:

You must reboot the camera for the changes to take effect. To do so, go to **SETTING – Basic – System – Initialize**.

6.3.2. PPPoE (Point-to-Point Protocol over Ethernet)

This menu provides options for configuring PPPoE connection. You can use a PPPoE connection to access the camera over the Internet when your ISP provides a dynamic IP address and a username and a password for PPPoE authentication.

To enable PPPoE, select the option for **[On]**. After that, the PPPoE parameters will appear (Pic. 6.23).

Pic. 6.23

IP address: enter a PPPoE IP address (obtained from the server).

User ID: enter a PPPoE username. The maximum length is 64 characters (assigned by your ISP or PPPoE provider).

Password: enter the PPPoE password. The maximum length is 32 (assigned by your ISP or PPPoE provider).

Re-type password: re-type the entered password to ensure that there are no typing mistakes.

Obtain DNS server address automatically: select this option to obtain a DNS address automatically.

Use the following DNS server address: a DNS server address is manually specified.

- **Primary DNS server:** enter the IP address of the primary DNS server.
- **Secondary DNS server:** enter the IP address of the secondary DNS server.

IMPORTANT:

You must reboot the camera for the changes to take effect. To do so, go to **SETTING – Basic – System – Initialize**.

IMPORTANT:

Once a PPPoE connection is established, the camera will not be available at the IP address specified in **SETTING – Basic – Network – Information** but will be available at the IP address obtained from the PPPoE server (**SETTING – General – Network – PPPoE**).

Use the option for **[IP notification]** to check the IP address assigned to the camera after a PPPoE connection is established (see [paragraph 6.3.6](#) for details).

6.3.3. DDNS (Dynamic DNS)

This menu provides options for configuring DDNS service. This service allows you to make your cameras accessible over the Internet even though they are assigned a dynamic IP address, which changes from time to time.

A domain name will be tied to the IP address of the camera. When the current IP address of the camera is changed, it is automatically tied to a predefined domain name, so that the camera can be accessed over the Internet any time despite its dynamic public IP address.

To use DDNS, select the option for **[On]** to enable it (*Pic. 6.24*).

IMPORTANT:

To use DDNS service, the camera must be connected to the Internet directly or through a router.

The screenshot shows the DDNS configuration interface for the BEWARD N35110 camera. The interface includes a sidebar with navigation options like Home, BASIC, System, Camera, Network, Information, PPPoE, DDNS (selected), UPnP, Bonjour, IP Notification, Security, and Advanced. The main area is titled 'DDNS' and contains a checkbox for 'DDNS' which is checked, and radio buttons for 'On' (selected) and 'Off'. Below this are several input fields: 'Server name' (pre-filled with 'http://www.dyndns.org'), 'User ID', 'Password', 'Re-type password', and 'Host name'. There is also a 'Periodical Update' section with radio buttons for 'Auto' and 'Periodical' (selected), and a dropdown menu set to '5 min'. At the bottom of the form are 'OK' and 'Cancel' buttons.

Pic. 6.24

Server name: select a DDNS provider.

User ID: enter the username that you chose at registration.

Password: enter the password that you chose at registration.

Re-type password: re-type the password to ensure that there are no typing mistakes.

Host name: enter the domain name that you chose at registration.

Periodical update: specify the interval at which DDNS server should check and update the IP address of the camera. The following options are available:

- **Auto:** DDNS server automatically updates the IP address.
- **Periodical:** choose the amount of time at which DDNS server will update the IP address of the camera. The following values are available: 5, 10, 15, 30, 60 minutes.

To update the IP address, the camera must be connected to the Internet, powered on, and the option for DHCP must be enabled.

NOTE:

For detailed information on how to configure DDNS, please refer to [Appendix F](#).

IMPORTANT:

You must reboot the camera for the changes to take effect. To do so, go to **SETTING – Basic – System – Initialize**.

6.3.4. UPnP (Universal Plug and Play)

If you are going to connect the camera to the Internet through a router, you can use a router that supports UPnP for automatic port forwarding. To use UPnP, you must enable in on your camera and your router and configure them (*Pic. 6.24*).

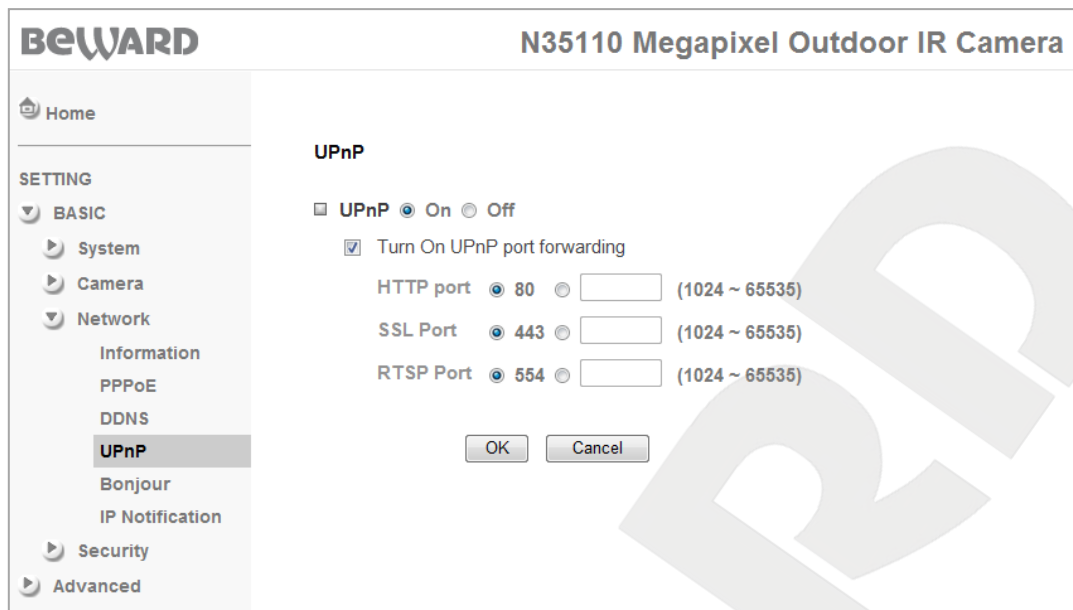
NOTE:

To use UPnP, your router must support it.

HTTP port: enter the HTTP port number that you want to use to access the camera over the Internet. For example, the value of the port you assigned is 10000. In this case, port 80 is used to access the camera over a local network and port 10000 is used to access the camera over the Internet. The default value is 80.

SSL port: enter the SSL port number that you want to use to access the camera through an HTTPS secure connection over the Internet. The default value is 443.

RTSP (MPEG-4) port: enter the RTSP port number that you want to use to access the camera over the Internet. The default value is 554.



Pic. 6.24

NOTE:

See your router's user manual for details on how to enable and configure the UPnP.

IMPORTANT:

Some routers do not support UPnP forwarding between LAN and WAN networks. Before configuring, make sure your router supports this option.

IMPORTANT:

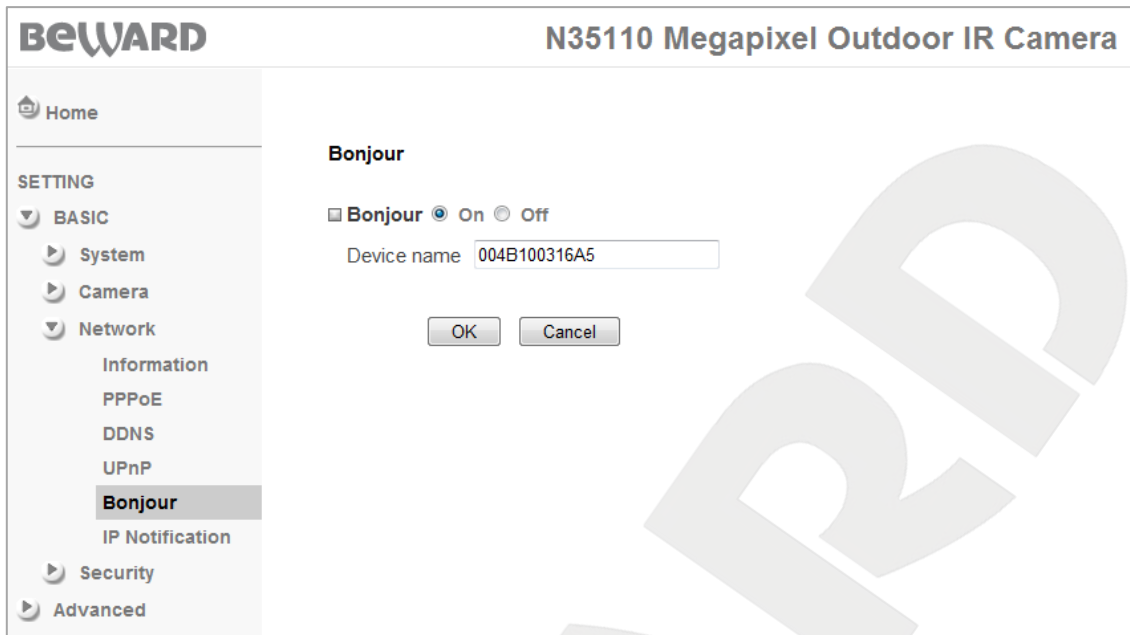
You must reboot the camera for the changes to take effect.. To do so, go to **SETTING – Basic – System – Initialize**.

6.3.5. Bonjour

This menu allows you to enable Bonjour. If this option is enabled, it allows the camera to be automatically discovered using Bonjour (*Pic. 6.25*).

NOTE:

Bonjour provides a general method to discover services on a local area network. The software is widely used throughout Mac OS X, and allows users to set up a network without any configuration.



Puc. 6.25

Device name: enter a name for identifying the camera on a network.

NOTE:

For detailed information about using Bonjour for OS Windows, go to www.apple.com.

6.3.6. IP notification

This menu provides options for configuring the camera to send an e-mail message when the network settings change (*Pic. 6.26*).

Pic. 6.26

Select the option for **[On]** and click **OK** to enable this function. After you save the changes, the following settings will be available:

Notify type: you can choose to be notified of the change of: **[DHCP]**, **[Static IP]**, or **[PPPoE]**.

If any of these items is selected, the camera will send an e-mail message containing the text of the **[Message]** box to the predefined e-mail address.

SMTP server name: enter the IP address or hostname of the SMTP server (64 characters maximum).

SMTP server port: enter the port number of the SMTP server. The default value is 25.

SSL: check this box if your provider requires SSL communications.

Authentication: choose the appropriate authentication type.

- **Off:** no authentication is required.
- **On:** authentication is required. You can choose **[SMTP]** or **[POP before SMTP]**.

POP server name: this item appears when the **[POP before SMTP]** option is selected. The POP server name is required for the authorization (64 characters maximum).

User name: enter the username to access the mail server (64 characters maximum).

Password: enter the password to access the mail server (64 characters maximum).

Recipient e-mail address: enter an e-mail address to which alert e-mail messages are sent (64 characters maximum). Multiple addresses (3 addresses maximum) are separated by semicolons **[;]**.

Administrator e-mail address: enter the sender's e-mail address (64 characters maximum).

Subject: enter the text to be shown in the “**Subject**” field for alert e-mail messages (64 characters maximum).

Message: specify your own text to include in alert e-mail messages (384 characters maximum).

By default, the e-mail message includes the following information: IP address <ip>, port <port>, MAC address <mac>, camera model <product>, firmware version <vfirm>, and web UI version <vweb>.

6.4. Security

This menu is divided into the following sections: **[Account]**, **[HTTPS]**, and **[IP filter]** (Pic. 6.27).



Pic. 6.27

6.4.1. Account

This menu provides options for managing user privileges, adding new user accounts with different privileges.

The camera has the built-in administrator account and its username and password are «**admin / admin**». This is a main user account and you cannot change its privileges but you can change its username and password. Besides, the Administrator can add up to 9 user accounts with different privileges (Pic. 6.28).

Account

User ID	User name	Password	Re-type Password	Viewer mode
Administrator	admin	*****	*****	Admin
User 1				Admin
User 2				Admin
User 3				Admin
User 4				Admin
User 5				Admin
User 6				Admin
User 7				Admin
User 8				Admin
User 9				Admin

Viewer authentication On Off Admin

OK Cancel

Pic. 6.28

User name: enter a name for the user (5-16 characters).

Password: enter a password for the user (5-16 characters). User can set a blank password.

Re-type Password: re-enter the password to ensure that there are no typing mistakes. If you re-type the password incorrectly, the camera displays an error message.

IMPORTANT:

The username and password may contain only Latin letters and numbers.

Viewer mode: select the privilege level for the user. There are three types of users:

- **Admin:** can access the configuration windows for the camera.
- **Operator:** can see live images and adjust image parameters. An Operator can access the **[Client setting]** and **[Image setup]** menu.
- **Viewer:** can only see live images. A Viewer can access only **[Client setting]** menu.

Viewer authentication: turn on or off user authorization to access the camera.

- **On:** when this option is selected, the user must enter the username and password to access the camera.
- **Off:** when this option is selected, the user must not enter the username and password to access the camera. A user may specify one of the following viewer modes: Admin, Operator, and Viewer.

When your account does not have sufficient permissions to access a menu, an authorization window will appear prompting you to login as an account that has the sufficient privileges.

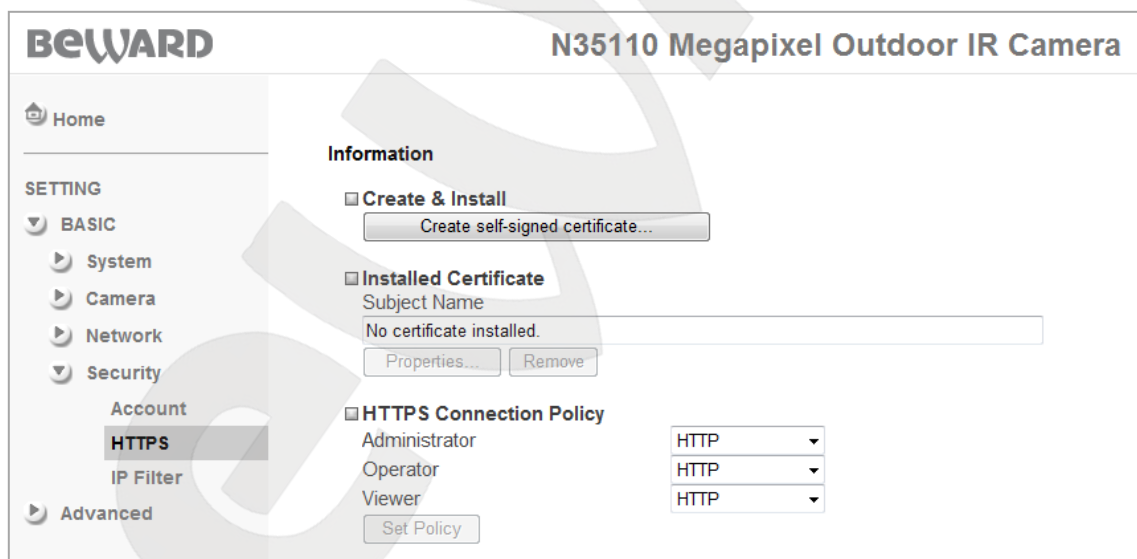
To add a new user or edit the existing one, enter or edit the required information. Click **[OK]** to save changes.

NOTE:

It is recommended to change the default username and password to help preserve privacy of the camera's image and secure the camera's parameters.

6.4.2. HTTPS

This menu provides options for configuring access to the camera not only through an HTTP connection (the camera's address resembles `http://<IP>/`), but also through an HTTPS secure connection (the camera's address resembles `https://<IP>/`) using the port 443, which extends the security of your data compared to the password protection. You can specify a connection policy for each viewer mode. For example, you can choose the HTTP connection for the Viewer mode and the HTTPS connection for the Administrator mode (*Pic. 6.29*).



Pic. 6.29

Create & Install: create and install a certificate for a secure HTTPS connection.

Installed Certificate: displays the installed certificate and allows you to delete it.

HTTPS Connection Policy: specify a connection policy for each viewer mode.

To create a secure HTTPS connection, you need to create a certificate first. Click the **[Create self-signed certificate...]** to create a certificate (*Pic. 6.30*).



Pic. 6.30

The **[Create self-signed certificate...]** will open. Complete all the fields and then click **[OK]** to save the certificate. Click the **[Properties]** button to view the certificate properties.

IMPORTANT:

When using an HTTPS connection, it secures only the parameters transferred between the computer and the camera but the video and audio streams are not secured.

6.4.3. IP Filter

The “**IP Filter**” function provides options for controlling access to the camera by designating a list of IP addresses that can access the camera and a list of IP addresses that cannot access the camera. This restriction is applicable only for the “**Operator**” and “**Viewer**” viewer mode and extends the security of your data (Pic. 6.31).

The screenshot shows the 'IP Filter' configuration page for the BEWARD N35110 Megapixel Outdoor IR Camera. The interface includes a sidebar with navigation options: Home, BASIC, System, Camera, Network, Security, Account, HTTPS, IP Filter (selected), and Advanced. The main content area is titled 'IP Filter' and contains the following sections:

- IP Filter:** A checkbox labeled 'IP Filter' is checked, with radio buttons for 'On' (selected) and 'Off'.
- Allow Range:** A checkbox labeled 'Allow Range' is checked. Below it are two rows of IP address input fields (Start IP Address and End IP Address) and an 'Add' button.
- Allow Range List:** A checkbox labeled 'Allow Range List' is checked. Below it is a dropdown menu showing '(Empty)' and a 'Delete' button.
- Deny Range:** A checkbox labeled 'Deny Range' is checked. Below it are two rows of IP address input fields (Start IP Address and End IP Address) and an 'Add' button.
- Deny Range List:** A checkbox labeled 'Deny Range List' is checked. Below it is a dropdown menu showing '(Empty)' and a 'Delete' button.

At the bottom of the page, there are 'OK' and 'Cancel' buttons.

Puc. 6.31

Allow range: a range of IP addresses that can access the IP camera.

Start IP address: type the start IP address of the allowed IP range.

End IP address: type the end IP address of the IP allowed range.

To set a range of allowed IP addresses, enter the IP addresses in “**Start IP address**” and “**End IP address**” and click the **[Add]** button, to delete a range of allowed IP addresses, click the **[Delete]** button.

Allow range list: a list of IP addresses that can access the IP camera.

Deny range: a range of IP addresses that cannot access the IP camera.

Start IP address: type the start IP address of the denied IP range.

End IP address: type the end IP address of the denied IP range.

To set a range of denied IP addresses, enter the IP addresses in “**Start IP address**” and “**End IP address**” and click the **[Add]** button, to delete a range of denied IP addresses, click the **[Delete]** button.

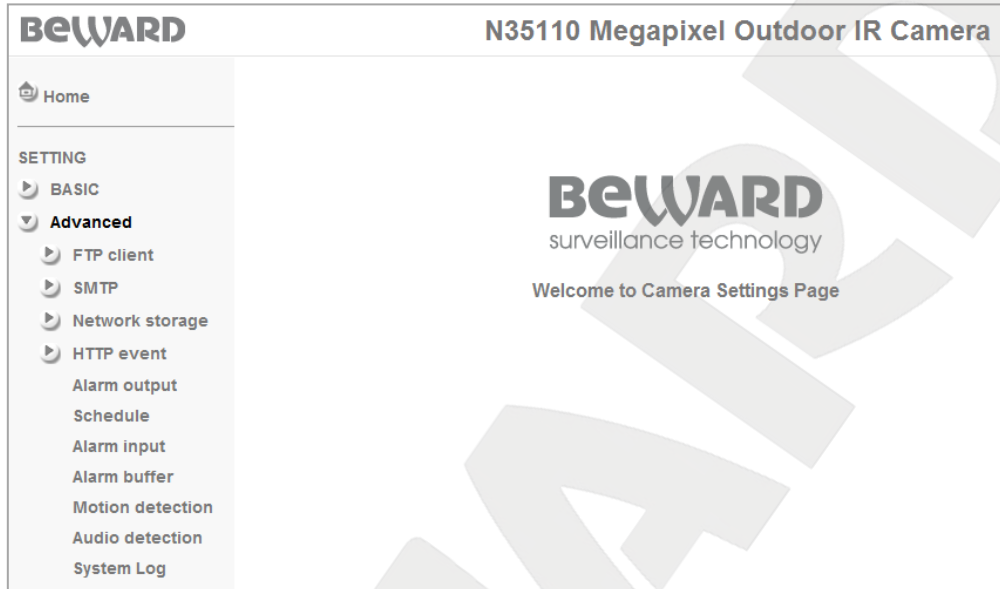
Deny range list: a list of IP addresses that cannot access the IP camera.

