

DK103M IP Converter Operation User Manual

Table of Contents

CHAPTER 1. SAFETY INSTRUCTIONS.....	3
CHAPTER 2. GENERAL INFO	5
2.1. BEWARD DK103M IP CONVERTER OVERVIEW.....	5
2.1.1. Key Features.....	5
2.1.2. Package contents.....	6
2.1.3. Default Settings.....	6
2.2. PURPOSE OF THIS MANUAL.....	6
CHAPTER 3. GETTING STARTED.....	8
3.1. INSTALLATION OF ACTIVEX COMPONENTS AND AUTHORIZATION	8
3.2. MAIN WINDOW (LIVE VIEW)	12
CHAPTER 4. REPLAY.....	15
CHAPTER 5. CONFIG: LOCAL CONFIG	17
CHAPTER 6. CONFIG: AUDIO SETTINGS.....	18
CHAPTER 7. CONFIG: VIDEO SETTINGS	20
7.1. ON-SCREEN TEXT.....	20
7.2. VIDEO CODING	21
CHAPTER 8. CONFIG. NETWORK SETTINGS	23
8.1. BASIC.....	23
8.2. LAN.....	25
8.3. PPPoE	26
8.4. UPnP	27
8.5. E-MAIL	28
8.6. FTP.....	29
8.7. DDNS.....	30
8.8. VPN	31
8.9. RTSP	32
8.10. HTTPS.....	33
8.11. SIP.....	35
8.12. Wi-Fi	38
8.13. 4G.....	42
CHAPTER 9. CONFIG: RECORD SETTINGS	43
9.1. MEMORY CARD.....	43
9.2. VIDEO RECORDING	44
9.3. SNAPSHOTTING	45
CHAPTER 10. CONFIG: ALARM SETTINGS.....	46
10.1. MOTION DETECTION SETTINGS	46
CHAPTER 11. CONFIG: DOOR OPEN	48
CHAPTER 12. CONFIG: SYSTEM.....	49
12.1. SYSTEM INFO	49
12.2. SYSTEM TIME	50
12.3. ACCESS POLICY.....	51
12.4. FW UPGRADE.....	52
12.5. RESTORE	54
12.6. REBOOT.....	55
12.7. SYSTEM LOG	56
CHAPTER 13. ALARM	57
CHAPTER 14. RECOMMENDATIONS ON SETTING AND OPERATION OF DKS103M.....	58
14.1. ACOUSTIC ECHO CANCELLATION	58
14.2. SOUND GAIN AND VOLUME ADJUSTING.....	59
APPENDICES.....	60
APPENDIX A. FACTORY DEFAULTS.....	60
APPENDIX B. MAINTENANCE	60

APPENDIX C. GLOSSARY	61
----------------------------	----

BEWARD

Chapter 1. Safety Instructions

Before using the product.

This product complies with all safety rules. However, improper use of any electric device can cause fires and severe damage. In order to avoid accidents, please read this Manual carefully before you start using this device.

ATTENTION!

Use accessories specified by the manufacturer only. Use of improper accessories may cause device breakdown.

Follow this Operation Manual.

Do not use or store the door station in severe environment:

- Avoid extremely low and high temperatures (The operating temperature of this IP Converter is 0°~+50°).
- Avoid prolonged exposure to direct sunlight, do not install near water and heat sources.
- Avoid exposure to water.
- Do not install near electromagnetic transmitters
- Avoid exposure to high vibration.

ATTENTION!

Contact our Service Center in case of malfunction.

In case of:

- Smoke or strange smell coming from the IP Converter.
- Water or foreign matter getting inside the IP Converter.
- The IP Converter getting damaged:

Do the following:

- Unplug the power cord and disconnect all other cords from the IP Converter.
- Contact our Service Center. You can find our contact information on our website:
<http://www.beward.ru/>.

Transportation

Transport the IP Converter carefully, using the original box and protective packing

Air flow

In order to avoid overheating, ensure that nothing is blocking the air circulation around the IP Converter!

Cleaning

Use a soft dry cloth to clean the surface of the device. To remove obstinate stains, apply a small amount of detergent on the cloth, then wipe the surface dry.

Do not use volatile solvents (alcohol-containing products, Benzene etc.) to avoid damaging the housing of the device.

Chapter 2. General Info

2.1. BEWARD DK103M IP Converter overview

BEWARD DK103M IP Converter is designed for organizing IP intercome systems based on already existing local networks without using any additional equipment (e.g. separate internal monitors). To start using the device you only have to install the software on your PC or Smartphone device and set it up. This device is:

- Low-cost
- Easy to install
- Remote Access Supported



Pic. 2.1

DK103M is used for analog-to-digital conversion and managing analog wired matrix intercom devices. In other words, this device converts analog intercoms into digital intercoms, while retaining the ability to use the analog monitor. The device allows for establishing video and audio connection between the Guest and the Client, conducting surveillance of the nearby territory, control of other devices that are connected to the single-user door station (electronic locks, garage door openers, light switches, alarm systems etc.) via Ethernet. The device is supported by modern network technologies, allowing it to be used a part of a complex IP Surveillance system.

DK103M is connected to the network via-T/100BASE-TX Ethernet interface. Its power is supplied from a DC 12V power source.

The device is even more reliable due to its SD card support that prevents loss of data in case of network failures.

2.1.1. Key Features

- Simultaneous encoding: H.264/H264, H.264/MJPEG, MJPEG /MJPEG
- Built-in web server for viewing and adjusting settings
- Built-in player for recorded videos
- Build-in microphone and speaker
- Power: DC 12 V
- Temperature: -0°C~+50°C

- Supported protocols: TCP/IP, SIP v.2.0, VPN, STUN, HTTP, HTTPS, FTP, SMTP, DDNS, DHCP, PPPoE, RTP, RTSP, UDP, UPnP, NTP, ONVIF v.2.41
- ONVIF v.2.41 support

2.1.2. Package contents

- DK103M IP Converter
- Self-tapping screws
- Wi-Fi antenna (for DKxxxW option)
- 4G USB modem (for DKxxx4G option)
- Terminal block (4 pcs.)
- CD with software and documentation

ATTENTION!

Package contents and device specification are subject to change without notice

2.1.3. Default Settings

- IP address: **192.168.0.99**
- Subnet Mask: **255.255.255.0**
- Gateway: **192.168.0.1**
- Username: **admin**
- Password: **admin**
- HTTP port: **80**
- Data Port: **5000**

2.2. Purpose of this Manual

Beward DK103M IP Converter can be used as a video surveillance device with a built-in web server and a web interface.

You can view the video broadcast by this device via the standard internet browser or via the free software included in the CD (Also can be downloaded from App Store and Play Market).

This User Manual contains the full information on how to operate the IP Converter via the web interface. It explains how to set up the web interface for use in local network or the Internet. To learn more about using the IP Converter software, please read the Software User Manuals

Despite the fact the several functions are only available in Beward Software (see BEWARD Intercom Software Operation Manual), the web version allows users to operate the IP Converter from any location with Internet access

This Manual contain the information needed to use the DK103M IP Converter without installing additional software.

2.3. Minimum System Requirements

Please make sure your PC meets the following minimum requirements:

Item	Requirement
CPU	2.6 Ghz Intel Core or AMD Athlon X2
Video Card	256 mb RAM or similar
RAM	2 Gb
OS	Windows 7, Windows 8
Internet Browser	Internet Explorer 11.0 or higher

ATTENTION!

Windows 7 Professional и Internet Explorer 11.0 are used in this Manual (though in some screenshots other OS and browser version may be depicted). In other OS and browsers some menu names may differ.

Chapter 3. Getting Started

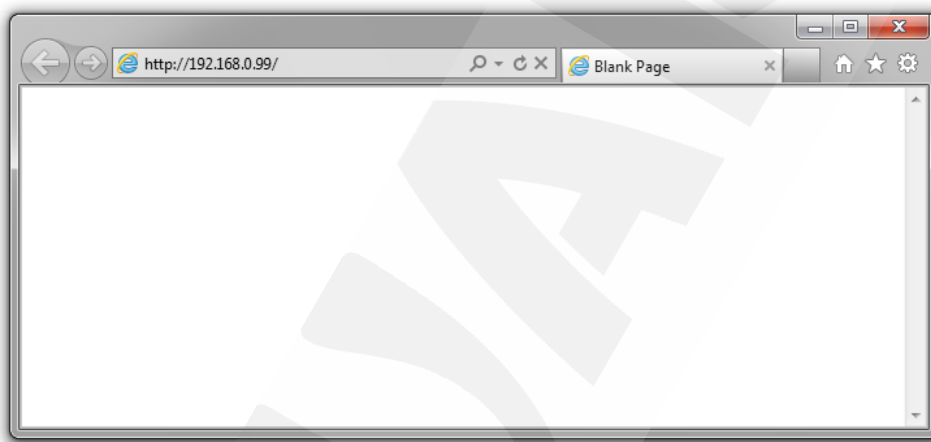
3.1. Installation of ActiveX components and Authorization

Step 1: Connect the device following the Installation User Manual.