IMPORTANT:

The IP address restriction is applicable only to the “**Operator**” and “**Viewer**” viewer mode and not applicable to the “**Admin**” viewer mode.

Chapter 7. SETTING: Advanced

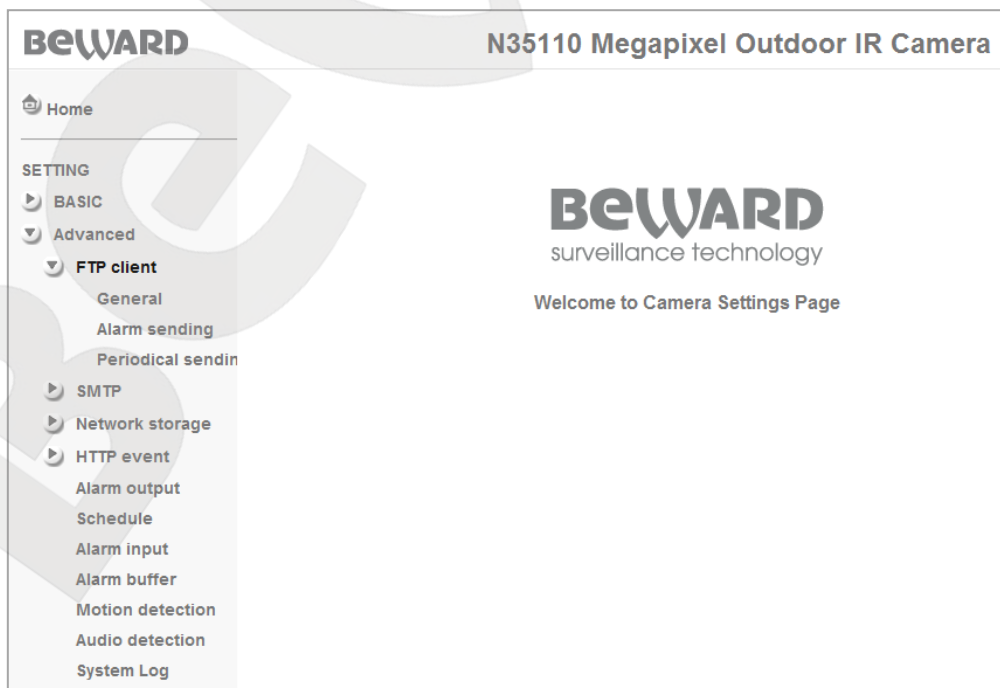
This menu is divided into the following sections: **[FTP client]**, **[SMTP]**, **[Network storage]**, **[HTTP event]**, **[Alarm output]**, **[Schedule]**, **[Alarm input]**, **[Alarm buffer]**, **[Motion detection]**, **[Audio detection]**, and **[System log]** (Pic. 7.1).



Pic. 7.1

7.1. FTP Client

This menu provides options for configuring file upload to an FTP server. When this option is enabled, event files can be uploaded within a designated schedule, during the specified times or when an event occurs (Pic.7.2).



Pic.7.2

7.1.1. General

This menu allows you to configure the FTP client (Pic. 7.3).

Pic. 7.3

Select the option for **[On]** to enable the FTP client or select the option for **[Off]** to disable it.

FTP server name: enter the IP address or hostname of the FTP server (64 characters maximum).

User name: enter the username to access the FTP server.

Password: enter the password to access the FTP server.

Re-type password: re-type the entered password to ensure that there are no typing mistakes.

Passive mode: select the option for **[On]** to enable the passive mode feature or select the option for **[Off]** to use the active mode.

Attached file type: select a file type you want to upload to the FTP. The following options are available:

- **Snapshot:** select this option to upload snapshot images.
- **Video clip:** select this option to upload video files.

IMPORTANT:

To playback recorded video, use the integrated player at **SETTING – Basic - Camera – Playback**, otherwise you may need to install third party software, e.g. VLC media player. Its official website is <http://www.videolan.org/vlc/>.

[Test]: click this button to check the server availability, the specified parameters and upload a test file.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.1.2. Alarm Sending

This menu provides options for configuring event-triggered file upload to FTP, for example, when motion or noise is detected or the alarm input changes its state as configured. Select the option for **[On]** to enable this option (*Pic. 7.4*).

Pic. 7.4

Remote path: specify the path to the FTP upload folder (64 characters maximum) for the event files. For example, ipcam/example.

Image file name: enter a name of the files that are uploaded to the FTP.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.

- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the **[Clear]** button to reset the sequence number anytime. When user clicks the **[Clear]** button it resets the sequence number and starts it from 000001.

Alarm: choose the desired options to designate the events that trigger the camera to upload files to FTP:

- **Motion detection:** the camera uploads files to FTP when motion is detected. To configure this option, click the **[Motion detection]** button (appears if the **[Motion detection]** box is checked) or go to **SETTING – Advanced – Motion detection**. See [paragraph 7.9](#) for details.
- **Audio detection:** the camera uploads files to FTP when noise is detected. To configure this option, click the **[Audio detection]** button (appears if the **[Audio detection]** box is checked) or go to **SETTING – Advanced – Audio detection**. See [paragraph 7.10](#) for details.

IMPORTANT:

When motion or noise is detected, the video files are sent with an interval of 10-20 seconds between them. The length of the video files is 5 seconds but the maximum size is 2 MB. When sending snapshot images, the camera sends 3 pre-event images, 3 post-event images and 1 image captured at the moment of the event. The pre-event and post-event images are sent with an interval of 1 image per 1-2 seconds and the groups of images are sent with an interval of 8-10 seconds between them.

- **Network link down:** the camera starts uploading files to FTP when the network link is down. When the connection is lost, the camera saves the records made before (the record length is specified in the “**Pre-alarm period**” menu) and after (the record length is specified in the “**Post-alarm period**” menu) the connection is lost to the alarm buffer.

After the connection is up, the camera uploads these files to FTP. If “**Video clip**” is selected in the “**Attached file type**” menu, the camera sends two files (pre- and post-event video). If “**Snapshot**” is selected in the “**Attached file type**” menu, the camera sends 1 image captured at the moment of the event, 3 pre-event images and 3 post-event images.

To configure this option, click the **[Alarm buffer]** button (appears if the **[Network link down]** box is checked) or go to **SETTING – Advanced – Alarm buffer**. See [paragraph 7.8](#) for details.

NOTE:

The maximum length of the records that are uploaded to FTP is 5 seconds. However, the maximum record size is 2 MB. Therefore, the length of the records may be less than 5 seconds even if the user specifies the value of 5 seconds in the **[Alarm buffer]** menu.

IMPORTANT:

When you configuring this menu, be aware that these parameters are applied to the other camera functions, for example to recording to network storage, FTP, etc.

IMPORTANT:

When using the **[Alarm buffer]** function, the camera sends the video that was captured before the connection was lost (use the “**Pre-alarm period**” option to specify the video length) and after the connection is lost (use the “**Post-alarm period**” option to specify the video length). To specify the length of the pre- and post-event video, you can also use the menu **SETTING – Advanced – Alarm buffer** (see [paragraph 7.8](#)).

- **Alarm input:** the camera starts uploading files to FTP when the alarm input changes its state as configured in the “**Trigger condition**” in the “**Alarm input**” menu. To configure this option, click the **[Alarm input]** button (appears if the **[Alarm input]** box is checked) or go to **SETTING – Advanced – Alarm input**. See [paragraph 7.7](#) for details.

Effective period: set a period for which the camera can upload files to FTP. The following options are available:

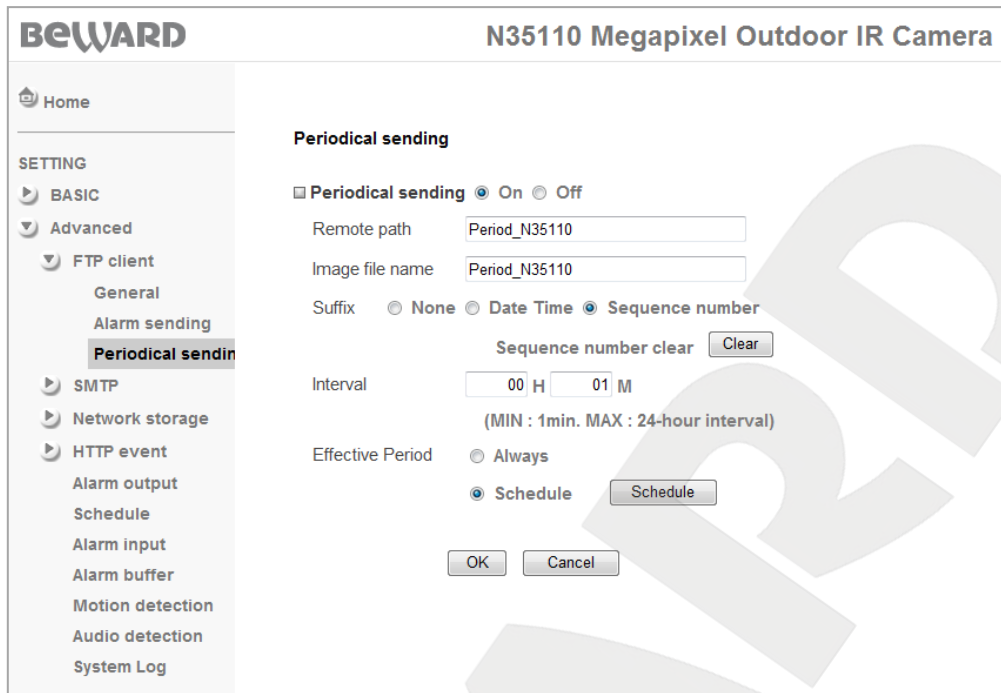
- **Always:** the camera can upload files any time.
- **Schedule:** select this option to configure the camera to upload files within a designated schedule. To configure this option, click the **[Schedule]** button (appears if the **[Schedule]** box is checked) or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for details

NOTE:

Click **[OK]** to save changes. Otherwise, the changes may not be saved.

7.1.3. Periodical Sending

This menu provides options to configure the camera to upload files to FTP within designated intervals. Select the option for **[On]** to enable this option (*Pic. 7.5*).



Pic. 7.5

Remote path: specify the path to the FTP upload folder (64 characters maximum) for the event files. For example, ipcam/example.

Image file name: enter a name of the files that are uploaded to the FTP.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **None:** suffix is not added to the file name.
- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.
- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the **[Clear]** button to reset the sequence number anytime. When user clicks the **[Clear]** button it resets the sequence number and starts it from 000001.

Interval: choose the amount of time to upload files at a certain frequency. The minimum amount of time is 1 minute; the maximum amount of time is 24 hours.

IMPORTANT:

The maximum length of the video file that is uploaded to FTP is 5 seconds.

Effective period: set a period for which the camera can upload files to FTP. The following options are available:

- **Always:** the camera can upload files any time.
- **Schedule:** select this option to configure the camera to upload files within a designated schedule. To configure this option, click the **[Schedule]** button (appears if the **[Schedule]** box is checked) or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for details

IMPORTANT:

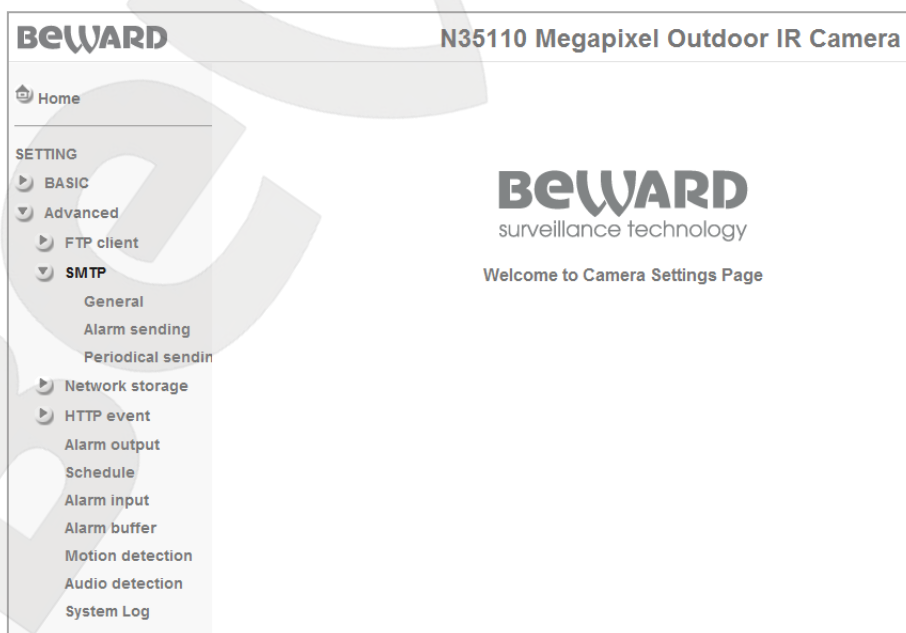
If an alarm-triggered recording started at the time of a periodical recording, the periodical recording and uploading of a file to FTP will start in the next interval of time that is specified in the **[Interval]** menu.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.2. SMTP

This menu provides options for configuring the e-mail alert. A video file or a snapshot image can be included as an attachment to the e-mail message. The e-mail alert can be triggered during the specified times or when an event occurs, such as motion detection or the activation of the alarm input, etc. The menu is divided into the following sections: **[General]**, **[Alarm sending]**, and **[Periodical sending]** (Pic. 7.6).



Pic. 7.6

7.2.1. General

Select the option for **[On]** to enable the e-mail alert or select the option for **[Off]** to disable it (Pic. 7.7).

Pic. 7.7

SMTP server name: enter the IP address or hostname of the SMTP server (64 characters maximum).

SMTP server port: enter the port number of the SMTP server. The default value is 25.

SSL: check this box if your provider requires SSL communications.

Authentication: choose the appropriate authentication type.

- **Off:** no authentication is required.
- **On:** authentication is required. You can choose **[SMTP]** or **[POP before SMTP]**.

POP server name: this item appears when the **[POP before SMTP]** option is selected. The POP server name is required for the authorization (64 characters maximum).

User name: enter the username to access the mail server (64 characters maximum).

Password: enter the password to access the mail server (64 characters maximum).

Recipient e-mail address: enter an e-mail address to which alert e-mail messages are sent (64 characters maximum). Multiple addresses (3 addresses maximum) are separated by semicolons [;].

Administrator e-mail address: enter the sender's e-mail address (64 characters maximum).

Attached file type: select a file type you want to attach to the e-mail. The following options are available:

- **Snapshot:** select this option to attach a snapshot image.
- **Video clip:** select this option to attach a video file.

IMPORTANT:

The maximum length of the video file that is attached to the e-mail is 5 seconds.

IMPORTANT:

To playback recorded video, use the integrated player at **SETTING – Basic – Camera – Playback**, otherwise you may need to install third party software, e.g. VLC media player. Its official website is <http://www.videolan.org/vlc/>.

Subject: enter the text to be shown in the “**Subject**” field for alert e-mail messages (64 characters maximum).

IMPORTANT:

The subject may contain only Latin letters and numbers.

Message: specify your own text to include in alert e-mail messages (384 characters maximum).

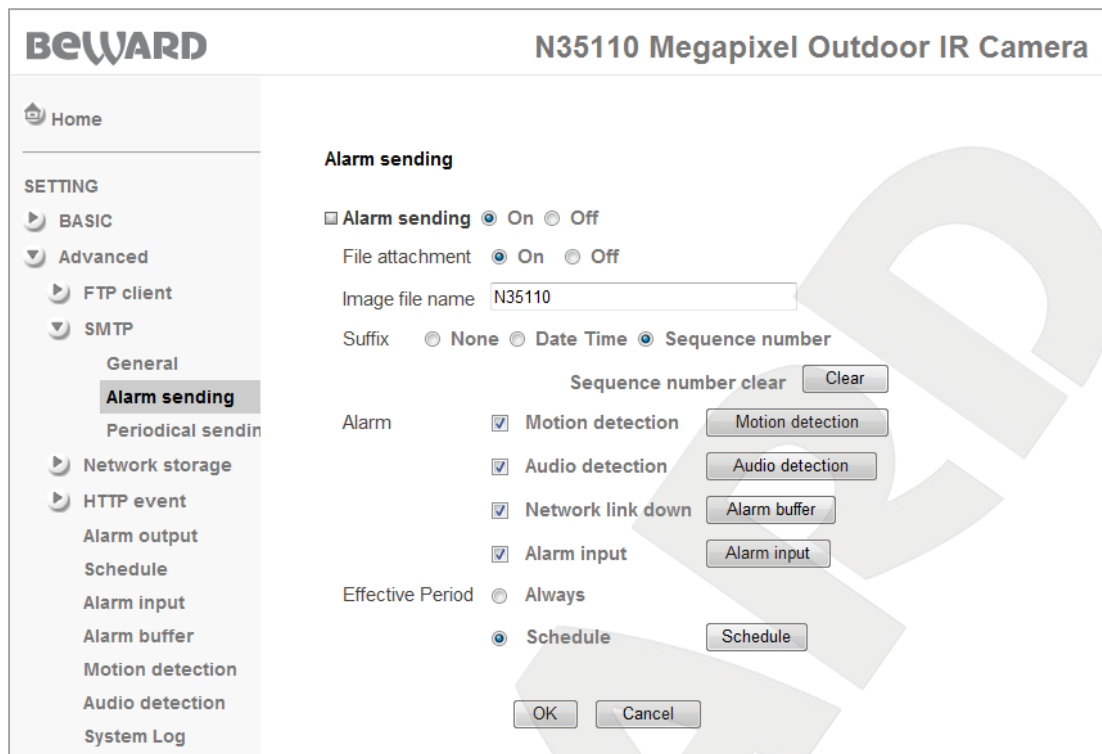
[Test]: test the e-mail alert setup and send a test alert e-mail message by clicking the **[Test]** button.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.2.2. Alarm Sending

This menu provides options for configuring event-triggered e-mail notification. Select the option for **[On]** to enable this option (*Pic. 7.8*).



Pic. 7.8

File attachment: select the option for **[On]** to attach a file to the alert e-mail message.

NOTE:

To select a file type, go to **SETTING – Advanced – SMTP – General**.

Image file name: enter a name of the files that are attached to the alert e-mail messages.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **None:** suffix is not added to the file name.
- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.
- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the **[Clear]** button to reset the sequence number anytime. When user clicks the **[Clear]** button it resets the sequence number and starts it from 000001.

Alarm: choose the desired options to designate the events that trigger the camera to send alert e-mail messages:

- **Motion detection:** the camera sends alert e-mail messages when motion is detected. To configure this option, click the **[Motion detection]** button (appears if the **[Motion detection]** box is checked) or go to **SETTING – Advanced – Motion detection**. See [paragraph 7.9](#) for details.
- **Audio detection:** the camera sends alert e-mail messages when noise is detected. To configure this option, click the **[Audio detection]** button (appears if the **[Audio detection]** box is checked) or go to **SETTING – Advanced – Audio detection**. See [paragraph 7.10](#) for details.

IMPORTANT:

When motion or noise is detected, the video files are sent with an interval of 10-20 seconds between them. The length of the video files is 5 seconds but the maximum size is 2 MB. When sending snapshot images, the camera sends 3 pre-event images, 3 post-event images and 1 image captured at the moment of the event. The pre-event and post-event images are sent with an interval of 1 image per 1-2 seconds and the groups of images are sent with an interval of 8-10 seconds between them.

- **Network link down:** the camera starts sending alert e-mail messages when the network link is down. When the connection is lost, the camera saves the records made before (the record length is specified in the “**Pre-alarm period**” menu) and after (the record length is specified in the “**Post-alarm period**” menu) the connection is lost to the alarm buffer.

After the connection is up, the camera sends these files to the specified e-mail addresses. If “**Video clip**” is selected in the “**Attached file type**” menu, the camera sends two files (pre- and post-event video). If “**Snapshot**” is selected in the “**Attached file type**” menu, the camera sends 1 image captured at the moment of the event, 3 pre-event images and 3 post-event images.

To configure this option, click the **[Alarm buffer]** button (appears if the **[Network link down]** box is checked) or go to **SETTING – Advanced – Alarm buffer**. See [paragraph 7.8](#) for details.

NOTE:

The maximum length of the records that are attached to the alert e-mail is 5 seconds. However, the maximum record size is 2 MB. Therefore, the length of the records may be less than 5 seconds even if the user specifies the value of 5 seconds in the **[Alarm buffer]** menu.

IMPORTANT:

When you configuring this menu, be aware that these parameters are applied to the other camera functions, for example to recording to network storage, FTP, etc.

IMPORTANT:

When using the **[Alarm buffer]** function, the camera sends the video that was captured before the connection was lost (use the “**Pre-alarm period**” option to specify the video length) and after the connection is lost (use the “**Post-alarm period**” option to specify the video length). To specify the length of the pre- and post-event video, you can also use the menu **SETTING – Advanced – Alarm buffer** (see [paragraph 7.8](#)).

- **Alarm input:** the camera starts sending alert e-mails when the alarm input changes its state as configured in the “**Trigger condition**” in the “**Alarm input**” menu. To configure this option, click the **[Alarm input]** button appears if the **[Alarm input]** box is checked) or go to **SETTING – Advanced – Alarm input**. See [paragraph 7.7](#) for details.

Effective period: set a period for which the camera can send alert e-mails when an event occurred. The following options are available:

- **Always:** the camera can send alert e-mails any time.
- **Schedule:** select this option to configure the camera to send alert e-mails within a designated schedule. To configure this option, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for details.

IMPORTANT:

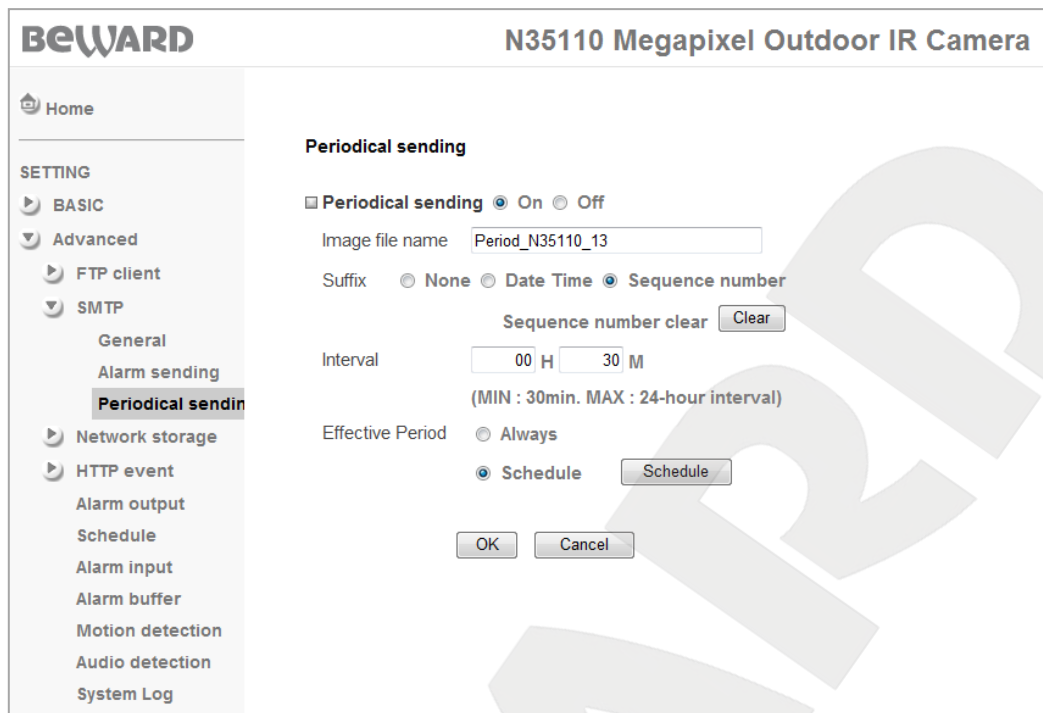
When using the “**Network link down**” option, the total length of the video that is attached to the alert e-mails depends on the length that is specified for pre- and post-event video.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.2.3. Periodical Sending

This menu provides options to configure the camera to send alert e-mails within designated intervals. Select the option for **[On]** to enable this option (*Pic. 7.9*).



Pic. 7.9

Image file name: this name will be used for the files that are attached to the alert e-mails that are sent within a designated schedule.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **None:** suffix is not added to the file name.
- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.
- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the **[Clear]** button to reset the sequence number anytime. When user clicks the **[Clear]** button it resets the sequence number and starts it from 000001.

Interval: choose the amount of time to send the alert e-mails at a certain frequency. The minimum amount of time is 30 minutes; the maximum is 24 hours.

IMPORTANT:

The maximum length of the video file that is attached to the e-mail is 5 seconds.

Effective period: set a period for which the camera can send alert e-mails when an event occurred. The following options are available:

- **Always:** the camera can send alert e-mails any time.
- **Schedule:** select this option to configure the camera to send alert e-mails within a designated schedule. To configure this option, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for details.

IMPORTANT:

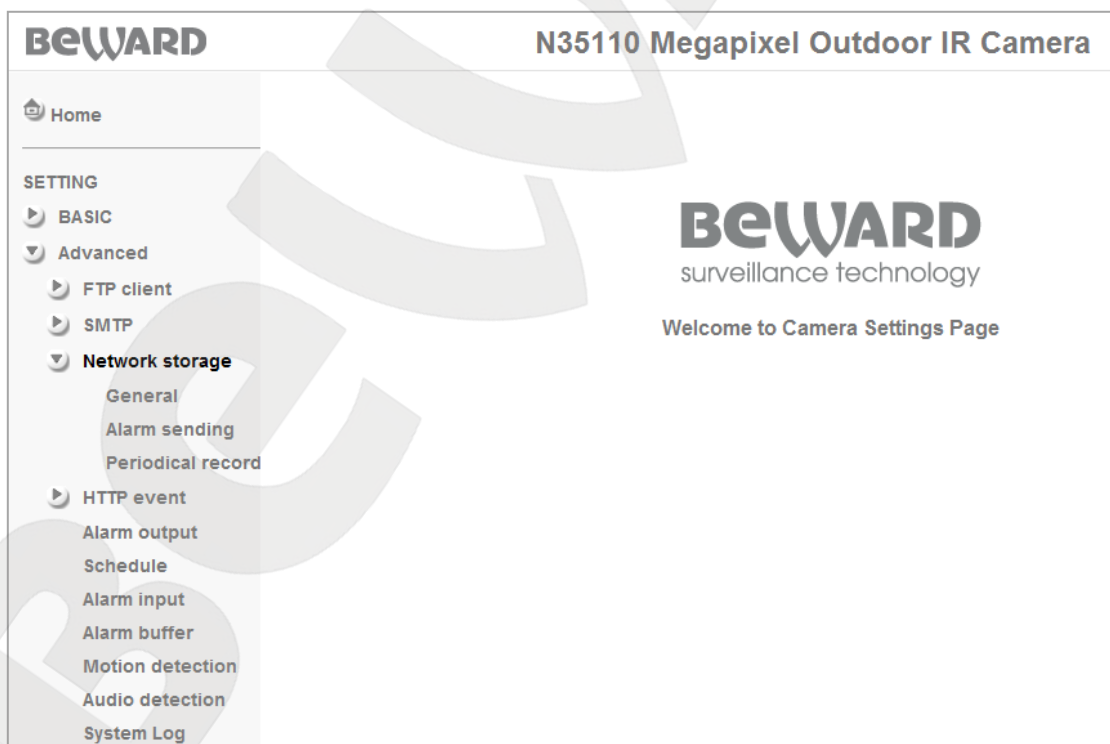
If the camera uploads event files to FTP and sends an alert e-mail at one time, it may skip the e-mail alert because the priority of uploading event files to FTP is higher.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.3. Network Storage

This menu provides options for configuring how the camera records to network attached storage (NAS) or to network shared folder. When this function is enabled, it allows continuous, periodical or alarm-triggered recording (*Pic. 7.10*).



Pic. 7.10

7.3.1. General

Select the option for **[On]** to enable the option for recording to network attached storage or select the option for **[Off]** to disable it (Pic. 7.11).

The screenshot shows the 'General' settings for network storage. The 'Network storage' checkbox is checked and set to 'On'. The 'Protocol' is set to 'Windows network (SMB/CIFS)'. The 'Network storage location' field contains '\\IPCamera004B100316A5' with a note '(for example: \\my_nas\folder)'. Below are fields for 'Workgroup', 'User name', 'Password', and 'Re-type password'. At the bottom are 'OK', 'Cancel', and 'Test' buttons.

Pic. 7.11

Protocol: select a protocol to access the network attached storage.

- **Windows network (SMB/CIFS):** select this option for Windows network storage (e.g. a Windows network shared folder).
- **Unix network (NFS):** select this option for Unix network shared folder (e.g. Linux OS).

Network storage location: specify the shared folder path. The camera creates a new folder named «IPCamera <MAC address>» at the provided path.

NOTE:

When specifying Windows storage path, note that the path should be in the form of \\NAS_server\Record; for Unix storage, the path should be in the form of NAS_Server:\Record, where “NAS_Server” is the IP address of the network storage or the shared folder.

If you select the Windows network protocol, it is necessary to specify the following parameters as well:

Workgroup: enter your Windows workgroup name. The entered name must match the workgroup name on the computer with the shared folder or the NAS server.

User name: enter the username to access the remote computer (or the NAS server).

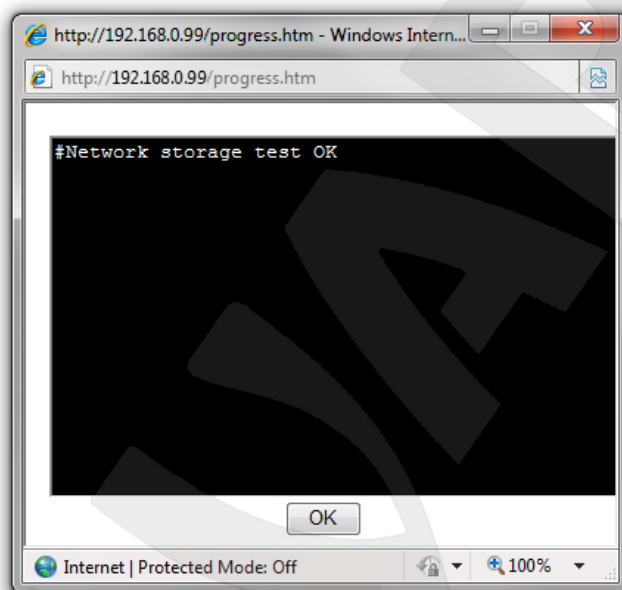
Password: enter the password to access the remote computer (or the NAS server).

Re-type password: re-type the entered password to ensure that there are no typing mistakes.

NOTE:

Make sure you have the permissions to create new folders and files.

After you entered all the information, click the **[Test]** button to check the NAS parameters. If the NAS function is configured correctly and the network storage is available, you will see a confirmation of successful test completion (*Pic. 7.12*).



Pic. 7.12

If the storage check is failed, please check the network storage address, its availability and the account settings.

IMPORTANT:

To playback the recorded video files, use the integrated player at **SETTING – Camera – Playback**, otherwise you may need to install third-party software, e.g. VLC media player. Its official website is <http://www.videolan.org/vlc/>.

NOTE:

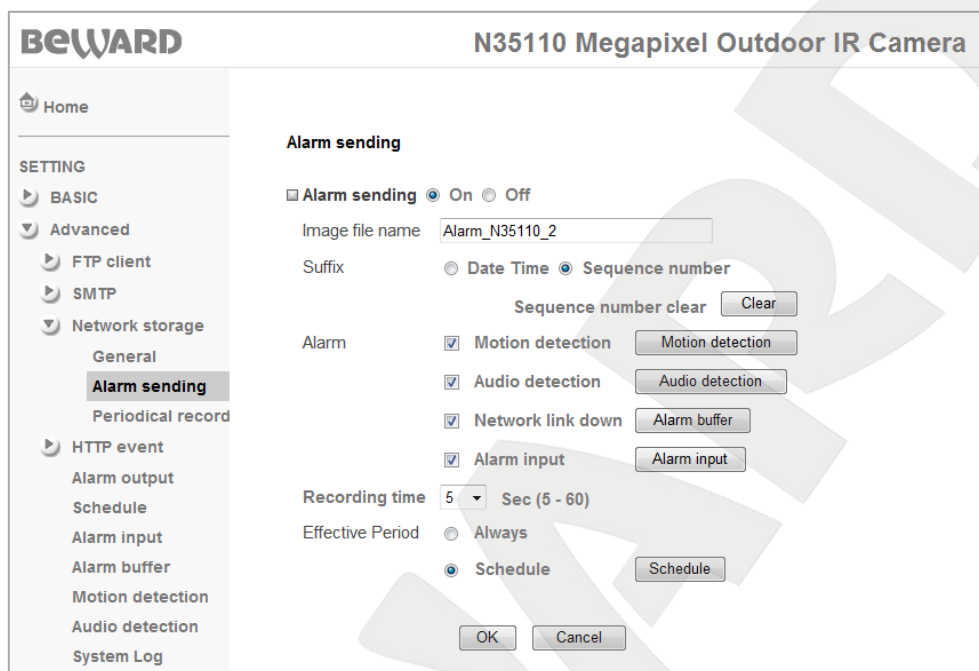
Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.3.2. Alarm Sending

This menu provides options for configuring event-triggered recording to network attached storage, for example the camera detects motion. Select the option for **[On]** (*Pic. 7.13*) to enable this function or select the option for **[Off]** to disable it.

NOTE:

For event-triggered recording, the recorded files are stored in the «Alarm» folder, which is located at the path that is specified in the [Network storage location].



Pic. 7.13

Image file name: enter a file name to save the records to network attached storage.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.
- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the [Clear] button to reset the sequence number anytime. When user clicks the [Clear] button it resets the sequence number and starts it from 000001.

Alarm: choose the desired options to designate the events that trigger the camera to start recording to NAS:

- **Motion detection:** the camera starts recording to NAS when motion is detected. To configure this option, click the [Motion detection] button (appears if the [Motion

detection] box is checked) or go to **SETTING – Advanced – Motion detection**. See [paragraph 7.9](#) for details.

- **Audio detection:** the camera starts recording to NAS when noise is detected. To configure this option, click the **[Audio detection]** button (appears if the **[Audio detection]** box is checked) or go to **SETTING – Advanced – Audio detection**. See [paragraph 7.10](#) for details.

IMPORTANT:

When motion or noise is detected, the length of the records that camera sends to NAS depends on the value specified in the **[Recording time]** menu.

- **Network link down:** the camera starts recording to NAS when the network link is down. When the connection is lost, the camera saves the records made before (the record length is specified in the “**Pre-alarm period**” menu) and after (the record length is specified in the “**Post-alarm period**” menu) the connection is lost to the alarm buffer.

After the connection is up, the camera sends these records to NAS. To specify the record length, click the **[Alarm buffer]** button (appears if the **[Network link down]** box is checked) or go to **SETTING – Advanced – Alarm buffer**. See [paragraph 7.8](#) for details.

IMPORTANT:

When you configuring this menu, be aware that these parameters are applied to the other camera functions, for example to recording to network storage, FTP, etc.

IMPORTANT:

When using the **[Alarm buffer]** function, the camera sends the video that was captured before the connection was lost (use the “**Pre-alarm period**” option to specify the video length) and after the connection is lost (use the “**Post-alarm period**” option to specify the video length).

NOTE:

The maximum length of the records that are sent to NAS is 5 seconds. However, the maximum record size is 2 MB. Therefore, the length of the records may be less than 5 seconds even if the user specifies the value of 5 seconds in the **[Alarm buffer]** menu.

- **Alarm input:** the camera starts recording to NAS when the alarm input changes its state as configured in the “**Trigger condition**” in the “**Alarm input**” menu. To configure this option, click the **[Alarm input]** button (appears if the **[Alarm input]** box is checked) or go to **SETTING – Advanced – Alarm input**. See [paragraph 7.7](#) for details.

Recording time: the length of the records, applies to all the designated events in this menu. This parameter determines the length of the video (from 5 to 60 seconds) recorded after the event occurred. The camera records in AVI format.

Effective period: set a period for which the camera can record to NAS when an event occurred. The following options are available:

- **Always:** the camera can record to NAS any time.
- **Schedule:** select this option to configure the camera to record to NAS within a designated schedule. To do so, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. See [paragraph 7.6](#) for details.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

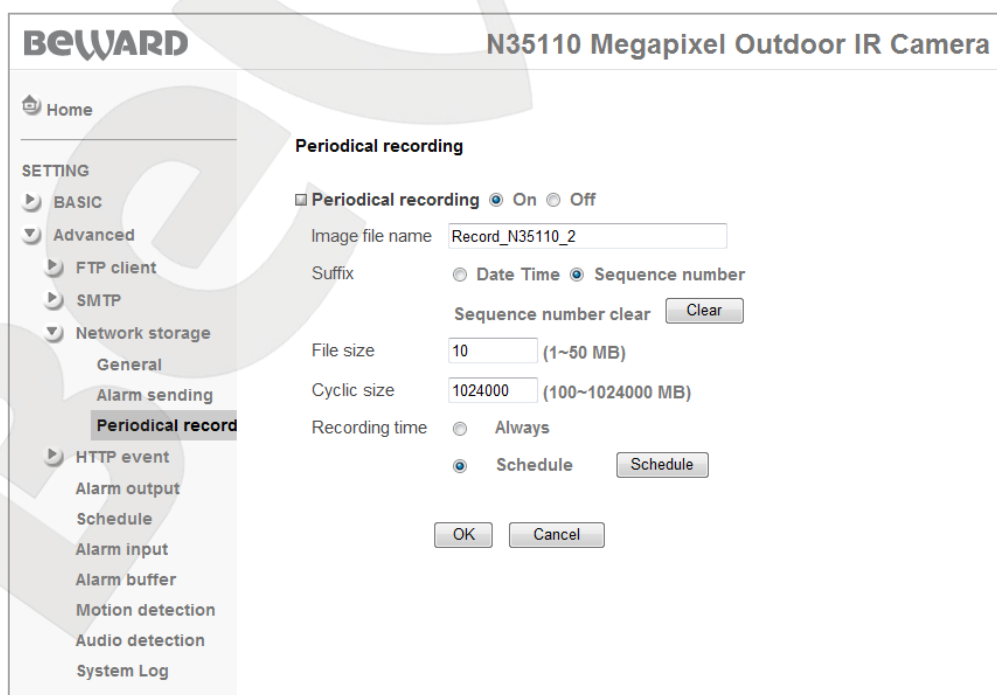
7.3.3. Periodical Recording

This menu provides options to configure the camera to record to shared folder or NAS within designated intervals.

Select the option for **[On]** to enable this option (*Pic. 7.14*) or select the option for **[Off]** to disable it.

NOTE:

For scheduled recording, the recorded files are stored in the “**Period**” folder, which is located at the path that is specified in the **[Network storage location]**.



Pic. 7.14

Image file name: enter a file name to save the records to network attached storage.

NOTE:

The file name may contain only Latin letters, reserved characters and numbers with no spaces in its name.

Suffix: select a suffix to add it to the file name. The following options are available:

- **Date Time:** adds the date and time that correspond to the date and time the file was created. This suffix contains the year as 4 digits, the month as 2 digits, the day as 2 digits, the hour as 2 digits, the minute as 2 digits, the second as 2 digits. Totally, this adds a fourteen-digit suffix to the file name.
- **Sequence number:** adds a six-digit sequence number to the file name. The sequence number starts from 000001 and increases in increments of 1. User can click the **[Clear]** button to reset the sequence number anytime. When user clicks the **[Clear]** button it resets the sequence number and starts it from 000001.

File size: specify the size (from 1 to 50 MB) of the files recorded to NAS. The camera records in AVI format.

Cyclic size: specify the disk space on the NAS or the shared folder. The size is from 100 MB to 1 TB. After the specified disk space is full, the oldest files are overwritten with the new ones.

NOTE:

When the maximum archive size is reached, it automatically overwrites the oldest files. However, the new files may be written with a time delay, which includes a total time required for deleting the old files and recording the new ones.

IMPORTANT:

If an alarm-triggered recording started at the time of a periodical recording, the periodical recording will be stopped and will re-start only after the alarm-triggered recording ends.