Step 2: Run Internet Explorer and enter the following path in the address : ***http://<IP>:<PORT>***, where ***<IP>*** is the IP address of the IP Converter, ***<PORT>*** is number of the port used for HTTP connection to the device.

NOTE:

The default IP address is **192.168.0.99**, default HTTP-port is – **80**. You don't need to enter the port number if you connect via the default HTTP port.



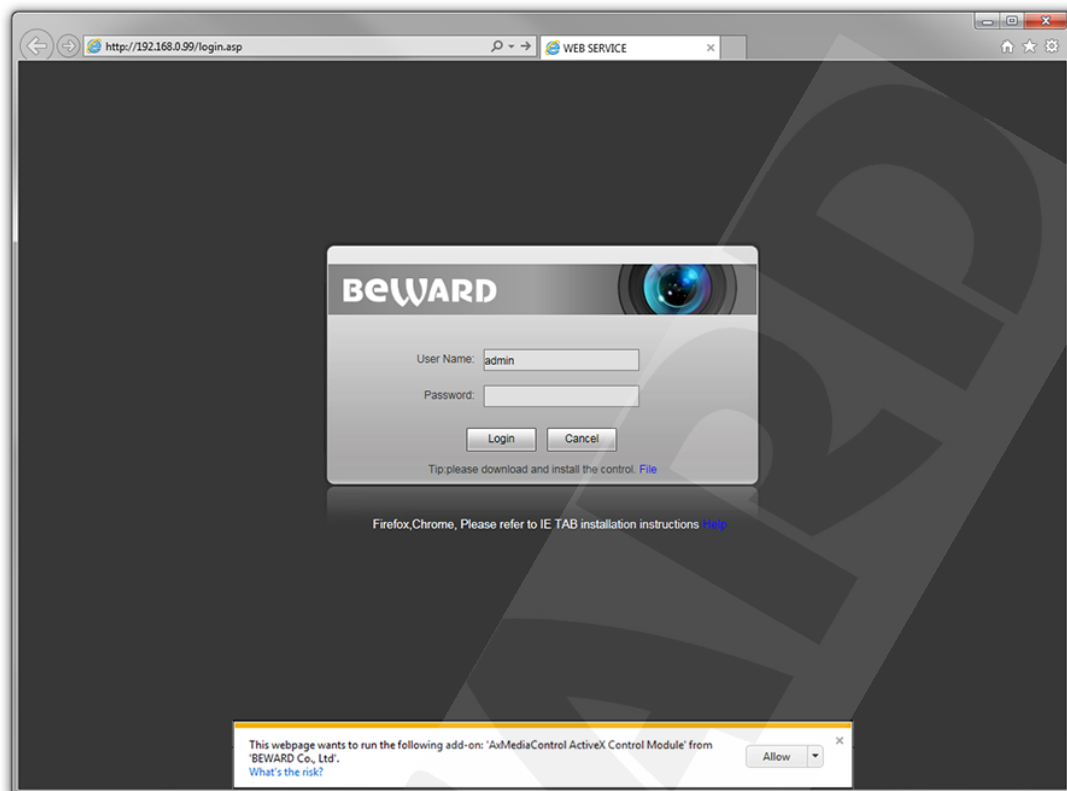
Pic. 3.1

If the path is correct, the authorization window will open.

NOTE:

There are 2 ways to obtain the IP address for the device: 1) Obtain the address automatically from the DHCP server according to your LAN setup. 2) Use the user-defined IP address. See [8.2](#) of this manual to learn more about the available network options. Please consult your system administration before using the device..

Step 3: To work with the web interface you need to install the ActiveX add-on. You will see the following system notification at the bottom of the window: “This webpage wants to run the following add-on: “AxMediaControl ActiveX Control Module” from “BEWARD Co., Ltd”



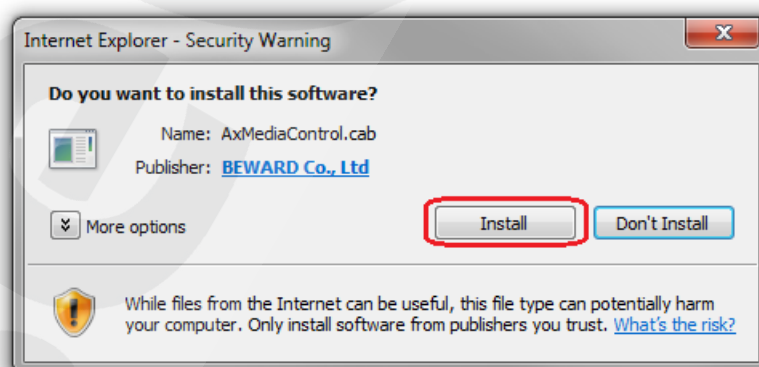
Pic. 3.2

Click **[Allow]** to start installation.

ATTENTION!

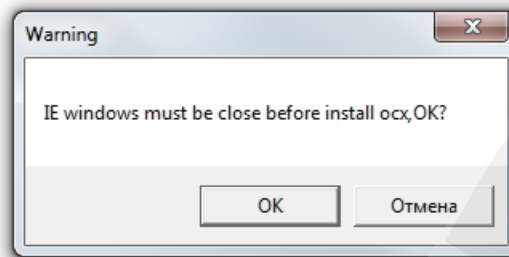
Installation of ActiveX components is only possible for 32-bit Internet Explorer..

Step 4: By default, the Internet Explorer security system will block the ActiveX installation. Click **[Install]** to continue (Pic. 3.3).



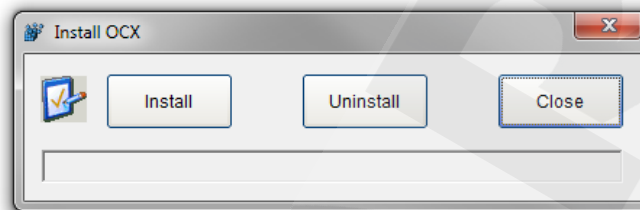
Pic. 3.3

Step 5: Close Internet Explorer and click **[OK]** in the Warning window (see Pic 3.4) if it pops up.



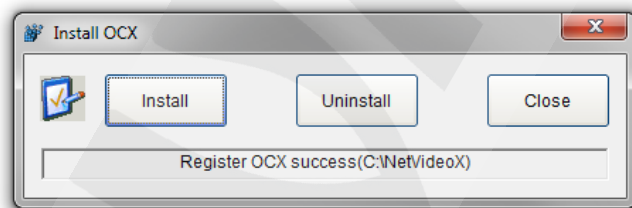
Pic. 3.4

Step 6: Click **[Install]** (see Pic. 3.5).



Pic. 3.5

Step 7: After completing the installation you will see the following «Register OCX success(C:\)» Click **[Close]** (see Pic. 3.6).



Pic. 3.6

NOTE:

Names of menus and option may differ when using different OS and internet browsers.