Recording time: set a period for periodical recording to NAS. The following options are available:

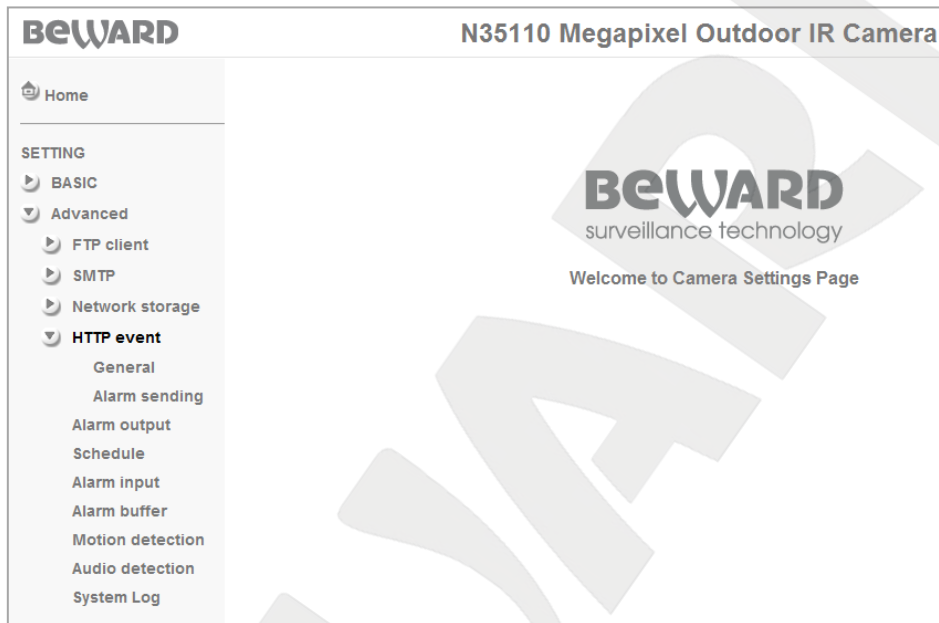
- **Always:** the camera can record to NAS any time.
- **Schedule:** select this option to configure the camera to record to NAS within a designated schedule. To configure this option, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. For related information, see [paragraph 7.6](#).

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.4. HTTP Event

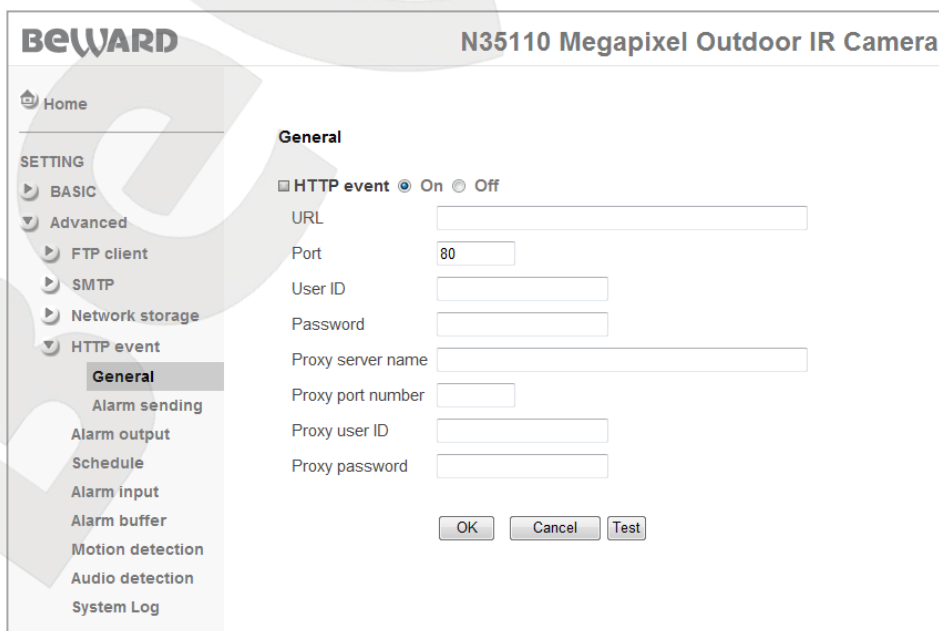
This menu provides options for configuring the sending of HTTP (CGI) requests to an external alarm device. This device, in turn, either sends a request to another alarm device or activates the alarm relay. For example, the camera sends an HTTP (CGI) request to the alarm device, which, in turn, closes the alarm relay contacts and generates an alarm. The menu is divided into two sections: **[General]** and **[Alarm sending]** (Pic. 7.15).



Pic. 7.15

7.4.1. General

This menu provides options for configuring access to an external alarm device (Pic. 7.16).



Pic. 7.16

URL: enter an IP address and a command prefix (64 characters maximum). For example, 192.168.1.7/cgi-bin/operator/ptzset.

NOTE:

You must enter the IP address of the device that handles CGI requests.

Port: enter a port number that is used for HTTP connections to the device. The default port is 80.

User ID: enter a username to access the device (64 characters maximum).

Password: enter a password to access the device (32 characters maximum).

Proxy server name: if you use a proxy server, enter its hostname or IP address (64 characters maximum).

Proxy port number: if you use a proxy server, enter its port number.

Proxy user ID: if you use a proxy server, enter a username to access it (64 characters maximum).

Proxy password: if you use a proxy server, enter a password to access it (32 characters maximum).

[Test] button: click this button to check the validity of the entered parameters and the connectivity. The test status window will open.

NOTE:

Click **[OK]** to save changes. Otherwise, the changes will not be saved.

7.4.2. Alarm Sending

This menu allows you to configure the sending of requests to an external alarm device when an event has occurred. Select the option for **[On]** to enable this feature (*Pic. 7.17*).

Pic. 7.17

Alarm: choose the desired options to designate the events that trigger an external device:

Motion detection: the external device is triggered when the camera detects motion. To configure this option, click the **[Motion detection]** button (appears if the **[Motion detection]** box is checked) or go to **SETTING – Advanced – Motion detection**. For related information, see [paragraph 7.9](#).

- **Parameter:** specify a CGI script (Go to **SETTING – Advanced – HTTP event– General** to set an IP address).
- **Message:** specify a request type. This option may be unavailable for some external devices.

Audio detection: the external device is triggered when the camera detects noise. To configure this option, click the **[Audio detection]** button (appears if the **[Audio detection]** box is checked) or go to **SETTING – Advanced – Audio detection**. For related information, see [paragraph 7.10](#).

- **Parameter:** specify a CGI script (Go to **SETTING – Advanced – HTTP event– General** to set an IP address).
- **Message:** specify a request type. This option may be unavailable for some external devices.

Network link down: activates the sending of images or video when the network link is down. When the connection is lost, the camera saves files to the alarm buffer. To configure the alarm buffer option, go to **SETTING – Advanced – Alarm buffer**. For related information, see [paragraph 7.8](#).

- **Parameter:** specify a CGI script (Go to **SETTING – Advanced – HTTP event– General** to set an IP address).
- **Message:** specify a request type. This option may be unavailable for some external alarm devices.

Alarm input: the external device is triggered when the alarm input changes its state as configured in the “**Trigger condition**” in the “**Alarm input**” menu . To configure this option, click the **[Alarm input]** button (appears if the **[Alarm input]** box is checked) or go to **SETTING – Advanced – Alarm input**. For related information, see [paragraph 7.7](#).

- **Parameter:** specify a CGI script (Go to **SETTING – Advanced – HTTP event – General** to set an IP address).
- **Message:** specify a request type. This option may be unavailable for some external alarm devices.

Effective period: set a period for which the external device can be activated. The following options are available:

- **Always:** the external device can be activated any time.
- **Schedule:** select this option to activate the external device within a designated schedule. To configure this option, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. For related information, see [paragraph 7.6](#).

7.5. Alarm Output

This section provides options for configuring the camera alarm output and external alarm devices to work together.

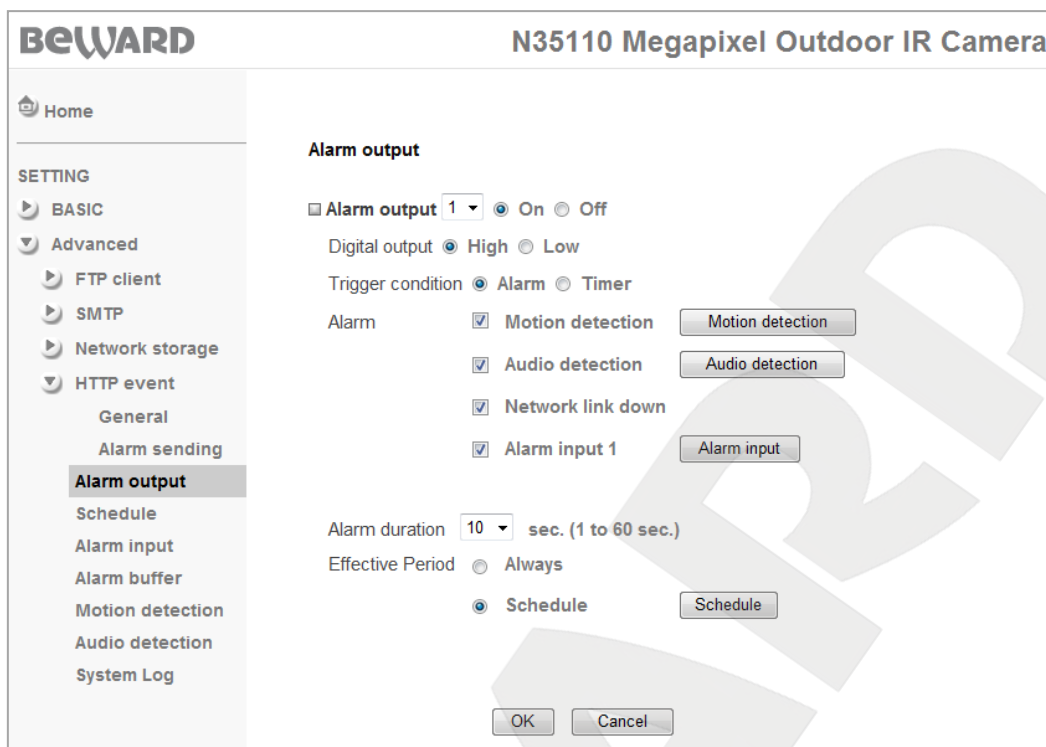
NOTE:

If you use external alarm devices, be aware that that the camera has logical I/O and exceeding the rated voltage and current (max 30 W and 12 V) is PROHIBITED!

IMPORTANT:

Please refer to the N35110 Installation User Manual before using the alarm input/output.

Select the option for **[On]** to enable the alarm output or select the option for **[Off]** to disable it (*Pic. 7.18*).



Pic. 7.18

Digital output: choose a voltage level at the camera alarm output:

- **High:** the alarm output is activated when the voltage level increases from 0 to 12 V.
- **Low:** the alarm output is activated when the voltage level decreases from 12 to 0 V.

Trigger condition: select a trigger that activates the alarm output.

Select the option for **[Alarm]** to activate the alarm output when an event has occurred.

Select the option for **[Timer]** to activate the alarm output according to the specified schedule. The time for which the alarm output is active depends on the specified time frames. When the **[Timer]** is selected, the **[Schedule]** button is available and allows you to specify the time frames.

Alarm: choose the desired options to designate the events that activate the alarm output:

- **Motion detection:** the alarm output is activated when the camera detects motion. To configure this option, click the **[Motion detection]** button (appears if the **[Motion detection]** box is checked) or go to **SETTING – Advanced – Motion detection**. For related information, see [paragraph 7.9](#).
- **Audio detection:** the alarm output is activated when the camera detects noise. To configure this option, click the **[Audio detection]** button (appears if the **[Audio detection]** box is checked) or go to **SETTING – Advanced – Audio detection**. For related information, see [paragraph 7.10](#).
- **Network link down:** the alarm output is activated once the connection is lost. To configure this option, go to **SETTING – Advanced – Alarm buffer**. For related information, see [paragraph 7.8](#).

- **Alarm input:** the alarm output is activated when the camera's alarm input is triggered. To configure this option, click the **[Alarm input]** button (appears if the **[Alarm input]** box is checked) or go to **SETTING – Advanced – Alarm input**. For related information, see [paragraph 7.7](#).

Alarm duration: set the duration of the alarm output state as configured in the **[Digital output]**.

Effective period: set a period for which the alarm output can be activated. The following options are available:

- **Always:** the alarm output can be activated any time.
- **Schedule:** select this option for the scheduled activation. To configure this option, click the **[Schedule]** button or go to **SETTING – Advanced – Schedule**. For related information, see [paragraph 7.6](#).

NOTE:

Once an event has occurred, the alarm output will be active during the time specified in the **[Alarm duration]**.

7.6. Schedule

This menu allows you to designate a schedule for the functions mentioned above. You can create a different schedule for each day of the week or apply it for a whole week by checking the **[Use the same time schedule every day]** box (*Pic. 7.19*).

The screenshot shows the 'Schedule' configuration page for the BEWARD N35110 Megapixel Outdoor IR Camera. The interface includes a sidebar menu on the left with 'Schedule' highlighted. The main content area is titled 'Schedule' and contains the following elements:

- Schedule selection:** A dropdown menu currently set to 'FTP - Alarm'.
- Start time:** 00 : 00
- End time:** 24 : 00
- Weekly Schedule:** A grid for days of the week (Mon-Sun). Each day has a dropdown menu (all currently set to '(Empty)') and 'Add' and 'Delete' buttons. A blue bar at the bottom of the grid indicates the active time period from 0 to 12 hours.
- Use the same time schedule every day:** A checked checkbox.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Pic. 7.19

Schedule selection: designate a schedule for a certain configured action. The following actions are available: **[FTP – Alarm]**, **[FTP – Periodical]**, **[E-mail (SMTP) – Alarm]**, **[E-mail (SMTP) – Periodical]**, **[Record – Alarm]**, **[Record – Periodical]**, **[Alarm output – Alarm]**, **[Alarm output – Timer]**, **[HTTP event– Alarm]**, **[IR schedule]**.

Start time, End time: choose the start time and the end time of the schedule. Use the first field to select an hour (00 to 23/24); use the second field to select a minute (00 to 55 in increments of 5).

Days of the week area: the following options are available for each day of the week:

- **Time frame:** a drop-down list containing the time frames that were specified for the schedule for each day of the week. If no time frame is specified, the drop-down list will be empty.
- **[Add] button:** adds the schedule that is defined in the **[Start time]** and **[End time]** fields.
- **[Delete] button:** clears the values that are in the **[Time frame]** field.

For user's convenience, the intervals appear as a scale, where blue color indicates that no time frame is set for this period and red color shows the specified time frames.

NOTE:

You can add up to 5 schedules for each day of the week.

Use the same time schedule every day: applies the schedule that was added for Monday to the whole week.

NOTE:

Click **[OK]** to save the current schedule.

7.7. Alarm Input

This menu allows you to define what the camera should do when external sensor is triggered.

NOTE:

If you use external sensors, be aware that the camera has logical I/O and exceeding the rated voltage and current (max 30 W and 12 V) is PROHIBITED!

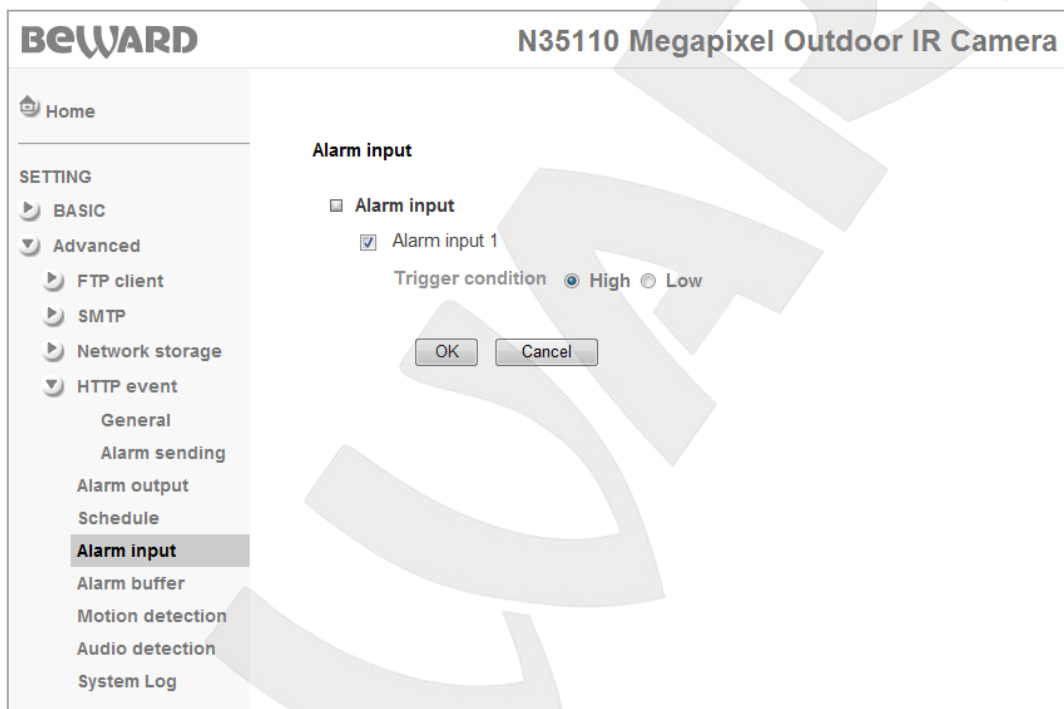
IMPORTANT:

Please refer to the N35110 Installation User Manual before using the alarm input/output.

Check the **[Alarm input]** box to enable the camera's alarm input or uncheck this box to disable it.

Trigger condition: select a voltage level at the camera alarm input:

- **High:** if this option is selected, the camera determines that an event has occurred when a 12 V power source is connected to the input pins, i.e. an alarm is generated when the voltage increases from 0 to 12 V.
- **Low:** if this option is selected, the camera determines that an event has occurred when a 12 V power source is disconnected from the input pins, i.e. an alarm is generated when the voltage decreases from 12 to 0 V.



Pic. 7.20

IMPORTANT:

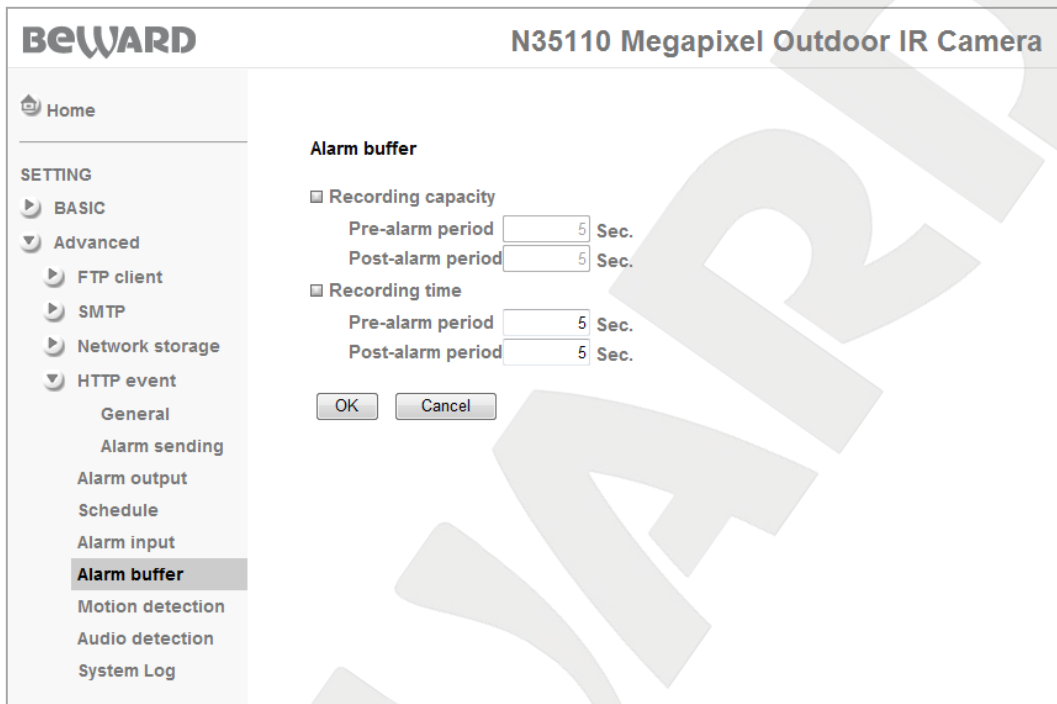
If use the input alarm contacts together with the output alarm contacts, you need to connect them to separate power sources. If the contacts are connected to the same power source, they may work incorrectly. For example, it may cause false triggering.

7.8. Alarm Buffer

This menu provides options for setting the length of the video that was captured when the connection was lost (network link down) to be further uploaded to an FTP server (a network storage) or sent via e-mail.