NOTE:

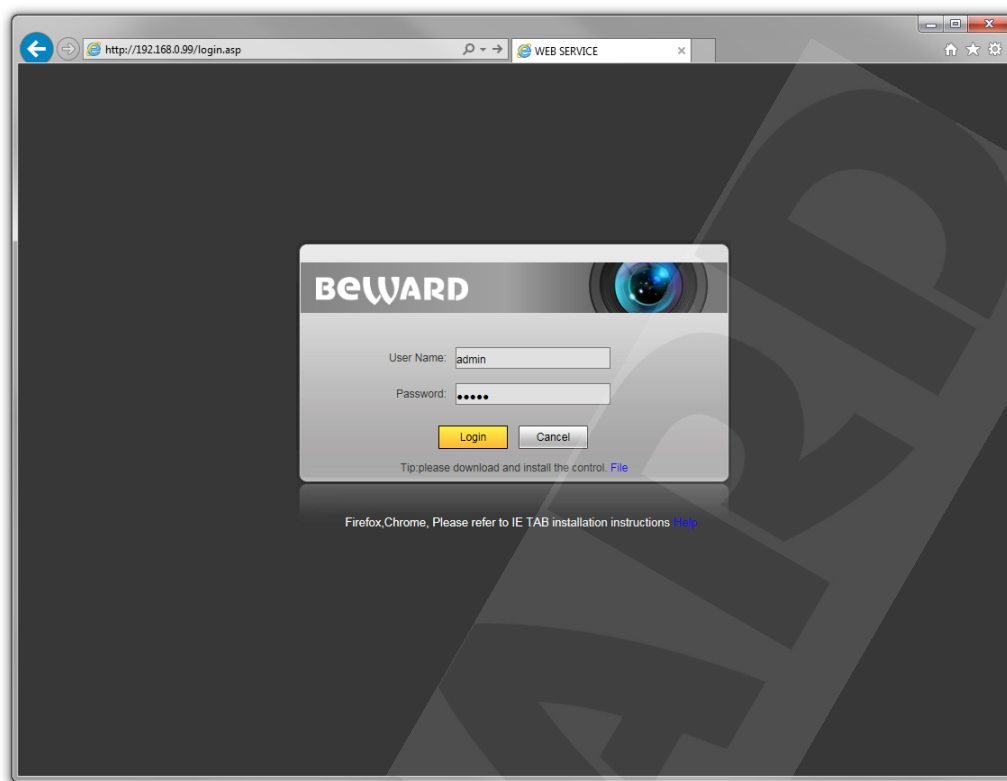
In Windows 7 with enabled user account control you an additional installation blocking window may appear. Give a positive answer permit installation

Step 8: Run Internet Explorer and enter the IP address of the IP Converter in the path field. .

Step 9: Enter username and password and click **[Login]**. Default username – **admin**, default password – **admin** (Pic. 3.7).

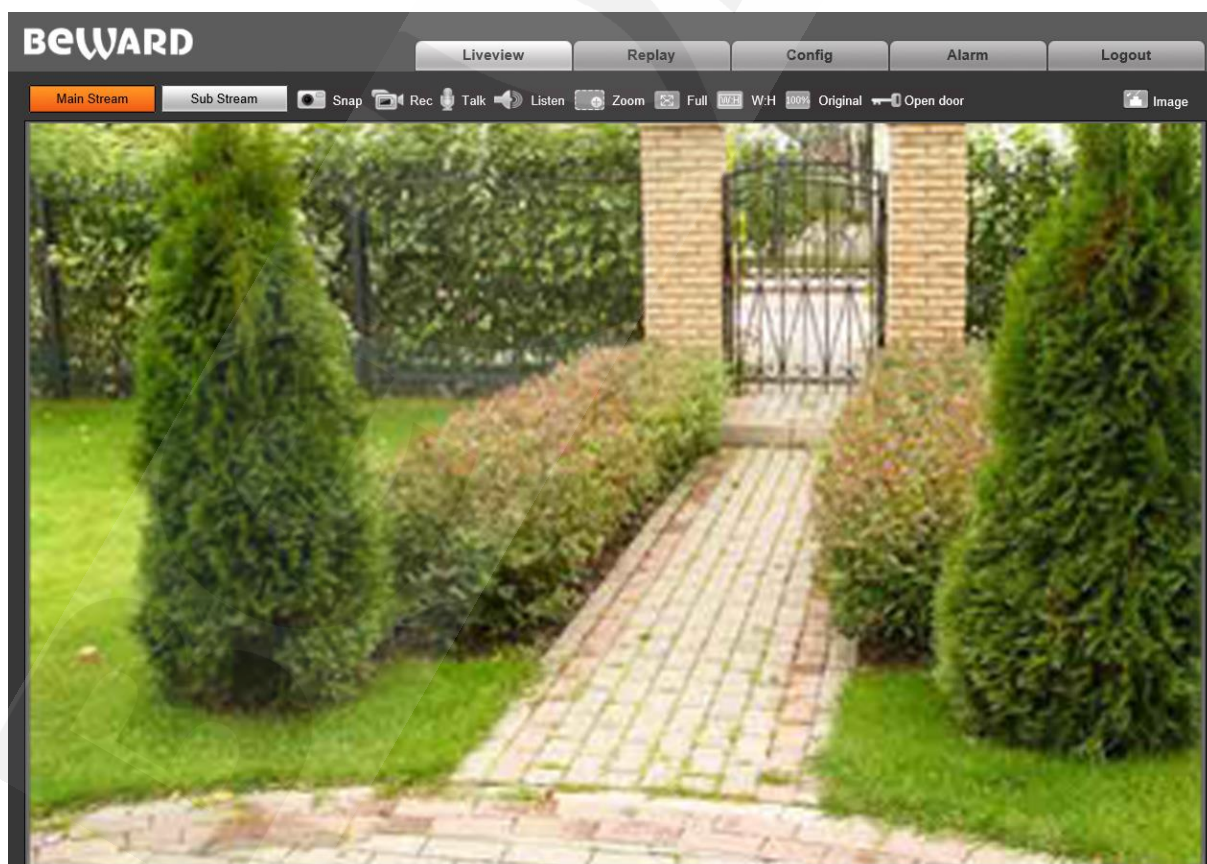
Attention!

After authorization you can change login and password in **Config – System – Access Policy**. If you lose your login and password, you can reset the IP Converter to default settings. To do so you need to press and hold the reset button 3 times for 10 seconds with 1 second pauses between each press



Pic. 3.7

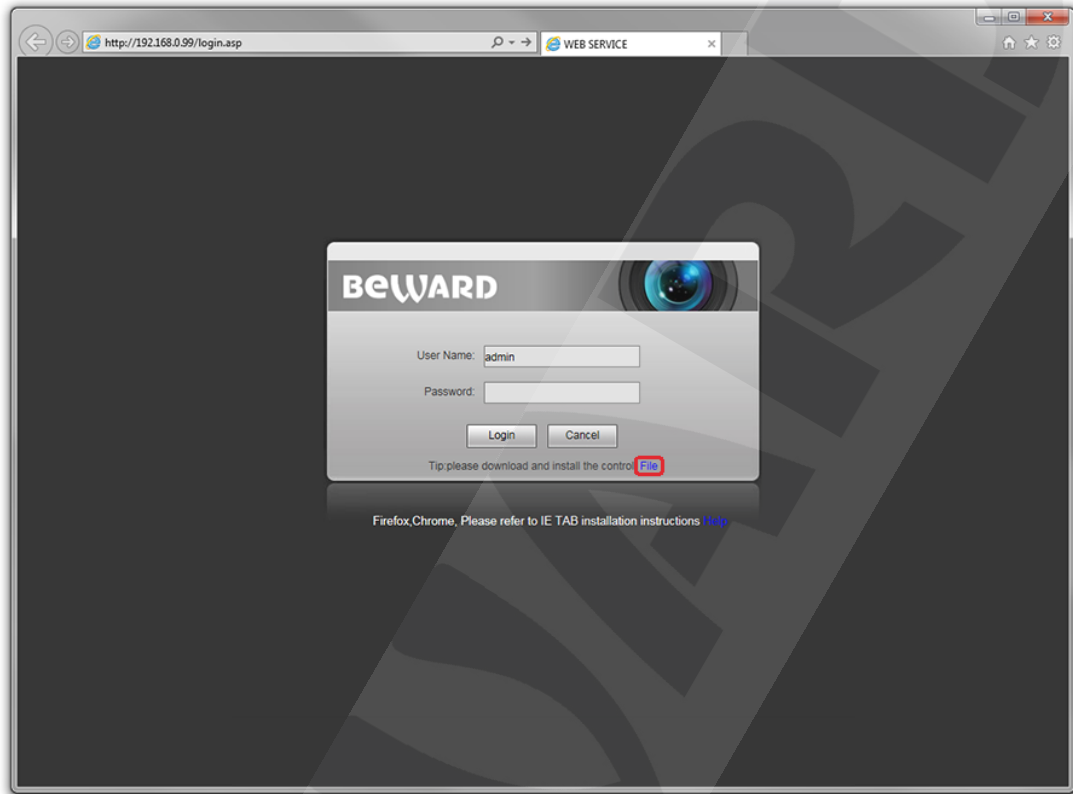
If successful, you will gain access to IP Converter's Web Interface (*Pic. 3.8*).



Pic. 3.8

The interface window has 5 following: **[Live View]**, **[Replay]**, **[Config]**, **[Alarm]**, **[Log Out]**, Each tab is explained in this Manual.

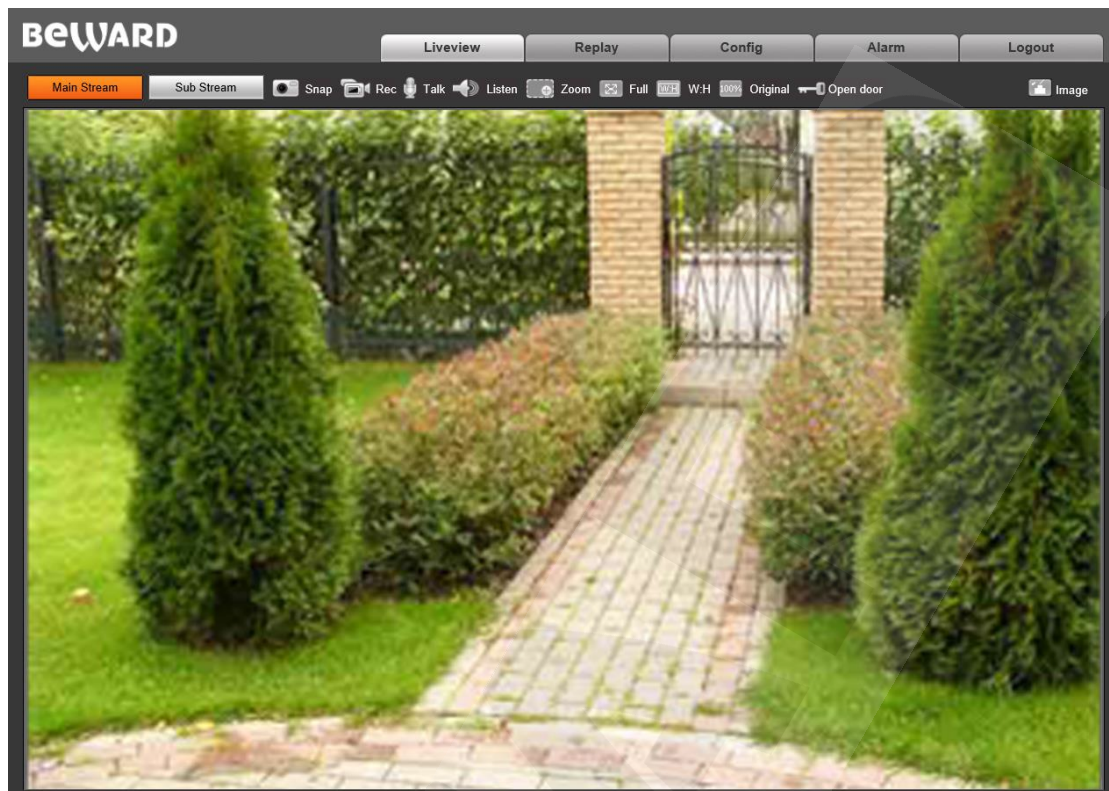
If you failed to install ActiveX correctly you can do it again by clicking the link in the authorization window (see pic.3.9) and following the instructions above



Pic. 3.9

3.2. Main Window (Live View)

The following functions are available in the **[Live View]** tab: Choose Main/Sub video stream., Snapshot. Video recording, “Talk” and “Listen” modes, Zoom, Full Screen mode, “Width:Height” mode, Original resolution, Open door and Image settings.



Pic. 3.11

Main Stream / Sub Stream: Display the main or the sub stream in the Live View window. The main stream is displayed at a higher resolution compared to the sub stream. The stream parameters can be adjusted in **Config – Video Settings – Video coding**(see paragraph [7.2](#)).

Snap: Press this button to make an instant snapshot of the camera display. Snapshots are stored in the local folder specified by the user (see paragraph [5](#)) as JPEG files.

Rec: Press this button to start recoding the livestream. The recorded footage will be saved in the in the local folder specified by the user (see paragraph [5](#)).as H.264 video files

Talk: Press this button to activate the two-way audio mode. When activated, sound transmits from the door station to the PC and vice-versa.

Listen: Press this button to listen to the sound from the door station microphone via PC speakers

Zoom: Press this button to enlarge a specific area of the video. Press **[Zoom]**, then press and hold the left mouse button to frame the area. The enlarged area of the video will appear in a new window. Close the “Zoom In” window and press the **[Zoom]** button to disable this function.

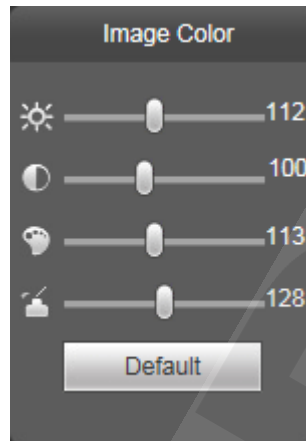
Full: Press this button to enter Full Screen mode. Press the **[ESC]** key or click the right mouse button to turn off Full Screen mode.

W:H: Press this button to apply the correct width to height ratio to the livestream display.

Original: Press this button to display the livestream at the original resolution. If the image is too big to fit the screen, you can use the scrollbars to navigate.

Open door: Press this button to open the door connected to the door station.

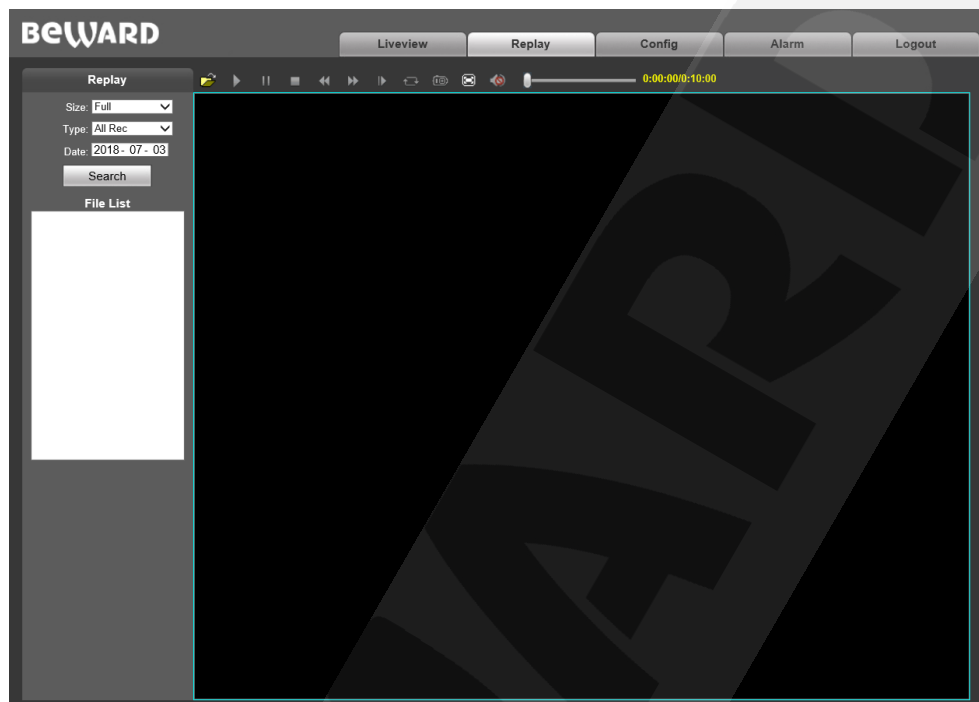
Image: Use this toolbar to adjust the following parameters: «Brightness», «Contrast», «Hue», «Saturation». If you want to restore to the default parameters, click **[Default]** (Pic. 3.12).



Pic 3.12

Chapter 4. Replay

Press «**Replay**», to open the web interface player tab where you can open videos and images that are stored in the memory card or your PC (Pic. 4.1).



Pic. 4.1

Size: Change the width to height ratio. Available options: Full (screen), 4:3, 16:9, 11:9.

Storage: choose the location of the files you saved. Available options : «**PC**» and «**Memory Card**» :

- **PC:** Search for files in a PC folder. The default path is «C:\MyIPCam\».
- **Memory Card:** Search for files in your SD card.

Type: Choose the file Type. Available types: «**All Rec**», «**Alarm Rec**», «**Schedule Rec**» and «**Images**».

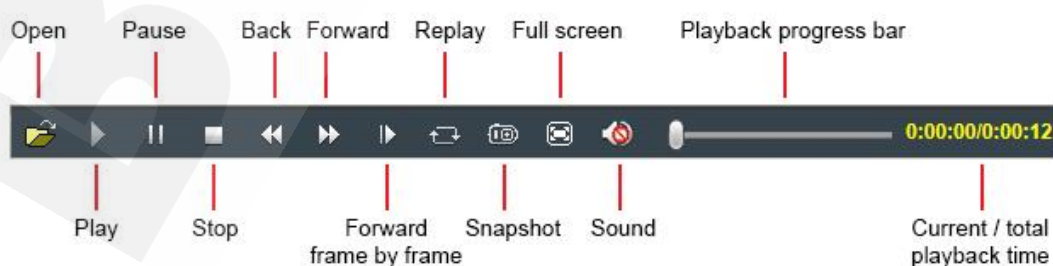
Date: choose the date for searching files.