IMPORTANT:

When using the **[Alarm buffer]** function, the camera sends the video that was captured before the connection was lost (use the “**pre-alarm period**” option to specify the video length) and after the connection is lost (use the “**post-alarm period**” option to specify the video length).



Pic. 7.21

Recording capacity: displays maximum video length.

- **Pre-alarm period:** maximum video length before the connection is lost.
- **Post-alarm period:** maximum video length after the connection is lost.

Recording time: allows you to set the video length.

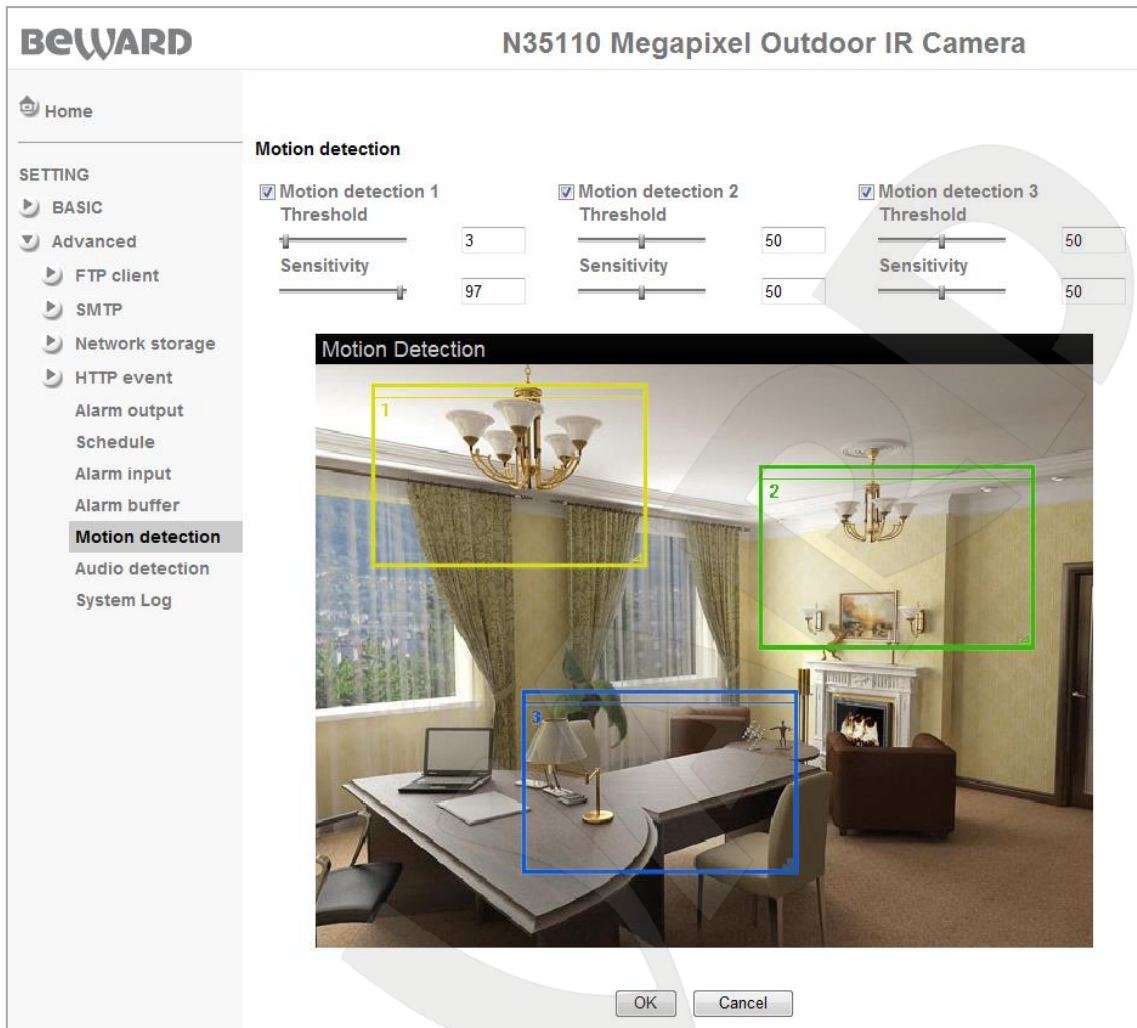
- **Pre-alarm period:** video length before the connection is lost.
- **Post-alarm period:** video length after the connection is lost.

IMPORTANT:

When you configuring this menu, be aware that these parameters are applied to the other camera functions, for example to recording to network storage, FTP, etc.

7.9. Motion Detection

The motion detection menu allows you to configure up to 3 detection areas that may cross each other. Besides, you can configure the threshold and the sensitivity for each of these areas. This saves recording space by triggering an alarm recording only when motion is detected in any of these areas. When the motion detection triggers, the camera creates an alert message or a video file and sends it to e-mail, FTP server, network storage, or over HTTP (*Pic. 7.22*).



Pic. 7.22

Threshold: specify the threshold for each of the areas at which motion detection is triggered. The closer the slider to the right position, the more activity is required to trigger an alarm.

Sensitivity: specify the sensitivity for each of the areas at which motion detection is triggered. The closer the slider to the right position, the more the sensor is sensitive to image changes.

Motion detection 1: check this box to enable this window.

Motion detection 2: check this box to enable this window.

Motion detection 3: check this box to enable this window.

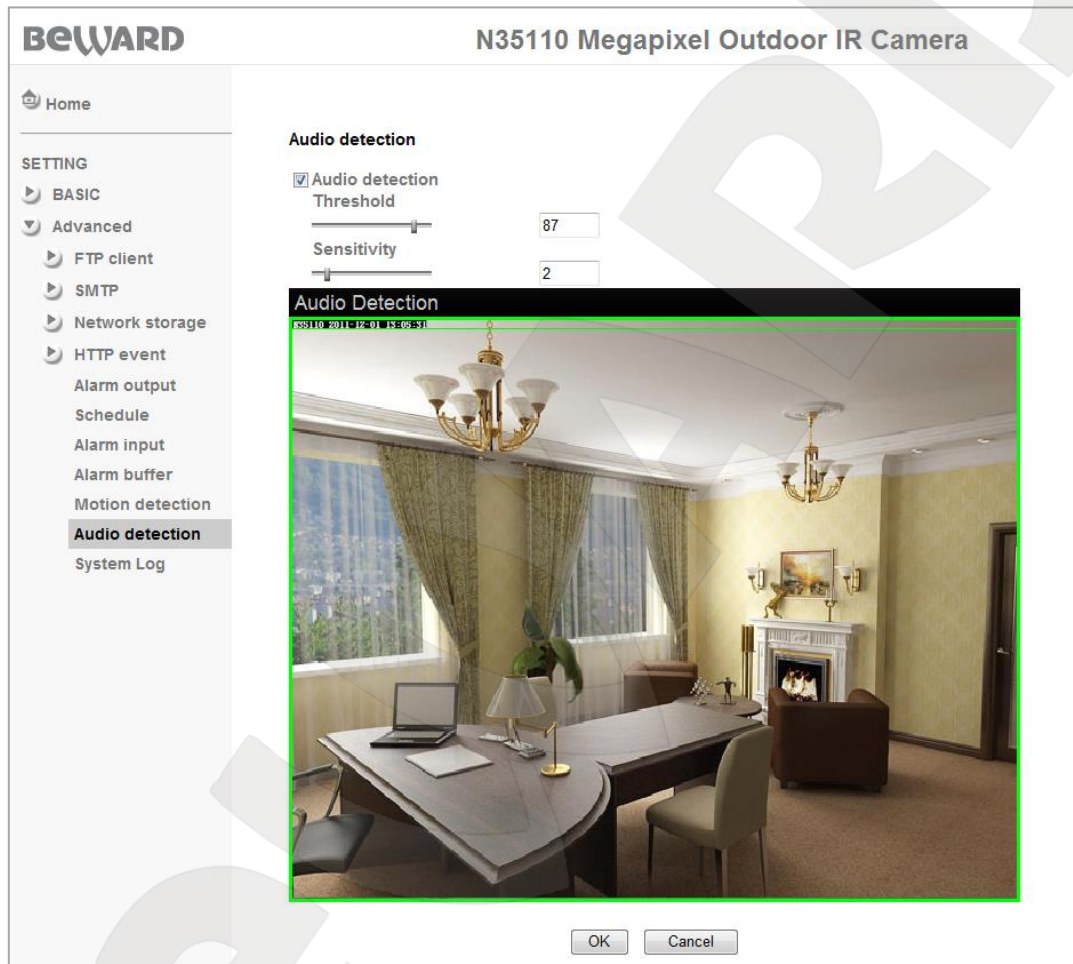
To specify the window size, drag the right bottom corner of the window. Drag an edge of the window to resize it. To move a window, click and hold left mouse button on the window and drag it to the desired area.

IMPORTANT:

When configuring this menu, be aware that these parameters are applied to all functions of the camera, such as recording to NAS, transferring files to FTP, etc.

7.10 Audio Detection

The audio detection module analyzes and responds to changes in noise level in the place where the camera is installed. This menu provides options for adjusting the audio detection threshold and sensitivity. This saves recording space by triggering an alarm recording only when audio is detected. When the audio detection triggers, the camera creates an alert message or a video file and sends it to e-mail, FTP server, network storage, or over HTTP (*Pic. 7.23*).



Pic. 7.23

Threshold: specify the threshold at which audio detection is triggered.

Sensitivity: adjust the audio detection sensitivity. The closer the slider to the right position, the more the sensor is sensitive.

You can see the sound indicator in the live view window. The green frame indicates that the camera detects noise; the red frame indicates that the threshold is exceeded and the audio detection is triggered.

IMPORTANT!

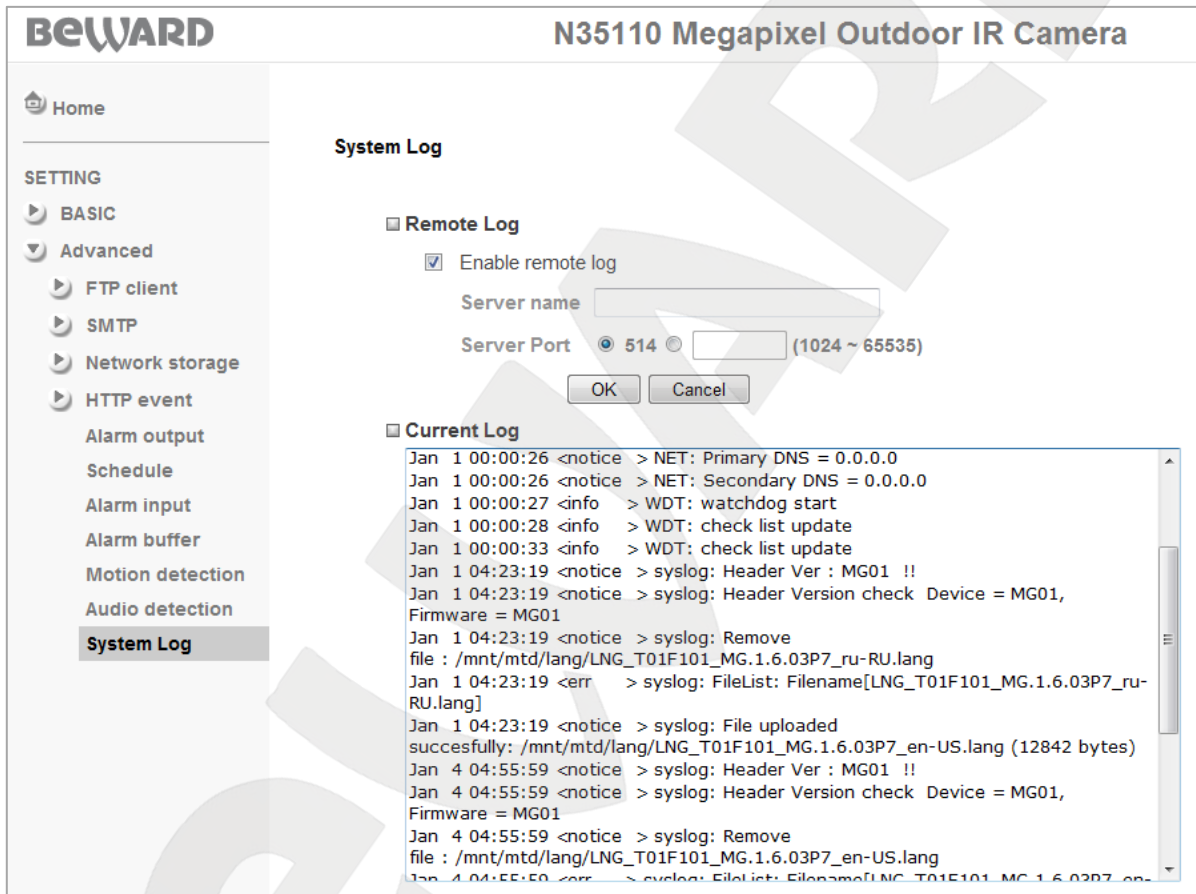
To use the audio detection as an event trigger, connect an external microphone to the camera and enable the audio codec at **SETTING – Basic – Camera – General**.

IMPORTANT!

When configuring this menu, be aware that these parameters are applied to all functions of the camera, such as recording to NAS, transferring files to FTP, etc.

7.11. System Log

The system log captures and stores information about changes to the camera configuration and its activities. The entries are added automatically once the camera is turned on (Pic. 7.24).



Pic. 7.24

Enable remote log: check this box to send the log information to a designated server.

Server name: enter the host name or IP address of the remote server.

Server port: enter the port number of the remote server (the default port is 514).

Current log: this box displays the system log entries for your camera.

Appendix

Appendix A. Bitrate Values

The tables below help you to estimate bitrate, considering the quality level and frames per second. See the information below to choose optimal parameters for your bandwidth.

For example, if you connect to the Internet over ADSL 256 kbps / 2 Mbps, the optimal solution is to select the standard quality, 640x480 resolution and 256 kbps bitrate.

A.1. H.264 15 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	2800	1900	300	90
Detailed	1700	1300	200	75
Good	1300	900	170	60
Standard	800	600	150	55
Medium	600	450	130	45

A.2. H.264 10 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	1900	1400	250	70
Detailed	1200	900	180	60
Good	900	650	160	55
Standard	650	450	130	50
Medium	450	350	120	40

A.3. H.264 kbps – fps

Resolution	Bitrate	Fps	Medium rate	Medium fps
1280*1024	6144	15	6300	15
1280*1024	6144	10	6300	10
1280*1024	2048	15	2200	15
1280*1024	2048	10	2200	10
1280*1024	512	15	550	15
1280*1024	512	10	550	10
1280*720	6144	15	6300	15
1280*720	6144	10	6300	10
1280*720	2048	15	2200	15

1280*720	2048	10	2200	10
1280*720	512	15	550	15
1280*720	512	10	550	10
640*480	6144	15	6300	15
640*480	6144	10	6300	10
640*480	2048	15	2200	15
640*480	2048	10	2200	10
640*480	512	15	550	15
640*480	512	10	550	16
320*240	6144	15	5100	15
320*240	6144	10	3600	10

A.4. MPEG4 15 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	3800	3000	600	130
Detailed	2900	2200	450	110
Good	1800	1400	300	90
Standard	1200	900	250	70
Medium	900	600	200	60

A.5. MPEG4 10 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	3000	2300	500	110
Detailed	2200	1600	400	100
Good	1400	1100	250	80
Standard	950	700	200	65
Medium	700	550	180	50

A.6. MPEG4 kbps – fps

Resolution	Bitrate	Fps	Medium rate	Medium fps
1280*1024	6144	15	5200	12
1280*1024	6144	10	6300	10
1280*1024	2048	15	2200	15
1280*1024	2048	10	2200	10

1280*1024	512	15	550	15
1280*1024	512	10	550	10
1280*720	6144	15	6300	15
1280*720	6144	10	6300	10
1280*720	2048	15	2200	15
1280*720	2048	10	2200	10
1280*720	512	15	550	15
1280*720	512	10	550	10
640*480	6144	15	6300	15
640*480	6144	10	6300	10
640*480	2048	15	2200	15
640*480	2048	10	2200	10
640*480	512	15	550	15
640*480	512	10	550	10
320*240	6144	15	2200	15
320*240	6144	10	1800	10

A.7. MJPEG 15 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	17500	16000	7800	2600
Detailed	12000	9500	4000	1500
Good	10000	6800	2900	1100
Standard	7000	5100	2200	800
Medium	4300	3200	1400	500

A.8. MJPEG 10 fps – kbps

Quality	1280*1024	1280*720	640*480	320*240
Excellent	16000	14500	5500	1700
Detailed	9000	6500	2700	1000
Good	6500	4700	2000	800
Standard	4700	3500	1500	600
Medium	2800	2200	1000	350

A.9. MJPEG kbps – fps

Resolution	Quality	Fps	Medium rate	Medium fps
1280*1024	Excellent	15	17500	8
1280*1024	Excellent	10	16000	8
1280*1024	Good	15	10000	15
1280*1024	Good	10	6500	10
1280*1024	Medium	15	4300	15
1280*1024	Medium	10	2800	10
1280*720	Excellent	15	16000	12
1280*720	Excellent	10	14500	10
1280*720	Good	15	6800	15
1280*720	Good	10	4700	10
1280*720	Medium	15	3200	15
1280*720	Medium	10	2200	10
640*480	Excellent	15	7800	15
640*480	Excellent	10	5500	10
640*480	Good	15	2900	15
640*480	Good	10	2000	10
640*480	Medium	15	1400	15
640*480	Medium	10	1000	10
320*240	Excellent	15	2600	15
320*240	Excellent	10	1700	10

Appendix B. Required Disk Space

This appendix provides information on required disk space for video records storage, considering its quality, bitrate and frames per second. The numbers listed in these tables are estimates only.

B.1. H.264 15 fps, 24-hour record, approximate disk space for 1 camera

Quality	1280*1024	1280*720	640*480	320*240
Excellent	232.4	157.7	24.9	7.5
Detailed	141.4	107.9	16.6	6.3
Good	107.9	74.7	14.2	5
Standard	66.4	49.8	12.5	4.6
Medium	49.8	37.4	10.8	3.8

B.2. H.264 10 fps, 24-hour record, approximate disk space for 1 camera

Quality	1280*1024	1280*720	640*480	320*240
Excellent	157.7	116.2	20.8	5.9
Detailed	99.6	74.7	15	5
Good	74.7	54	13.3	4.7
Standard	54	37.4	10.8	4.2
Medium	37.4	29.1	10	3.4

B.3. H.264 24-hour record, approximate disk space for 1 camera

Resolution	Bitrate	Fps	Disk space, GB
1280*1024	6144	15	522.9
1280*1024	6144	10	522.9
1280*1024	2048	15	182.6
1280*1024	2048	10	182.6
1280*1024	512	15	45.7
1280*1024	512	10	45.7
1280*720	6144	15	522.9
1280*720	6144	10	522.9
1280*720	2048	15	182.6
1280*720	2048	10	182.6
1280*720	512	15	45.7

1280*720	512	10	45.7
640*480	6144	15	522.9
640*480	6144	10	522.9
640*480	2048	15	182.6
640*480	2048	10	182.6
640*480	512	15	45.7
640*480	512	10	45.7
320*240	6144	15	423.3
320*240	6144	10	298.8

B.4. MPEG4 15 fps, 24-hour record, approximate disk space for 1 camera

Quality	1280*1024	1280*720	640*480	320*240
Excellent	315.4	249	49.8	10.8
Detailed	240.7	182.6	37.4	9.2
Good	149.4	116.2	24.9	7.5
Standard	99.6	74.7	20.8	5.9
Medium	74.7	49.8	16.6	5

B.5. MPEG4 10 fps, 24-hour record, approximate disk space for 1 camera

Quality	1280*1024	1280*720	640*480	320*240
Excellent	249	190.9	41.5	9.2
Detailed	182.6	132.8	33.2	8.3
Good	116.2	91.3	20.8	6.7
Standard	78.9	58.1	16.6	5.4
Medium	58.1	45.7	14.5	4.2

B.6. MPEG4 24-hour record, approximate disk space for 1 camera

Resolution	Bitrate	Fps	Disk space, GB
1280*1024	6144	15	431.6
1280*1024	6144	10	522.9
1280*1024	2048	15	182.6
1280*1024	2048	10	182.6
1280*1024	512	15	45.7
1280*1024	512	10	45.7

1280*720	6144	15	522.9
1280*720	6144	10	522.9
1280*720	2048	15	182.6
1280*720	2048	10	182.6
1280*720	512	15	45.7
1280*720	512	10	45.7
640*480	6144	15	522.9
640*480	6144	10	522.9
640*480	2048	15	182.6
640*480	2048	10	182.6
640*480	512	15	45.7
640*480	512	10	45.7
320*240	6144	15	182.6
320*240	6144	10	149.4

Appendix C. Requests for Images from IP Camera

This appendix contains standard request for images from IP camera.