[Search]: Press this button to start searching files.

File list: The search results are listed here in chronological order

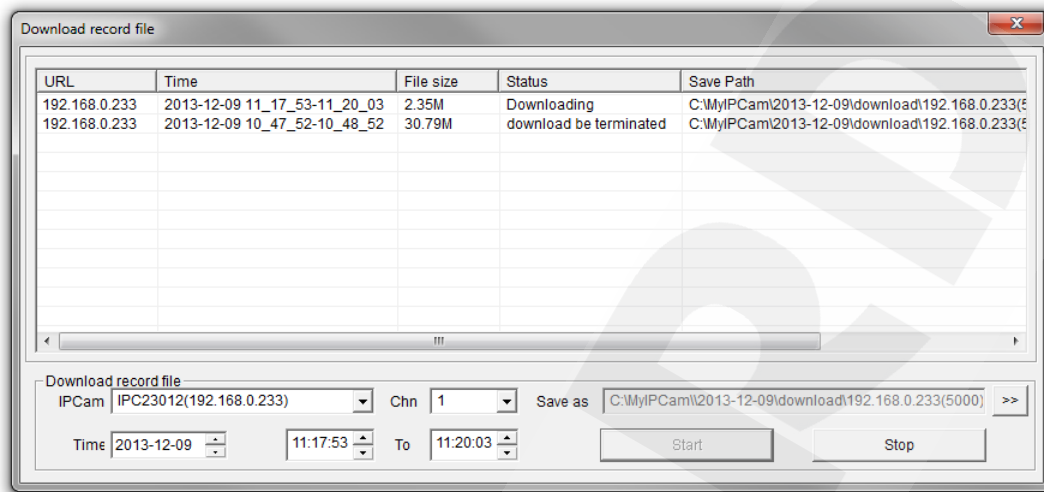
[Play]: Select a file in the File List and press this button to play it.

You can use the following toolbar (see Pic. 4.2).



Pic. 4.2

[Save]: Press this button to save the files from the SD card on your PC. Select a file in the File List and press [Save]. A new window will appear that shows progress (*Pic. 4.3*).



Pic. 4.3

IPCam: Door Station/IP Converter ID and its IP address.

Chn: Channel #, choose "1" for the door station/IP Converter

Time: Set the date and the time period you want to save.

NOTE:

All footage from the time period you set will be saved as one file.

Make sure that you have the rights to create new objects in the storage catalog you chose. In Windows 7 you may need to run Internet Explorer as administrator to allow saving files on the local disk

[>>]: Choose the path to save files.

[Start]: Start saving files.

[Stop]: Stop saving files.

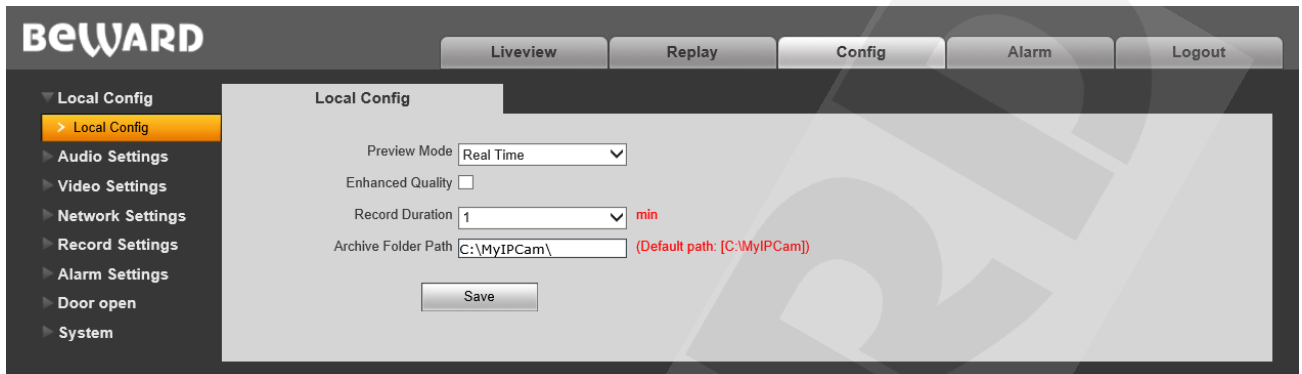
Note!

In Windows 7 (and later OS version) you may have to run Internet Explorer as administrator to ensure that the web interface player is working properly.

Chapter 5. Config: Local Config

Go to the “**Config**” tab to work with settings menu of the device

The following picture shows the **Local Config** menu:



Pic. 5.1

Preview Mode:— «Real Time» and «Fluency» modes are available.

«Real Time» mode does not use the buffering procedure and the videostream is displayed without delay in the «Live View» tab. Any delays and visual defects might be caused by the high load on your LAN.

«Fluency» mode uses the buffering procedure and the videostream is displayed with slight delay (less than 1 second) in the «Live View» tab. Use this mode in case of delay or visual defects.

Enhanced Quality: Enabling this option improves the video quality but also increases the CPU load.

Record Duration: Set the duration of recorded files (in minutes).

Archive Folder Path: Set the local folder to store video and image files. Default Path: C:\MyIPCam\.

NOTE:

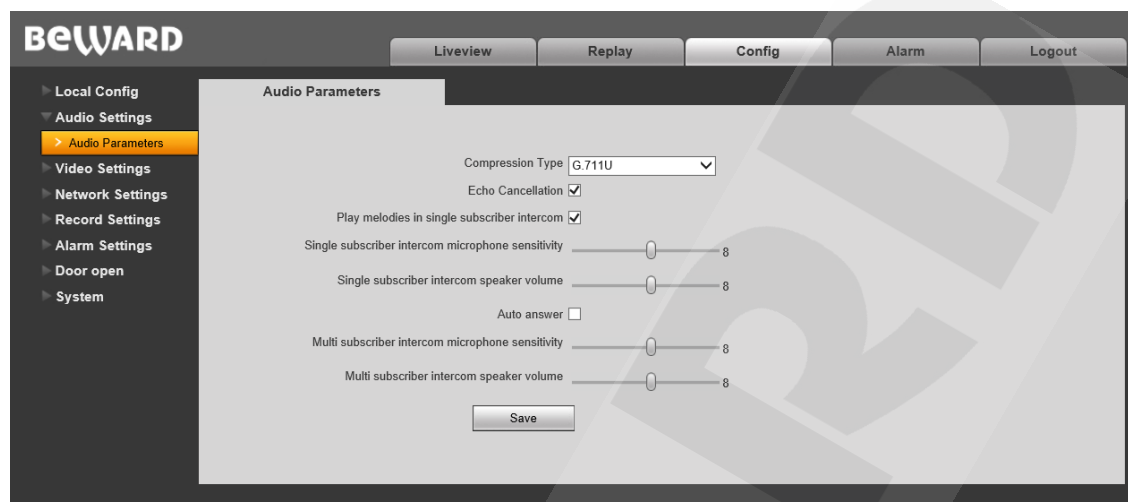
Make sure that you have the rights to create new objects in the archive folder. Otherwise you will be unable to save files.

In Windows 7 you need to run Internet Explorer as administrator to save files in the local disk.

Press **[Save]** to apply new settings.

Chapter 6.Config: Audio Settings

The following picture shows the “**Audio Parameters**” Menu.



Pic. 6.1

Compression Type: Default – G.711U. Also available: G.711A и G.726.

Echo Cancellation: Enable / disable additional echo cancellation. Use this option if the hardware echo cancellation is insufficient.

Play melodies in single subscriber Intercom: if this option is enabled, the call melodies will be played via IP Converter. Disable this option if a single-user intercom monitor is connected to your IP Converter. Otherwise the monitor will play the call melodies.

Single Subscriber Intercom Microphone Volume: set the volume level of single-user video intercom microphone . (0~15).

Single Subscriber Intercom Speaker Volume: set the volume level of single-user video intercom speaker. (0~15).

Auto answer: If this option is enabled, the IP Converter will immediately answer the call (Client-side) from the multi-user video intercom, establishing audio/video connection. Is the option is disabled, the connection will be established only when Client answers the call (make sure your single user intercom monitor is able to turn off video feed in the door station during calls). If you are not using a single-user intercom monitor, disable this option.