1. http://<IP>:<http_port> - provides access to IP camera, http port means camera HTTP port, the default value is 80, <IP> means camera IP address, the default value is 192.168.0.99.

If the default values are used, the request is:

<http://192.168.0.99>.

2. http://<IP>:<http_port>/index.2.htm – provides access to camera image and the controls are not displayed, http port means camera HTTP port, the default value is 80, <IP> means camera IP address, the default value is 192.168.0.99.

If the default values are used, the request is:

<http://192.168.0.99/index2.htm> - provides access to camera image and the controls are not displayed.

3. <https://<IP>> - provides secured access to IP camera over https through the port 443, <IP> means camera IP address, the default value is 192.168.0.99.

If the default values are used, the request is:

<https://192.168.0.99> - provides secured access to IP camera over https.

4. <http://<IP>:<port>/mobile.htm> - allows you to get an image from a mobile phone over GPRS, port means camera HTTP port, the default value is 80, <IP> means camera IP address, the default value is 192.168.0.99.

If the default values are used, the request is:

<http://192.168.0.99/mobile.htm>

5. <rtsp://<IP>:<port>/video.3gp> – request for 3GP video, port means camera RTSP port, the default value is 554, <IP> means camera IP address, the default value is 192.168.0.99.

If the default values are used, the request is:

<rtsp://192.168.0.99:554/video.3gp>

6. http://<IP>:<http_port>/jpg/image.jpg – request for a JPEG image port means camera HTTP port, the default value is 80, <IP> means camera IP address, the default value is 192.168.0.99. If the default values are used, the request is:

<http://192.168.0.99/jpg/image.jpg>

7. <http://<IP>:< port>/video.mp4> – request for MPEG4 video, port means camera RTSP port, the default value is 554, <IP> means camera IP address, the default value is 192.168.0.99. If the default values are used, the request is:
<rtsp://192.168.0.99:554/video.mp4>
8. <http://<IP>:< port>/video.mjpg> - request for MJPEG video, port means camera RTSP port, the default value is 554, <IP> means camera IP address, the default value is 192.168.0.99. If the default values are used, the request is:
<rtsp://192.168.0.99:554/video.mjpg>
9. <http://<IP>:< port>/video.h264> - request for H.264 video, port means camera RTSP port, the default value is 554, <IP> means camera IP address, the default value is 192.168.0.99. If the default values are used, the request is:
<rtsp://192.168.0.99:554/video.h264>

Appendix D. Port Values

Port	Default Value	Range of Values
HTTP	80	1124..65535
HTTP forwarding over UPnP	80	1024..65535
HTTPS forwarding over UPnP	443	1024..65535
RTSP	554	1124..65535
RTSP forwarding over UPnP	554	1024..65535
RTP start port	5000	1124..65516
RTP end port	7999	1143..65535
Multicast video port	25	1..65535
Multicast audio port	514	1..65535
SMTP	80	1..65535
System log remote server port	-	1..65535
Event server port	1999	-
Proxy port	80	1024..65535
Motion detection	80	1024..65535
H.264 (HTTP) stream	80	1024..65535
MPEG4 (HTTP) stream	8091	1024..65535
MJPEG (HTTP) stream	8071	1024..65535
MPEG4 (HTTP SSL) stream	80	1124..65535
MJPEG (HTTP SSL) stream	80	1024..65535

Appendix E. Factory Defaults

This table provides camera factory defaults

Parameter	Value
IP address	192.168.0.99
Subnet mask	255.255.255.0
Gateway	192.168.0.1
Username (administrator)	admin
Password (administrator)	admin
HTTP port	80
RTSP port	554
SMTP port	25

Appendix F. Accessing the Camera over the Internet Using DynDNS service

F.1. Overview of Internet Access to Cameras Using DynDNS service

If a computer is assigned a temporary IP address changing from one session to the next, it means the computer is assigned a dynamic IP address. Many ISPs use this type of addressing. However, in order to access a device over the Internet any time, you need to contact your ISP and ask them to assign a static IP address, or use a Dynamic DNS (DDNS) service.

The Dynamic DNS service allows you to make your cameras accessible over the Internet even though they are assigned a dynamic IP address, which changes from time to time. All external users can always access the camera using its domain name.

The Dynamic DNS service allows you to access your camera over the Internet using its domain name, which might be similar to `www.camera1.dvrDNS.org`, instead of an IP address.

To do so, create an account at the DDNS server website such as www.dyndns.org, enter your camera's current IP address and choose a domain name that will be used to access your camera.

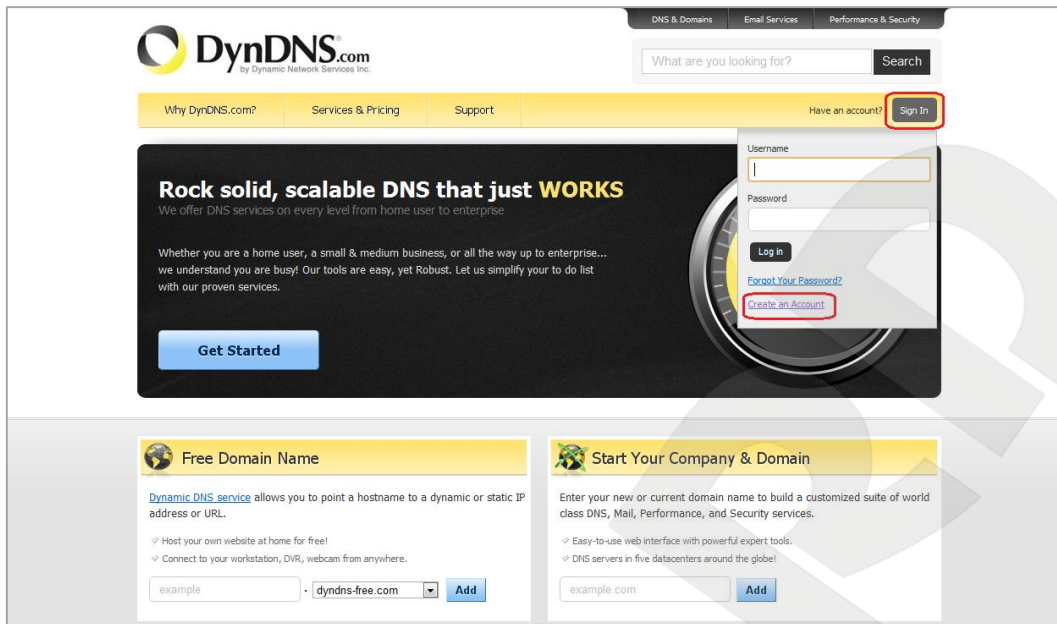
When either the IP address is changed or a new connection is established, the ISP assigns your camera a new IP address. Then it is processed by the software built into the camera and sent to the DDNS server. The DDNS provider ties the domain name you chose to the dynamic IP address.

For this example, we use the following DDNS provider: www.dyndns.com. To tie a domain name to the IP address of your camera, follow the steps below:

- Create an account at www.dyndns.com – **[Account]**.
- Choose a domain name for your camera – **[Hostname]**. You can use any domain name that is not already being used. For this example, we use `camera184` and thus have the following domain name: `www.camera184.dvrDNS.org`.
- Set up your equipment.

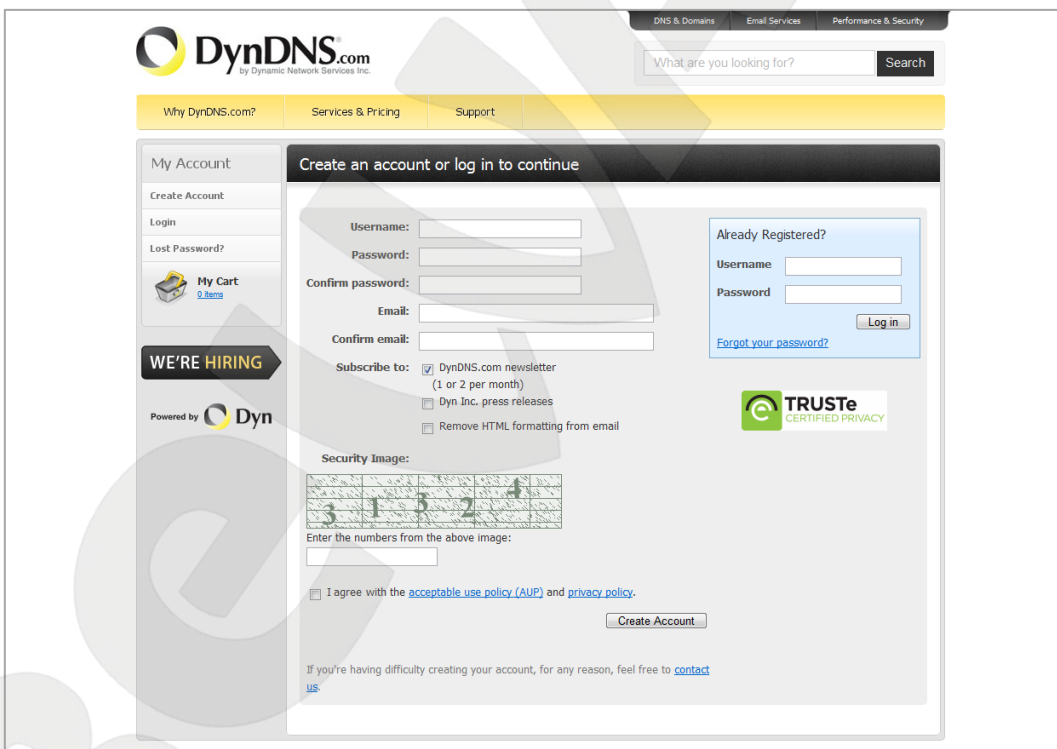
F.2. Creating an Account at DynDNS Service

Step 1: open your browser and go to www.dyndns.com, click the **[Sign In]** in the upper right corner and select the **[CreateanAccount]** in the drop-down menu (*Pic. F.1*).



Pic. F.2

Next you will see the Create an account page (Pic. F.3).



Pic. F.3

Step 2: enter a username that is not already being used (the **[Username]** field) and a password (the **[Password]** and **[Confirm password]** fields).

NOTE:

You need to confirm the password to ensure that there are no typing mistakes. You must enter the same password in both fields.

In the **[Email]** and **[Confirm email]** fields, enter your e-mail address. You will receive a confirmation e-mail to the specified address. An e-mail address can only be associated with one domain name.

NOTE:

A fee is required to associate one e-mail address with multiple domain names.

NOTE:

You need to confirm the e-mail address to ensure that there are no typing mistakes. You must enter the same e-mail address in both fields.

Check the **[DynDNS.com newsletter]** box to get newsletters from DynDNS or uncheck this box if you wish to cancel newsletters.

Enter the numbers from the image and check the **[I agree with the acceptable use policy (AUP) and privacy policy]** box, which means that you agree with AUP and privacy policy to create one free account.

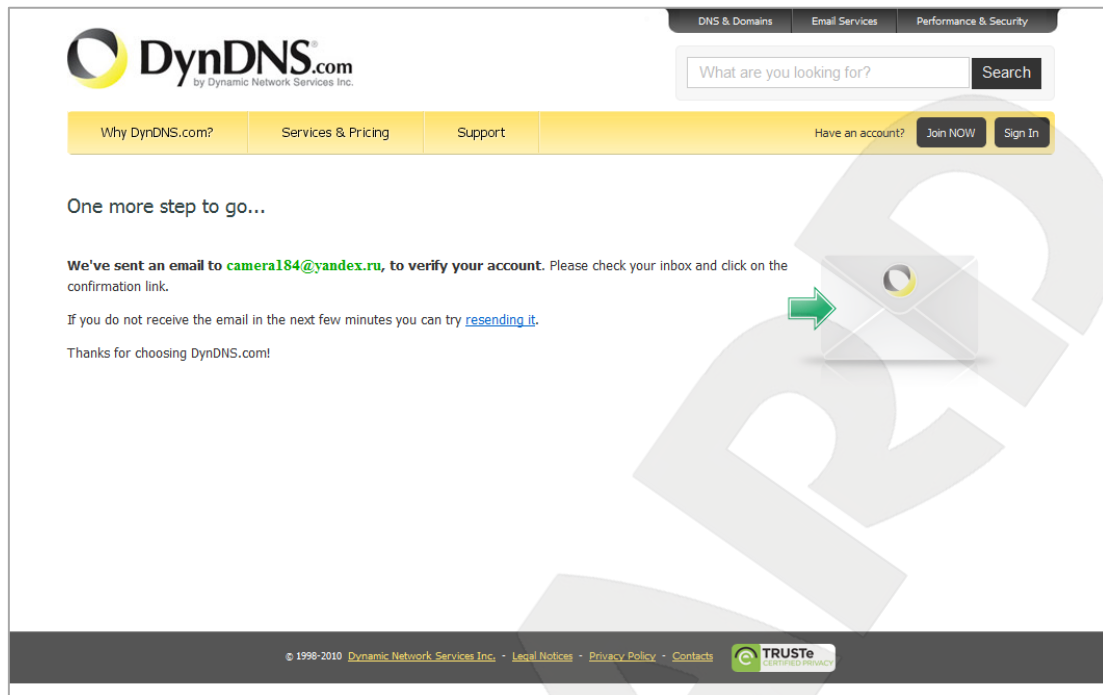
For this example, we use **[Username]** – camera184, **[Email]** - camera184@yandex.ru.

Click the **[Create Account]** button to complete the registration process (*Pic. F.4*).

The screenshot displays the DynDNS.com registration interface. At the top, there is a search bar and navigation tabs for 'DNS & Domains', 'Email Services', and 'Performance & Security'. Below this is a yellow navigation bar with links for 'Why DynDNS.com?', 'Services & Pricing', and 'Support'. The main content area is titled 'Create an account or log in to continue'. On the left, a 'My Account' sidebar contains links for 'Create Account', 'Login', 'Lost Password?', and 'My Cart'. The registration form itself has several sections: a main form with fields for Username (camera184), Password (masked), Confirm password (masked), Email (camera184@yandex.ru), and Confirm email (camera184@yandex.ru); a 'Subscribe to:' section with checkboxes for 'DynDNS.com newsletter (1 or 2 per month)', 'Dyn Inc. press releases', and 'Remove HTML formatting from email'; a 'Security Image' section with a grid of numbers (3, 1, 5, 2, 4) and a text input field containing '31324'; and a checkbox for 'I agree with the acceptable use policy (AUP) and privacy policy.' followed by a 'Create Account' button. On the right, there is an 'Already Registered?' section with fields for Username and Password, a 'Log in' button, and a 'Forgot your password?' link. A 'TRUSTe CERTIFIED PRIVACY' logo is also visible.

Pic. F.4

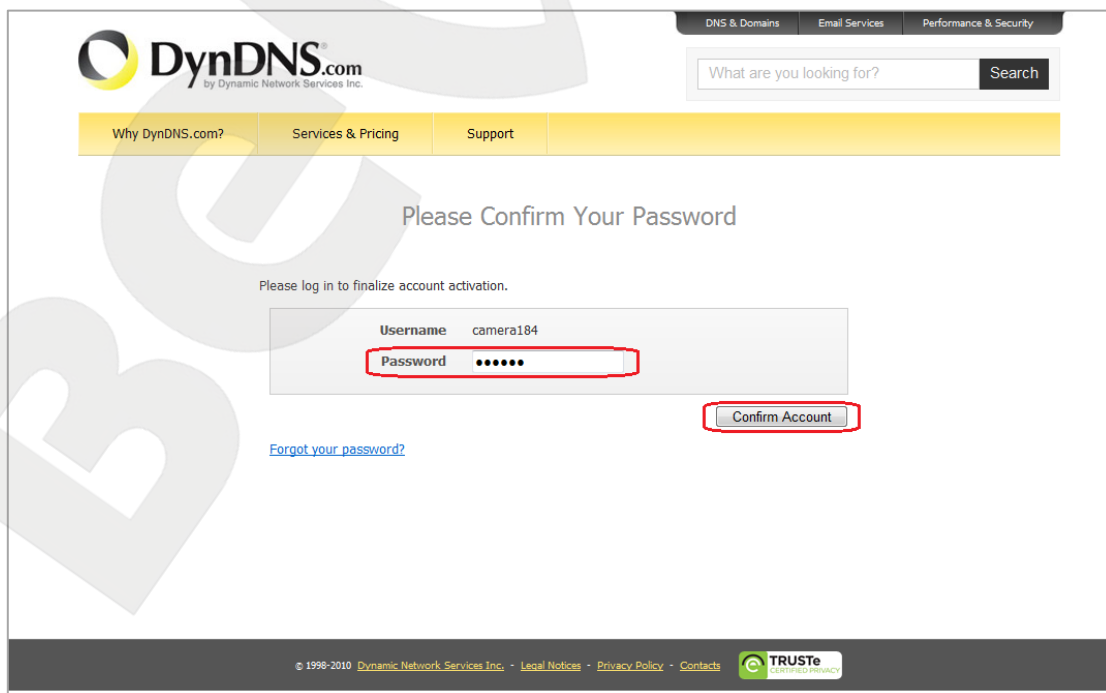
Step 3: if everything is correct, you will see the **[One more step to go...]** page (Pic. F.5).



Pic. F.5

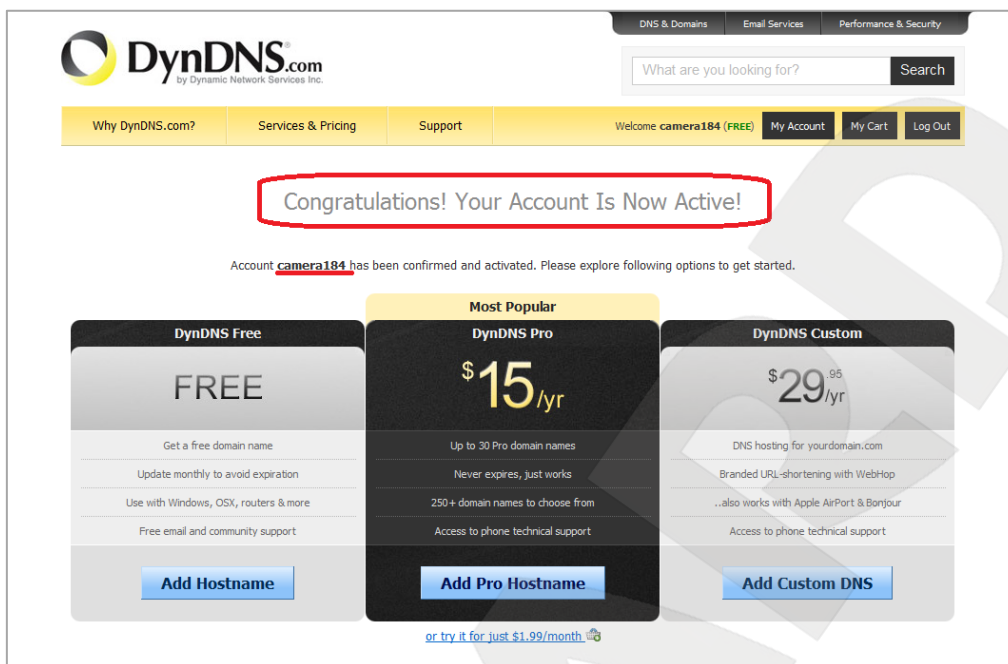
Step 4: you will receive an email confirmation message from «DynDNS Support» (the e-mail address is support@dyndns.com) to the email address you specified in your registration form. Click the link to confirm the registration and to activate your account.

After clicking the link from the e-mail, you will be sent to the confirmation page to activate your account. Enter your username and your password to log in and click the **[Confirm Account]** button (Pic. F.6).