Multi subscriber intercom microphone sensitivity: set the microphone sensitivity of the multiuser intercom. (0~15).

Multi subscriber intercom speaker volume: set the speaker sensitivity of the multiuser intercom. (0~15).

See Table 6.1 to see microphone/speaker sensitivity values for popular single-user video intercoms

Single-User Video Intercom	Microphone Sensitivity	Speaker Sensitivity
Kenwei KW-139MCS	12	10
JSB-V05M	10	10
Activision AVC-305	14	13
Kocom KC-MC20	13	11
Polyvision PVD-104CM2	15	12
Quantum QM-305N	12	8
Commax DRC-4CHC	11	14

Attention!

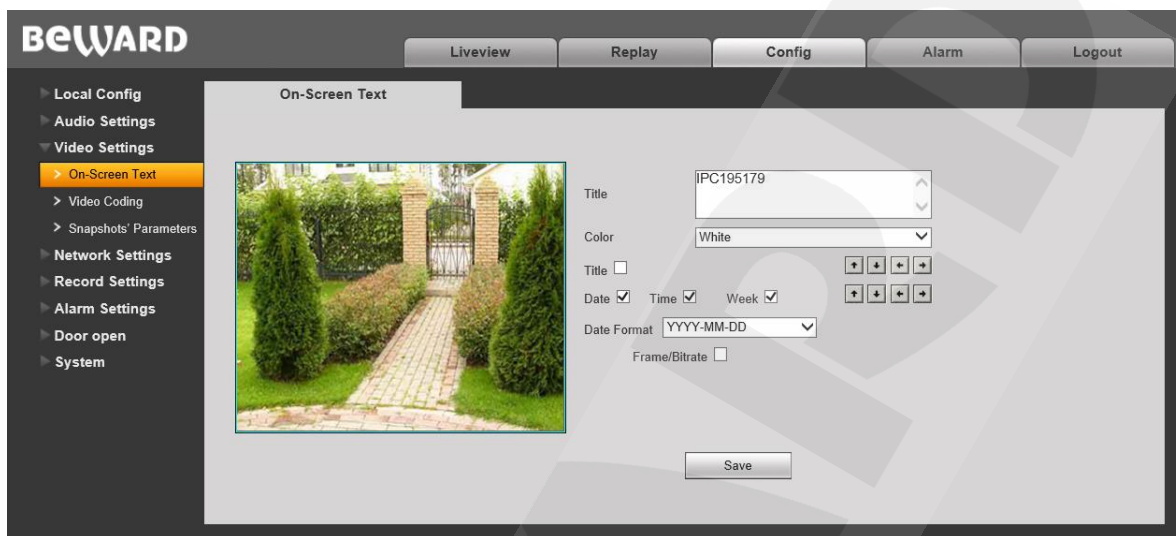
The sound quality depends on the intercoms currently used. After a series of in-house tests, we have found out that sound quality varies in all intercoms.

Press **[Save]**.to apply new settings

Chapter 7. Config: Video Settings

7.1. On-Screen Text

The following picture shows the “On-Screen Text” menu



Pic. 7.1

Title: Enter text (e.g. IP Converter/Door Station name) that will be displayed at the bottom left corner of the screen.


Color: Choose the text color. Available colors: **white, black, yellow, red, blue.**

Title: show/hide title.

Date / Time / Day: show/hide date/ time/ weekday.

Date Format: choose date format.

Framerate / Bitrate: show/hide the current framerate and bitrate on the screen

You can also change positions of the text elements. To do so use . (top row for title, bottom row for everything else).

Press **[Save]**.to apply new changes

7.2. Video Coding

The “Video Coding” menu is shown in *Pic. 7.2*.

This menu contains settings for the Main and Sub streams. The main stream provides the higher resolution and video quality compared to the sub stream. Thus, you can record high quality video via the main stream while watching the sub stream in real time, even in case of low network capacity.

The screenshot displays the 'Video Coding' configuration page in the BEWARD web interface. It is divided into two columns for 'Main Stream' and 'Sub Stream'. Both streams are configured with 'Main Profile' and 'H.264' encoder. The Main Stream has a resolution of 960x480 and Normal quality, while the Sub Stream has a resolution of 640x480 and Basic quality. Both have 'Advanced' settings enabled and 'VBR' rate control. The Main Stream bitrate is 1600 kbit/s and frame rate is 25 fps, while the Sub Stream bitrate is 348 kbit/s and frame rate is 25 fps. Both have an I-frame of 50. There are 'LAN' and 'WAN' buttons for each stream, and a 'Save' button at the bottom. A note at the bottom indicates that LAN and WAN refer to default settings.

Pic. 7.2

Profile: Baseline and Main profile are available.

Encoder mode: H.264 and MJPEG formats are available.

Resolution: set the stream resolution

- Main stream: 1280x960, 1280x720;
- Sub stream: 720x576, 640x480, 320x240.

Quality: “Basic”/”Normal”/”Fine”.

NOTE:

You can change quality only if the «**Advanced**» option is disabled.

Advanced: Enabling this option grants access to the following parameters. :

Rate control: Choose the type of bitrate control:

- **CBR:** Constant bitrate is prioritized while the image quality may change over time. The current bitrate value approaches the bitrate value you specify in the “Bitrate” field. You can also specify permitted deviation in the “Bitrate fluctuation” field.

VBR: Image quality is prioritized, while the bitrate may vary, according to different conditions in the surveillance area. The average bitrate value will approach the value you specify in the “Bitrate” field but the current value may vary significantly

Bitrate fluctuation: «Self-adaption» means that the bitrate value will be controlled by software. By selecting « $\pm 10\%$ » ~ « $\pm 50\%$ » the bitrate will change according to surveillance conditions within the permitted deviation

Bitrate: set the data transmission speed (available range: 30 ~ 16384 kbit/s). Higher bitrate value results in higher image quality as well higher resource requirements

Frame rate: Set the framerate. it is not recommended to set to high value at low network bitrate, which would result in choppy video.

I frame: Set the interval of I-frames. Available range: 1-200. Lower value results in higher bitrate and higher image quality. It is recommended to set to the same value as the framerate.

[LAN], [WAN]: Templates of coding settings – allow to set the recommended value for LAN and WAN connections with one click.

[LAN]:

- Main stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 4096 kbit/s
- Sub stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 512 kbit/s

[WAN]: «I-frame» – 25, «Frame» – 5 fps, «Rate control» – VBR, «Bitrate» – 384 kbit/s.

Press **[Save]** to apply new settings.

Chapter 8. Config. Network Settings

8.1. Basic

The “Basic Settings” menu is shown below.

The screenshot shows the BEWARD web interface. At the top, there are tabs for Liveview, Replay, Config, Alarm, and Logout. The left sidebar contains a tree view of configuration options: Local Config, Audio Settings, Video Settings, Network Settings (expanded), Basic (selected), LAN, PPPOE, UPnP, E-mail, FTP, DDNS, VPN, RTSP, HTTPS, SIP, Record Settings, Alarm Settings, Door open, and System. The main content area is titled 'Basic Settings' and contains the following fields:

- Data Port: 5000
- HTTP Port: 80
- ONVIF Port: 2000
- Activate USB for 4G modem: ☐
- ☐ Enable port forwarding
- ☒ Automatic UPnP-server address
- UPnP-server: 192.168.0.1
- External IP address:
- Data port: 0
- HTTP port: 0
- RTSP port: 0
- ONVIF port: 0
- Save button

Pic. 8.1

Data Port: Port used for video data transmission. Default value – 5000. Recommended values – 1124-7999 (This field is not recommended to change without necessity).

HTTP Port: Port used for a web browser. Default value – 80. Recommended values – 80 и 1124-7999 (This field is not recommended to change without necessity).

ONVIF port: Port used for ONVIF protocol. Default value – 2000. Recommended values – 1124-7999 (This field is not recommended to change without necessity).

Activate USB for 4G modem: enable this option to use the device's USB socket to connect the 4G modem.

1. Enable **Activate USB for 4G modem**
2. Press **[Save]**
3. Turn off power
4. Connect the 4G modem to the IP Converter via USB socket.
5. Turn on power

See [8.13](#) for 4G settings.

ATTENTION!

If you are using DK103MW with the pre-installed Wi-Fi module, then the Wi-Fi will turn off the moment you enable USB for 4G modem. Wi-Fi and 4G cannot be used simultaneously.

Enable port mapping – The IP Converter connects to the router and automatically forwards its ports behind NAT.