Pic. F.6

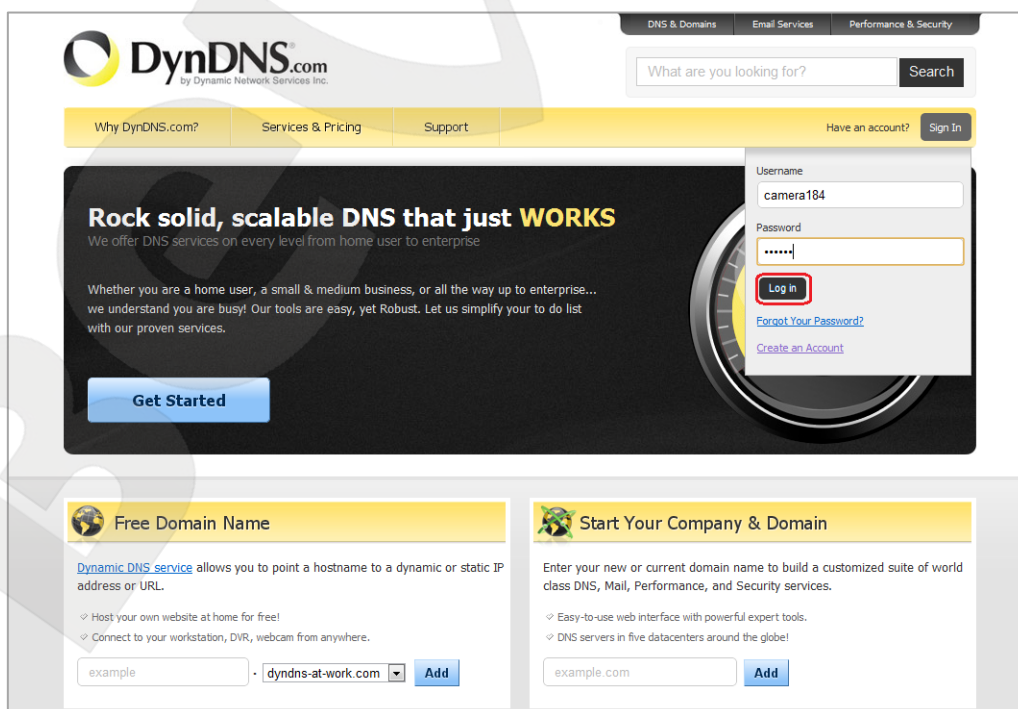
Step 5: your DynDNS account is created (Pic. F.7).



Pic. F.7

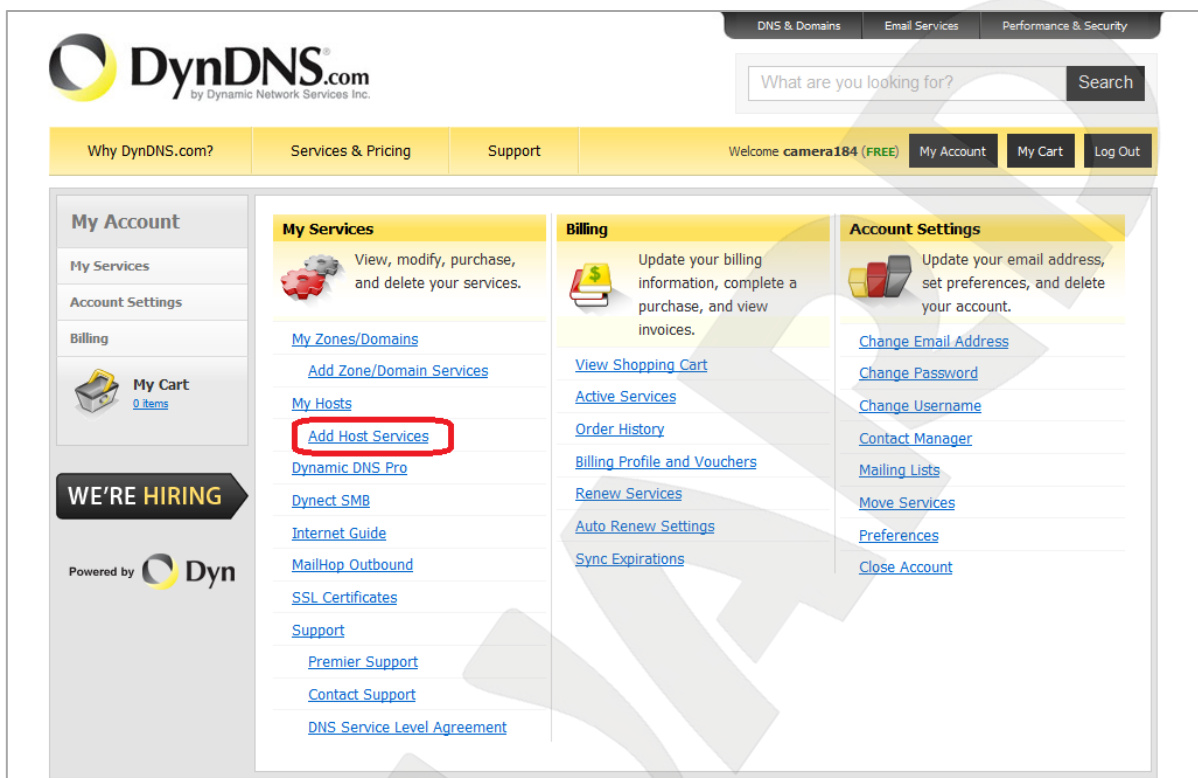
F.3. Creating a Domain Name at DynDNS

Step 1: open your browser, go to www.dyndns.com and log in with your username and your password. To do so, click the **[Sign In]** button in the upper right corner and enter your username in the **[Username]** field and your password in the **[Password]** field, then click the **[Log In]** button (Pic. F.8).



Pic. F.8

Step 2: if the username and password are correct, you will see your account settings page. To continue, click the **[AddHostServices]** (Pic. F.9).



Pic. F.9

Step 3: in the opened page, configure the connection settings. Select a domain. For this example, we use dyndns.org.

In the **[Hostname]** field, enter a domain name for you camera (e.g. camera184). If the domain name is available, the camera will be accessible at camera184.dyndns.org (Pic. F.10).

The screenshot shows the DynDNS.com 'Add New Hostname' page. The page has a navigation bar with 'DNS & Domains', 'Email Services', and 'Performance & Security'. A search bar is present. Below the navigation bar, there are links for 'Why DynDNS.com?', 'Services & Pricing', and 'Support'. A welcome message for 'camera184 (rss)' is displayed, along with 'My Account', 'My Cart', and 'Log Out' buttons.

The main content area is titled 'Add New Hostname'. It includes a sidebar for 'My Account' with sections for 'My Services' (Dynamic DNS Pro, Internet Guide, SLA, Premier Support, Zone Level Services, Host Services, Dynect SMB, MailHop Outbound, Renew Services) and 'Account Settings' (Billing, My Cart). The main form contains the following fields and options:

- Hostname:** camera184 · dyndns.org
- Wildcard:** create *.host.dyndns-yourdomain.com alias (for example to use same settings for www.host.dyndns-yourdomain.com)
- Service Type:**
 - Host with IP address
 - WebHop Redirect (URL forwarding service)
 - Offline Hostname
- IP Address:** 89.105.128.207
Your current location's IP address is 89.105.128.207
TTL value is 60 seconds. [Edit TTL...](#)
- Mail Routing:** I have mail server with another name and would like to add MX hostname...
- What do you want to use this host for?** Select services and devices you would like to use with this hostname.
 - Work From Home Office or VPN:** vpn, remote file access, remote desktop, mail server, web server, chat server, ftp backup, ssh, database, voip
 - Hosting and Design For Web Sites and Blogs:** blog, gallery, wiki, portfolio, ecommerce, web page
 - Remote Access For Devices:** dvr, webcam, data storage, cctv, printer, alarm and security, thermostat, weather station, game server, home automation
- Add To Cart** button

Pic. F.10

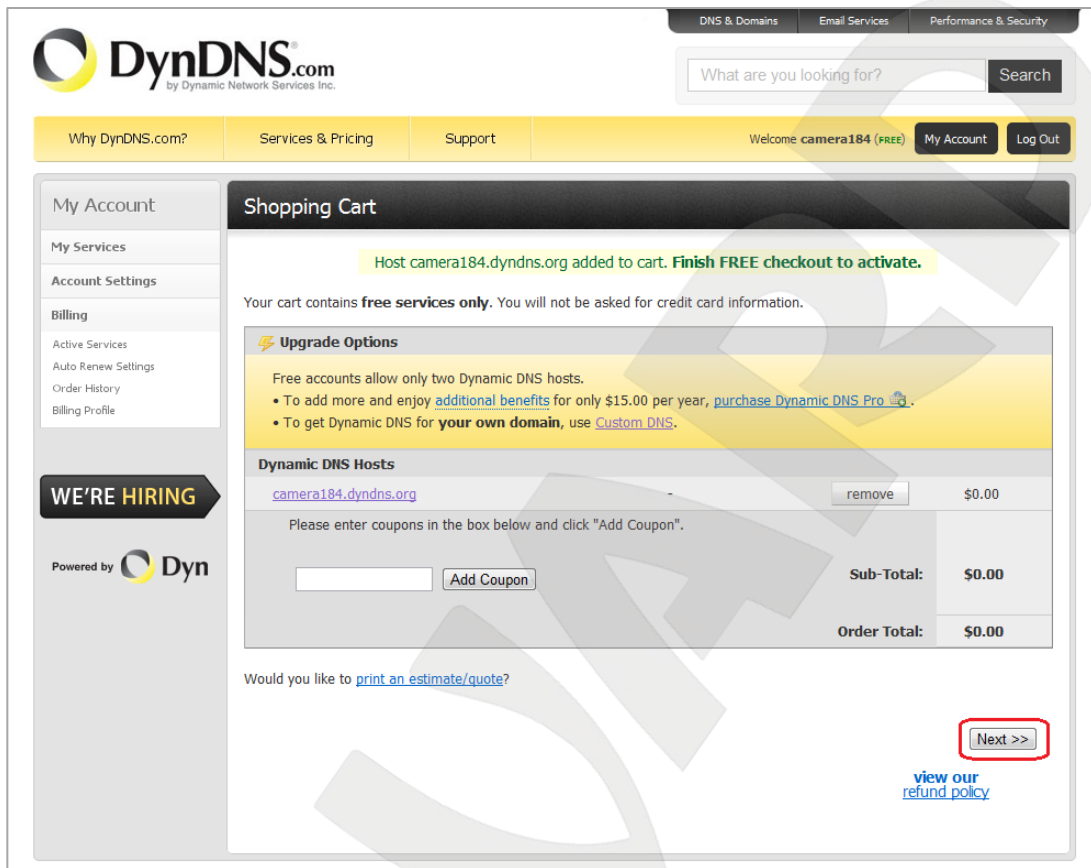
To tie the current IP address of your camera to the specified domain name, please enter its IP address in the **[IP address field]**. By default, DynDNS service determines the IP address from which you are connecting to the service (Pic. F.11).

The close-up shows the 'IP Address:' label followed by an empty text input field. Below the field, the text reads: 'Your current location's IP address is 89.105.128.207' and 'TTL value is 60 seconds. [Edit TTL...](#)'

Pic. F.11

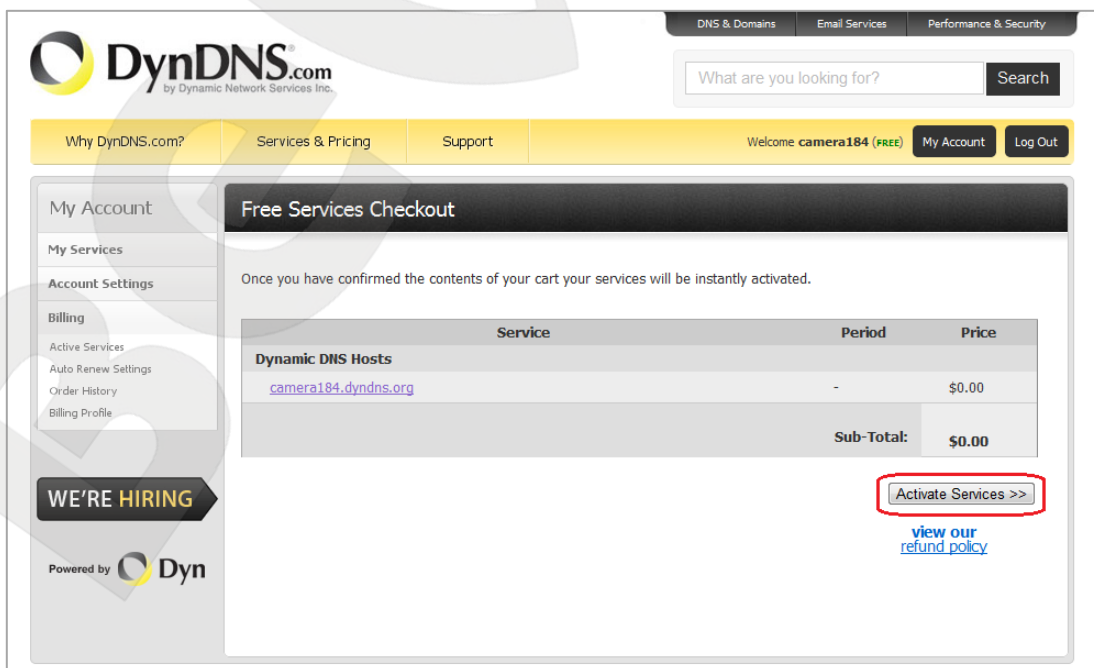
Enter the IP address assigned by your ISP and click the **[Add To Cart]** button.

Step 4: if the domain name is created successfully, you will see the confirmation page. In the provided example, camera184.dyndns.org domain name is created. To activate your domain name, click **[Next]** (Pic. F.12).



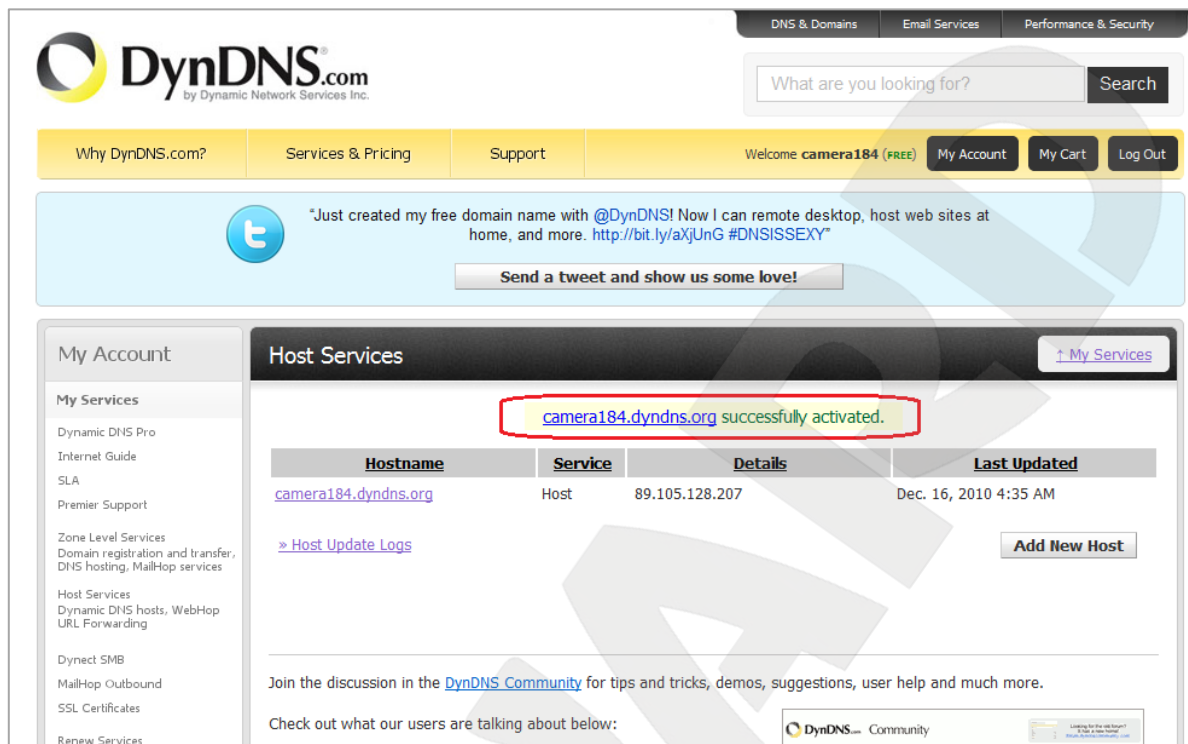
Pic. F.12

In the opened page, click the **[Activate Service]** button (Pic. F.13).



Pic. F.13

Step 5: if your domain name is activated successfully, you will see the confirmation page (Pic. F.14).



Pic. F.14

Step 6: your domain name is created.

F.4. Setting up the Equipment to Work with DynDNS

After the previous steps are completed, you need to set up your camera according to your registration details at DynDNS service (see [paragraph F.2](#), [F.3](#)).

The IP camera and a router (in case if you camera is connected to the Internet through a router) can both update the IP address at DynDNS server.

To set up your camera to work with DynDNS service, please follow the steps below:

IMPORTANT!

Your camera must be connected to the Internet directly.

Step 1: enable the [DDNS] option at **SETTING – Basic – Network – DDNS**.

Step 2: select a DDNS provider in the [Server name].

Step 3: enter the username that you chose at registration in the [User ID].

Step 4: enter the password that you chose at registration in the [Password].

Step 5: re-type the password in the [Re-type password].

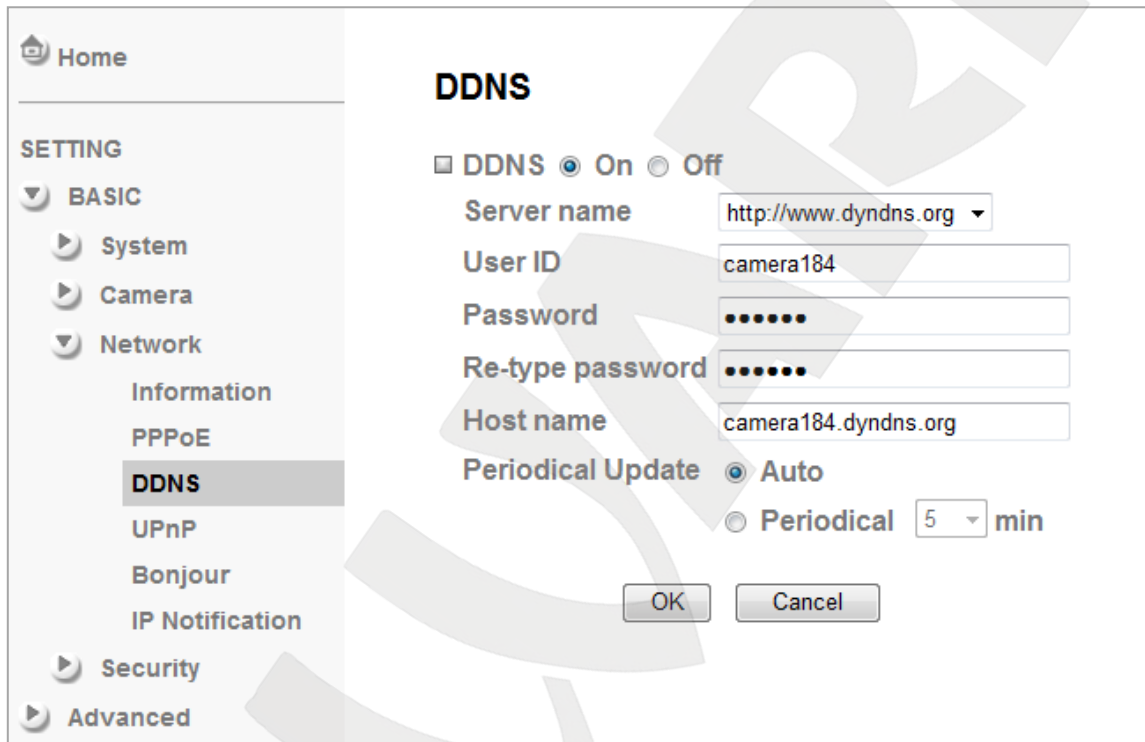
Step 6: enter the domain name that you chose at registration in the [Host name].

IMPORTANT!

For detailed information on how to configure the camera through the web interface, please refer to [paragraph 6.3.3](#).

According to the registration details that were specified at DynDNS server (see [paragraph F.2](#), [F.3](#)), select “www.dyndns.org” in the **[Server name]** field. Enter “camera184” in the **[User ID]** and “123456” in the **[Password]**. Enter “camera184.dyndns.org” in the **[Host name]** (*Pic. F.15*).