Note: *Automatic port mapping must be supported by your network hardware.*

Automatic UPnP-server address: the devices will automatically look for a UPnP server that supports port mapping. Enabled by default.

UPnP server – IP address of the server that will automatically forward ports behind NAT Address. If there multiple available UPnP servers available, enter the desired address into the field manually (**Automatic UPnP-server address** must be disabled). By default, the address is a wired or wireless (if using Wi-Fi) gateway. If the device has two active interfaces (Wi-Fi and LAN), then the main Wi-Fi gateway will be used as a UPnP server.

External IP address: external IP address of the device as it seems from “Behind NAT”. Read only.

Data Port/HTTP Port/RTSP Port/OnVIF Port: redirected external ports of the device, received via router. Read only. If redirection is unsuccessful, the value is «0»

Press **[Save]** to save new settings.

8.2 LAN

The “LAN” settings menu is shown below.

Pic. 8.2

Enable IPv6: Allows 128-bit IP addresses for IP Converter connections.

DHCP: Automatically receive main network parameters from a DHCP server (The server must be set up in local network).

IP Version (available if IPv6 is enabled): Select «IPv6», to use 128-bit IP addresses

IP address: Enter IP address if DHCP is disabled.

Subnet mask: Default value is 255.255.255.0 (This field is not recommended to change).

Gateway: set the gateway address.

Main DNS: set the preferable DNS address.

Sub DNS: set the alternative DNS address.

MAC: MAC address of the IP Converter (This field is not recommended to change).

NOTE:

IP addresses in the network must be unique when assigning an IP address to the IP Converter. Applying new settings in the “LAN” menu requires a reboot.

ATTENTION!

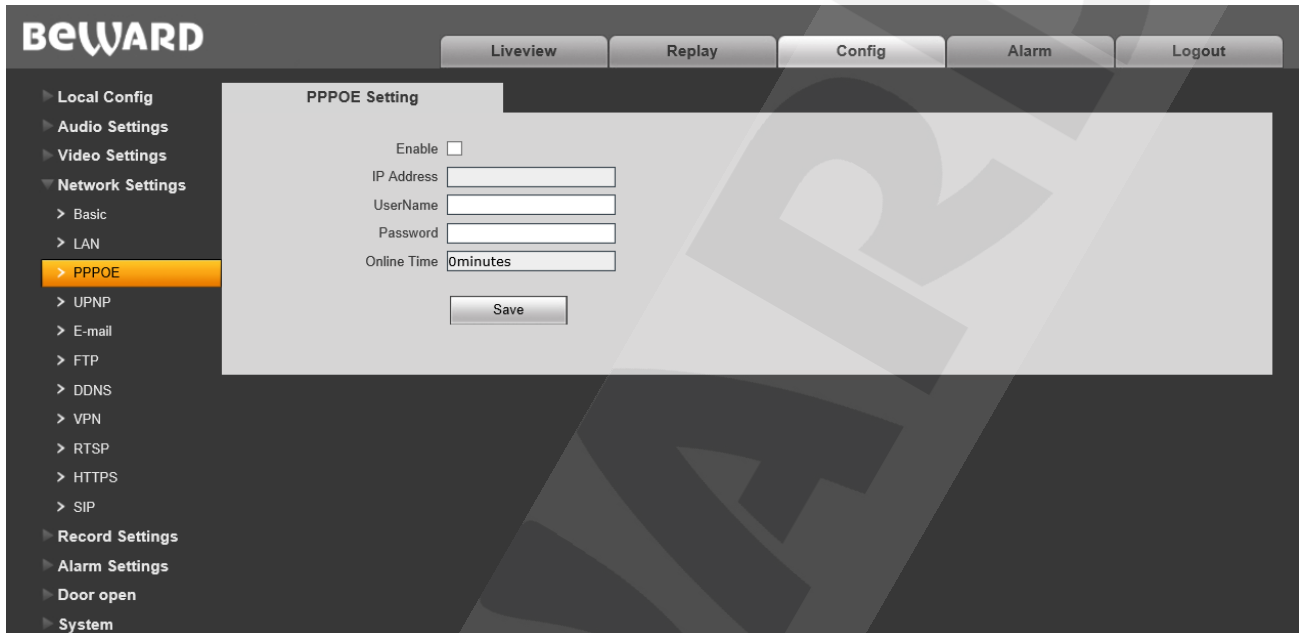
After changing the network settings the IP Converter will automatically reboot .

Press **[Save]**.to apply new settings

8.3. PPPoE

The “PPPoE” settings menu is shown below.

This menu allows setting up the PPPoE network that can be used to connect the IP Converter to the Internet after obtaining the dynamic IP address, username and password from your Internet Provider.



Pic. 8.3

Enable: Enable/disable PPPoE.

Authentication Type: choose the authentication protocol.

IP address: IP address or domain name of the PPPoE server (given by the server)

Username: enter your username for the PPPoE connection.

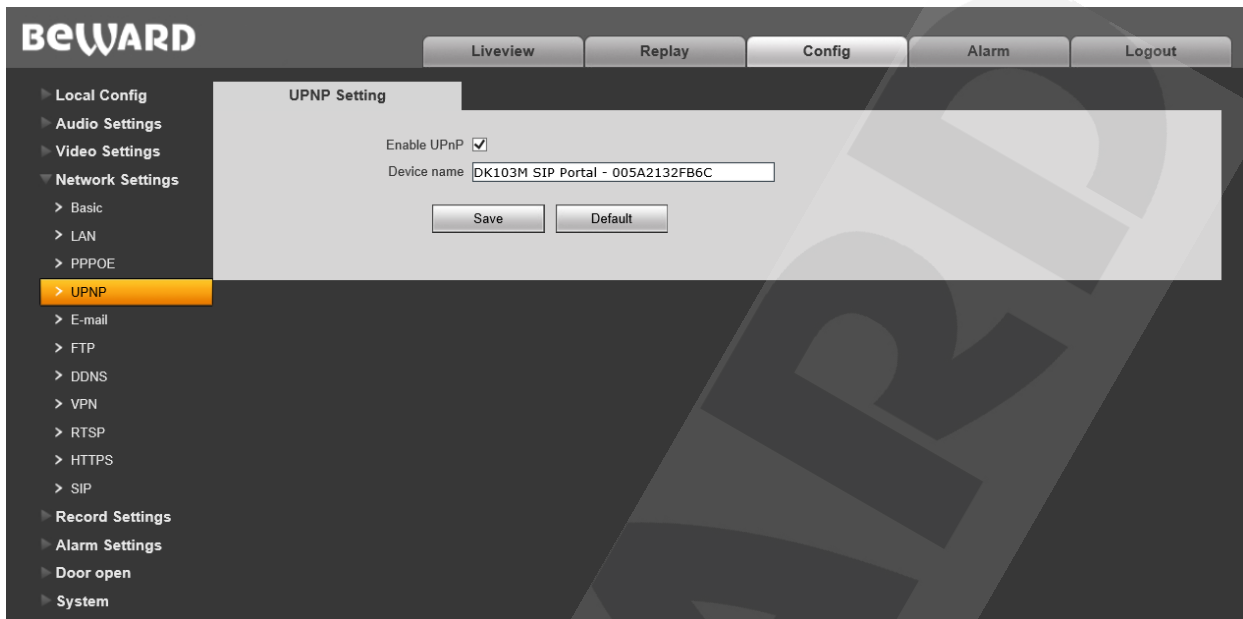
Password: enter your password for the PPPoE connection.

Online Time: Duration of connection.

Press [**Save**] to apply new settings.