Step 7: click **[OK]** to save the changes.



Pic. F.15

IMPORTANT!

After you configure the network settings, you must reboot the camera.

IMPORTANT!

If a host is not updated within 35 days, it will be removed from the system.

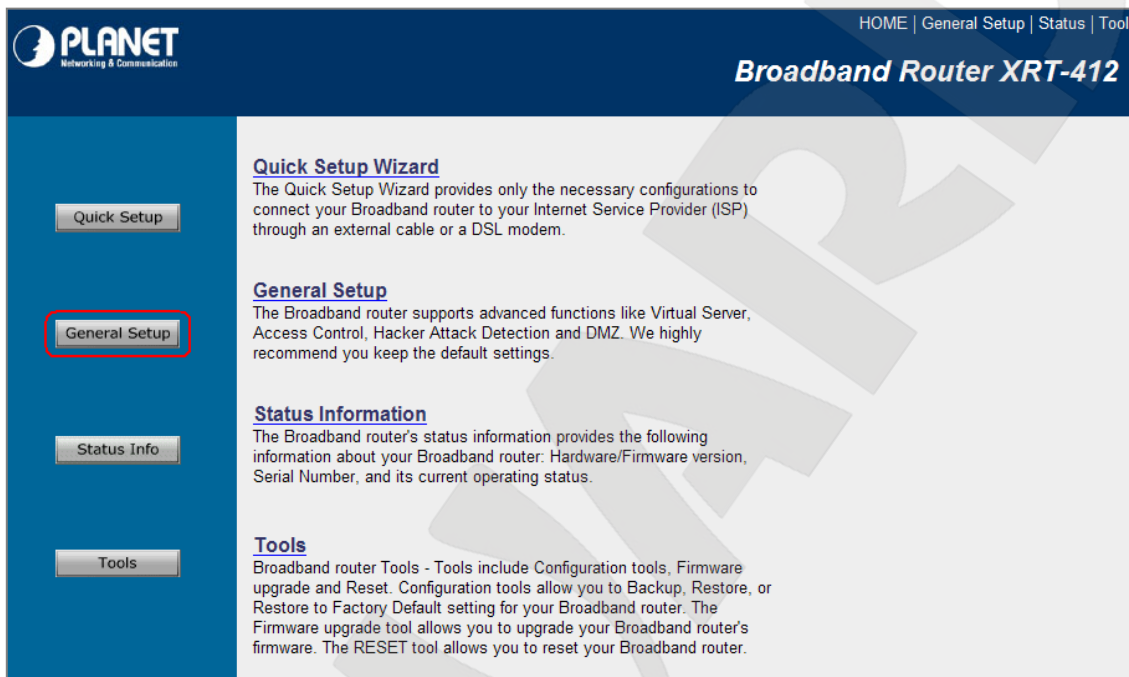
Step 8: the camera configuration is completed.

Let's consider an example of setting up DDNS on a router by configuring Planet XRT-401D. Routers of other manufacturers are configured identically; please refer to the router's manual for more information on how to configure DDNS. The router is configured to work with DynDNS as follows:

IMPORTANT!

Make sure your router supports DDNS, is connected to the Internet and configured properly.

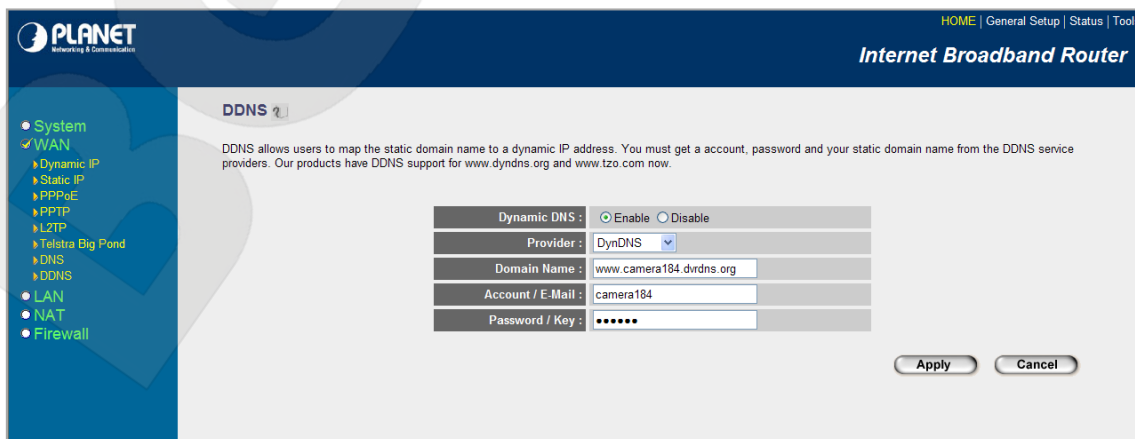
Step 1: enter the IP address of your router in the browser address field. In the appeared window, enter your username and your password. After successful authorization, the router settings page appears. Click the **[General Setup]** (Pic. F.16).



Pic. F.16

Step 2: click the **[DDNS]** in the opened menu. Click the **[Enable]** to enable the DDNS option.

Step 3: according to the registration details that were specified at DynDNS server (see [paragraph F.2](#), [F.3](#)), select “www.dyndns.org” in the **[Provider]** field. Enter “camera184.dyndns.org” in the **[Domain Name]**, enter “camera184” in the **[Account / E-Mail]** and “123456” in the **[Password / Key]** field (Pic. F.17).



Pic. F.17

IMPORTANT!

Make sure you have entered the valid data; otherwise, your router will not be able to connect to the DDNS server.

Step 4: click the **[Apply]** to save the changes.

Step 5: the router configuration is completed.

If everything is configured correctly, your camera will be available from anywhere in the world and accessible under the unique name that is easy to remember. From now on, you need to enter <http://camera184.dyndns.org> in your browser address field to access your camera and if everything was done correctly, you should see the camera main window.

Appendix G. Glossary

3GP (3GPP file format) is a multimedia container format defined by the Third Generation Partnership Project (3GPP) for 3G UMTS multimedia services. It is used on 3G mobile phones but can also be played on some 2G and 4G phones.

ActiveX is a standard that enables software components to interact with one another in a networked environment, regardless of the language(s) used to create them. Web browsers may come into contact with ActiveX controls, ActiveX documents, and ActiveX scripts. ActiveX controls are often downloaded and installed automatically as required.

Asymmetric Digital Subscriber Line (ADSL) is an obsolete type of Digital Subscriber Line technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voiceband modem can provide.

Angle is the field of view, relative to a standard lens in a 35mm still camera, expressed in degrees, e.g. 30°. For practical purposes, this is the area that a lens can cover, where the angle of view is determined by the focal length of the lens. A wide-angle lens has a short focal length and covers a wider angle of view than standard or telephoto lenses, which have longer focal lengths.

ARP (Address Resolution Protocol) is used to associate an IP address to a hardware MAC address. A request is broadcast on the local network to discover the MAC address for an IP address.

Aspect ratio is a ratio of width to height in images. A common aspect ratio used for television screens and computer monitors is 4:3. High-definition television (HDTV) uses an aspect ratio of 16:9.

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Autoiris (or DC-Iris). This special type of iris is electrically controlled by the camera, to automatically regulate the amount of light allowed to enter.

Bit rate: (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

Backlight Compensation compensates for strong backlighting, so that subjects appear clearly instead of as silhouettes.

Bonjour, also known as zero-configuration networking, Bonjour enables automatic discovery of computers, devices, and services on IP networks. Bonjour allows devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. Bonjour is developed by Apple Computer Inc.

CCD (Charged Coupled Device). This light-sensitive image device used in many digital cameras is a large integrated circuit that contains hundreds of thousands of photo-sites (pixels) that convert light energy into electronic signals. Its size is measured diagonally and can be 1/4", 1/3", 1/2" or 2/3".

CGI (Common Gateway Interface) is a specification for communication between a web server and other (CGI) programs. For example, a HTML page that contains a form might use a CGI program to process the form data once it is submitted.

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C. In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.9.205.22 /18 means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are 8, 16, 24, and 32.

Complementary metal–oxide–semiconductor (CMOS) is a technology for constructing integrated circuits. CMOS technology is used in microprocessors, microcontrollers, static RAM, and other digital logic circuits. CMOS technology is also used for several analog circuits such as image sensors (CMOS sensor), data converters, and highly integrated transceivers for many types of communication.

Dynamic DNS is a method/protocol/network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information.

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators automate and centrally manage the assignment of Internet Protocol (IP) addresses to network devices in a network. DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary, depending on how long a user is likely to require the network connection at a particular location. DHCP also supports static addresses for e.g. computers running web servers, which need a permanent IP address.

Digital zoom is a method of decreasing (narrowing) the apparent angle of view of a digital photographic or video image. Digital zoom is accomplished by cropping an image down to a centered area with the same aspect ratio as the original, and usually also interpolating the result back up to the pixel dimensions of the original. It is accomplished electronically, with no adjustment of the camera's optics, and no optical resolution is gained in the process.

Domain server can also be used by organizations that wish to centralize the management of their (Windows) computers. Each user within a domain has an account that usually allows them to log in to and use any computer in the domain, although restrictions may also apply. The domain server is the server that authenticates the users on the network.

Ethernet is the most widely installed local area network technology. An Ethernet LAN typically uses special grades of twisted pair wires. The most commonly installed Ethernet systems are 10BASE-T and 100BASE-T10, which provide transmission speeds up to 10 Mbps and 100 Mbps respectively.

Factory default settings are the settings that originally applied for a device when it was first delivered from the factory. If it should become necessary to reset a device to its factory default settings, this will, for many devices, completely reset any settings that were changed by the user.

Firewall works as a barrier between networks, e.g. between a Local Area Network and the Internet. The firewall ensures that only authorized users are allowed to access the one network from the other. A firewall can be software running on a computer, or it can be a standalone hardware device.

Focal length is measured in millimeters; the focal length of a camera lens determines the width of the horizontal field of view, which in turn is measured in degrees.

FPS (frames per second) a measure of how much information is used to store and display motion video. The term applies equally to film video and digital video. Each frame is a still image; displaying frames in quick succession creates the illusion of motion. The more frames per second (fps), the smoother the motion appears.

Frame is a complete video image. In the 2:1 interlaced scanning format of the RS-170 and CCIR formats, a frame is made up of two separate fields of 262.5 or 312.5 lines interlaced at 60 or 50 Hz to form a complete frame, which appears at 30 or 25 Hz. In video cameras with a progressive scan, each frame is scanned line-by-line and not interlaced; most are also displayed at 30 and 25 Hz.

FTP (File Transfer Protocol) is an application protocol that uses the TCP/IP protocols, used to exchange files between computers/devices on networks.

Full-duplex means transmission of data in two directions simultaneously. In an audio system this would describe e.g. a telephone system. Half-duplex also provides bi-directional communication, but only in one direction at a time, as in a walkie-talkie system.

G.711 is the default pulse code modulation (PCM) standard for Internet Protocol (IP) private branch exchange (PBX) vendors, as well as for the public switched telephone network (PSTN). G.711 digitizes analog voice signals producing output at 64 kilobits per second (Kbps).

Gain is the amplification factor and the extent to which an analog amplifier boosts the strength of a signal. Amplification factors are usually expressed in terms of power. The decibel (dB) is the most common way of quantifying the gain of an amplifier.

Gateway is a point in a network that acts as an entry point to another network. In a corporate network for example, a computer server acting as a gateway often also acts as a proxy server and a firewall server. A gateway is often associated with both a router, which knows where

to direct a given packet of data that arrives at the gateway, and a switch, which furnishes the actual path in and out of the gateway for a given packet.

HTTP (Hypertext Transfer Protocol) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the web. The HTTP protocol runs on top of the TCP/IP suite of protocols.

HTTPS (Hypertext Transfer Protocol over SSL) is a web protocol used by browsers and web servers to encrypt and decrypt user page requests and the pages returned by the server. The encrypted exchange of information is governed by the use of an HTTPS certificate (issued by a Certificate Authority), which guarantees the authenticity of the server.

Hub is used to connect multiple devices to the network. The hub transmits all data to all devices connected to it, whereas a switch will only transmit the data to the device it is specifically intended for.

ICMP is a network protocol useful in Internet Protocol (IP) network management and administration. ICMP is a required element of IP implementations. ICMP is a control protocol, meaning that it does not carry application data, but rather information about the status of the network itself.

IEEE 802.11 is a family of standards for wireless LANs. The 802.11 standard supports 1 or 2 Mbit/s transmission on the 2.4 GHz band. IEEE 802.11b supports data rates up to 11 Mbit/s on the 2.4 GHz band, while 802.11g allows up to 54 Mbit/s on the 5 GHz band.

Interlacing. Interlaced video is video captured at 50 pictures (known as fields) per second, of which every 2 consecutive fields (at half height) are then combined into 1 frame. Interlacing was developed many years ago for the analog TV world and is still used widely today. It provides good results when viewing motion in standard TV pictures, although there is always some degree of distortion in the image.

Internet Explorer (formerly Microsoft Internet Explorer, commonly abbreviated IE or MSIE) is a series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating systems, starting in 1995.

IP66 is a two digit number developed by the international electrical Commission, and is used to provide Ingress Protection (IP) rating to a piece of electronic equipment or to an enclosure for electronic equipment. The Ingress protection code indicates the level and amount of protection. The first digit means no ingress of dust; complete protection against contact. The second digit means water projected in powerful jets (12.5mm nozzle) against the enclosure from any direction shall have no harmful effects.

IP camera. The terms IP camera, network camera and Internet camera all refer to the same thing - a camera and computer combined in one unit. It operates as stand-alone unit and only requires a connection to the network.

JPEG (Joint Photographic Experts Group). Together with the GIF file format, JPEG is an image file type commonly used on the web. A JPEG image is a bitmap, and usually has the file extension '.jpg' or ".jpeg." When creating a JPEG image, it is possible to configure the level of compression to use. As the lowest compression (i.e. the highest quality) results in the largest file, there is a trade-off between image quality and file size.

kbit/s (kilobits per second) is a measure of the bit rate, i.e. the rate at which bits are passing a given point. See also Bit rate.

LAN (Local Area Network) is a group of computers and associated devices that typically share common resources within a limited geographical area.

Lux is a standard unit of illumination measurement.

MAC address (Media Access Control address) is a unique identifier associated with a piece of networking equipment, or more specifically, its interface with the network. For example, the network card in a computer has its own MAC address.

Mbit/s (Megabits per second) is a measure of the bit rate, i.e. the rate at which bits are passing a given point. Commonly used to give the "speed" of a network. A LAN might run at 10 or 100 Mbit/s.

Motion JPEG is a simple compression/decompression technique for network video. Latency is low and image quality is guaranteed, regardless of movement or complexity of the image. Image quality is controlled by adjusting the compression level, which in turn provides control over the file size, and thereby the bit rate.

MPEG-4 is a group of audio and video coding standards and related technology. The primary uses for the MPEG-4 standard are web (streaming media) and CD distribution, conversational (videophone), and broadcast television. Most of the features included in MPEG-4 are left to individual developers to decide whether to implement them or not. This means that there are probably no complete implementations of the entire MPEG-4 set of standards. To deal with this, the standard includes the concept of "profiles" and "levels", allowing a specific set of capabilities to be defined in a manner appropriate for a subset of applications.

Multicast is a bandwidth-conserving technology that reduces bandwidth usage by simultaneously delivering a single stream of information to multiple network recipients.

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

NTSC (National Television System Committee) is an analog color encoding system used in television systems in Japan, the United States and other parts of the Americas. NTSC defines the video signal using 525 TV lines per frame, at a refresh rate equal to 30 frames per second. See also PAL.

ONVIF (Open Network Video Interface Forum) is a global and open industry forum with the goal to facilitate the development and use of a global open standard for the interface of physical IP-based security products. Or in other words, to create a standard for how IP products within video surveillance and other physical security areas can communicate with each other. ONVIF is an organization started in 2008 by Axis Communications, Bosch Security Systems and Sony.

PAL (Phase Alternating Line) is an analog color encoding system used in television systems in Europe and in many other parts of the world. PAL defines the video signal using 625 TV lines per frame, at a refresh rate equal to 25 frames per second.

Power over Ethernet or PoE provides power to a network device via the same cable as used for the network connection. This is very useful for IP-Surveillance and remote monitoring applications in places where it may be too impractical or expensive to power the device from a power outlet.

PPP (Point-to-Point Protocol) is a protocol that uses a serial interface for communication between two network devices. For example, a PC connected by a phone line to a server.

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with DSL services where individual users connect to the DSL modem over Ethernet and in plain Metro Ethernet networks.

Progressive scan, as opposed to interlaced video, scans the entire picture, line by line every sixteenth of a second. In other words, captured images are not split into separate fields as in interlaced scanning.

Jack-45 is an eight-wire connector used to connect computers onto a local-area networks (LAN), especially Ethernets. RJ-45 connectors look similar to the RJ-11 connectors used for connecting telephone equipment, but they are a bit wider.

Router is a device that determines the next network point to which a packet should be forwarded on its way to its final destination. A router creates and/or maintains a special routing table that stores information on how best to reach certain destinations. A router is sometimes included as part of a network switch.

RTP is an Internet protocol for the transport of real-time data, e.g. audio and video. It can be used for media-on-demand as well as interactive services such as Internet telephony.

RTSP (Real Time Streaming Protocol) is a control protocol, and a starting point for negotiating transports such as RTP, multicast and Unicast, and for negotiating codecs.

RTSP can be considered a “remote control” for controlling the media stream delivered by a media server. RTSP servers typically use RTP as the protocol for the actual transport of audio/video data.

Shutter is the device on the camera that opens and closes to control how long the focal plane is exposed to light.

SMTP is used for sending and receiving e-mail. However, as it is “simple,” it is limited in its ability to queue messages at the receiving end, and is usually used with one of two other protocols, POP3 or IMAP. These other protocols allow the user to save messages in a server mailbox and download them periodically from the server.

SMTP authentication is an extension of SMTP, whereby the client is required to log into the mail server before or during the sending of email. It can be used to allow legitimate users to send email while denying the service to unauthorized users, such as spammers.

SSL/TLS (Secure Socket Layer/Transport Layer Security). These two protocols (SSL is succeeded by TLS) are cryptographic protocols that provide secure communication on a network. SSL is commonly used over HTTP to form HTTPS, as used e.g. on the Internet for electronic financial transactions. SSL uses public key certificates to verify the identity of the server.

Subnet & subnet mask is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address. The subnet mask is the part of the IP address that tells a network router how to find the subnet that the data packet should be delivered to. Using a subnet mask saves the router having to handle the entire 32-bit IP address; it simply looks at the bits selected by the mask.

Switch is a network device that connects network segments together, and which selects a path for sending a unit of data to its next destination. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route. Some switches include the router function.

TCP is used along with the Internet Protocol (IP) to transmit data as packets between computers over the network. While IP takes care of the actual packet delivery, TCP keeps track of the individual packets that the communication (e.g. requested a web page file) is divided into, and, when all packets have arrived at their destination, it reassembles them to re-form the complete file.

TCP is a connection-oriented protocol, which means that a connection is established between the two end-points and is maintained until the data has been successfully exchanged between the communicating applications.

Time to live (TTL) is mechanism that limits the lifespan of data in a computer or network. TTL may be implemented as a counter or timestamp attached to or embedded in the data. Once the prescribed event count or timespan has elapsed, data is discarded. In computer networking, TTL prevents a data packet from circulating indefinitely. In computing applications, TTL is used to improve performance of caching or improve privacy.

UDP is a communications protocol that offers limited service for exchanging data in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP). The advantage of UDP is that it is not required to deliver all data and may drop network packets when there is e.g. network congestion. This is suitable for live video, as there is no point in re-transmitting old information that will not be displayed anyway.

Universal Plug and Play (UPnP) is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Uniform Resource Locator or Unified Resource Locator (URL) is a character string that specifies where a known resource is available on the Internet and the mechanism for retrieving it.

Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones (called "cellular phones" in some countries) that uses the protocol.

Web server is a program, which allows Web browsers to retrieve files from computers connected to the Internet. The Web server listens for requests from Web browsers and upon receiving a request for a file sends it back to the browser.

The primary function of a Web server is to serve pages to other remote computers; consequently, it needs to be installed on a computer that is permanently connected to the Internet. It also controls access to the server whilst monitoring and logging server access statistics.

Wireless LAN is a wireless local area network that uses radio waves as its carrier: where the network connections for end-users are wireless. The main network structure usually uses cables.