8.4 UPnP

The “UPnP” settings menu is shown below



Pic. 8.4

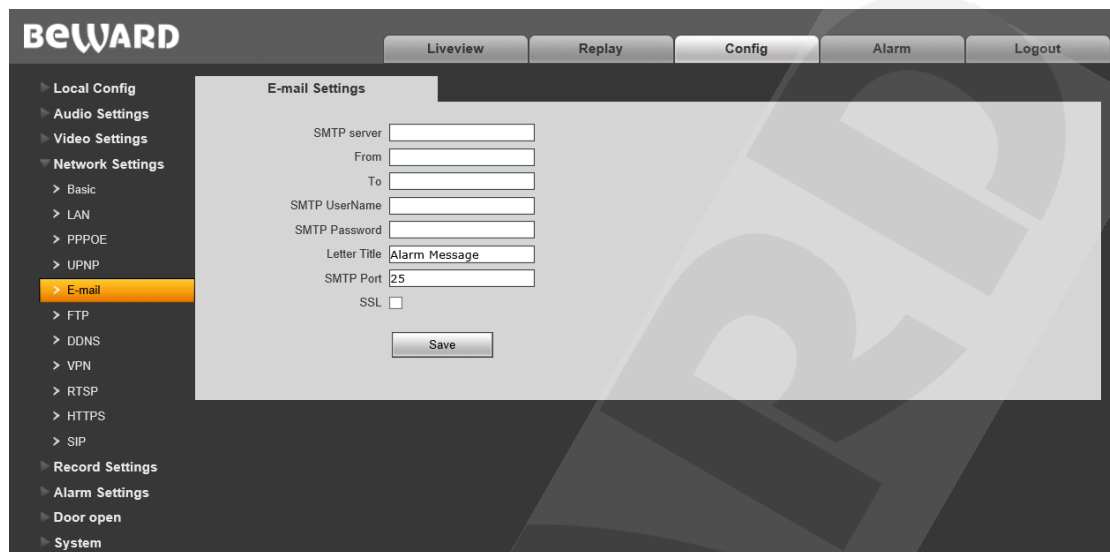
Enable UPnP: enable/disable network detection via UPnP

Device name: Name that will be displayed in UPnP search results.

Press **[Save]** to apply new settings.

8.5. E-mail

The “E-mail” settings menu is shown below



The screenshot shows the BEWARD web interface. At the top, there are tabs for Liveview, Replay, Config, Alarm, and Logout. The left sidebar lists various configuration categories: Local Config, Audio Settings, Video Settings, Network Settings (expanded), Basic, LAN, PPPOE, UPNP, E-mail (highlighted), FTP, DDNS, VPN, RTSP, HTTPS, SIP, Record Settings, Alarm Settings, Door open, and System. The main content area is titled 'E-mail Settings' and contains the following fields:

- SMTP server: [text input]
- From: [text input]
- To: [text input]
- SMTP UserName: [text input]
- SMTP Password: [text input]
- Letter Title: [text input] (value: Alarm Message)
- SMTP Port: [text input] (value: 25)
- SSL: [checkbox]

A 'Save' button is located at the bottom of the form.

Pic. 8.5

This menu contains parameters of the e-mail client used to send image snapshots via e-mail.

SMTP server: Enter the IP address or the name of the SMTP server in use.

From: enter the sender's e-mail address

To: enter the receiver's e-mail address. Mail messages will be sent to this address.

SMTP Username: enter your username to access the SMTP server.

SMTP Password enter your password to access the SMTP server.

SMTP port: enter the port number of the SMTP server (default value – 25).

SSL: enable if your Internet provider requires SSL.

Press **[Save]** to apply new settings.

8.6. FTP

The “FTP” settings menu is shown below:

Pic. 8.6

This menu contains parameters of the FTP client used for sending video footage and snapshots to the FTP server. You can set up 2 servers. If the main server is not available, the sub server can be used instead

Address: IP address of the FTP server.

Port: port of the FTP server.

FTP Catalog: Set the folder for recorded files on the FTP server. If the folder does not exist, it will be created automatically in the root server folder.

Username / Password: enter your username and password to access the FTP server.

Port from /to: Range of ports to access the FTP server.

NOTE:

Make sure you have enough rights to save files to the FTP server in use

Press [**Save**] to apply new settings.

8.7. DDNS

The “DDNS” settings menu is shown below:

The screenshot displays the BEWARD web interface for DDNS configuration. The left sidebar lists various settings categories, with 'DDNS' highlighted under 'Network Settings'. The main configuration area includes an 'Enable' checkbox, a 'URL' field with 'noip.com' as a hint, a 'Service Provider' dropdown menu, and input fields for 'UserName', 'Password', and 'Domain'. Below these are fields for 'Server URL' (pre-filled with 'www.noip.com'), 'Server Port' (30000), 'Data port' (5000), 'HTTP port' (80), and an 'Update Interval' dropdown set to '30 minutes'. A 'Save' button is located at the bottom of the form. A small text note at the bottom left of the form area says 'Domain e.g. test1.noip.com'.

Pic. 8.7

This menu contains parameters for setting the connection via DDNS service. DDNS allows you access the IP Converter from the Internet even if you only have a dynamic IP address.

Every time your current IP address is changed, it is automatically compared with the specific domain name used to access the IP Converter from the Internet at any moment.

Enable: enable/disable DDNS.

DDNS server: select DDNS provider from the list.

Username: enter the username obtained from the DDNS provider website after registration.

Password: enter the password obtained from the DDNS provider website after registration.

Domain: enter the domain name obtained after registration.

Server URL: enter the URL address of the DDNS provider.

Server Port: enter the port used for DDNS. Default value: 30000 (This field is not recommended to change).

Data port: enter the data port used for port mapping.

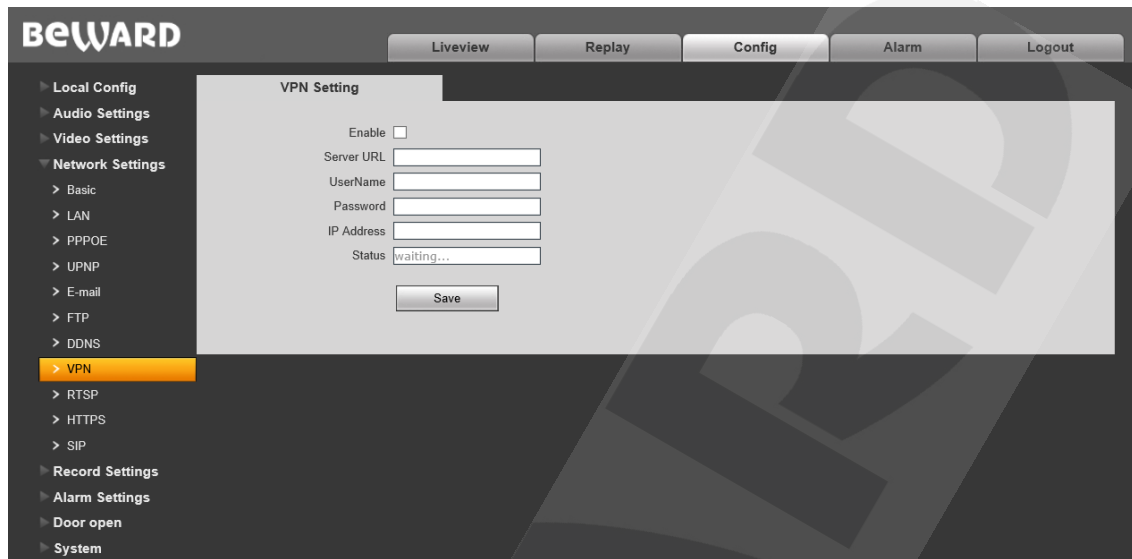
HTTP port: enter the HTTP port used for port mapping.

Update Interval: set the interval at which the device will update IP address on the DDNS server after IP address change.

Press **[Save]** to apply new settings.

8.8. VPN

The “VPN” settings menu is shown below:



The screenshot displays the BEWARD web interface for VPN configuration. The top navigation bar includes 'Liveview', 'Replay', 'Config', 'Alarm', and 'Logout'. The left sidebar lists various settings categories, with 'Network Settings' expanded and 'VPN' selected. The main content area, titled 'VPN Setting', contains the following fields:

- Enable:** A checkbox to toggle VPN functionality.
- Server URL:** A text input field for the VPN server's address.
- UserName:** A text input field for the VPN username.
- Password:** A text input field for the VPN password.
- IP Address:** A text input field for the IP address assigned after connection.
- Status:** A text field showing the current connection status, currently displaying 'waiting...'.

A 'Save' button is located at the bottom of the form to apply the changes.

Pic. 8.8

Enable: enable/disable VPN.

Server URL: enter the IP address or the domain name of the VPN server.

Username: enter your username to access the VPN server..

Password: enter your password to access the VPN server.

IP address: IP address obtained after connecting to the VPN server

Status: Current connection status.

Press [**Save**] to apply new settings.

8.9. RTSP

If RTSP is enabled you will be able to watch the video stream from the IPConverter/door station in real time via third-party players that support standard RTSP protocol (VLC, Quick Time, Real Player etc.).

Enter the following request to access the video stream via third party RTSP clients
rtsp://<IP>:<PORT>/av<X>_<Y>

- **<IP>** – IP address of the device;
- **<PORT>** – RTSP port of the device (default value – 554.);
- **<X>** – command of the video stream channel. The channels begin with 0. Since the IP Converter/door station has a single channel, enter “0”
- **<Y>** – command of the video stream profile: 0 – main stream, 1 – sub stream.

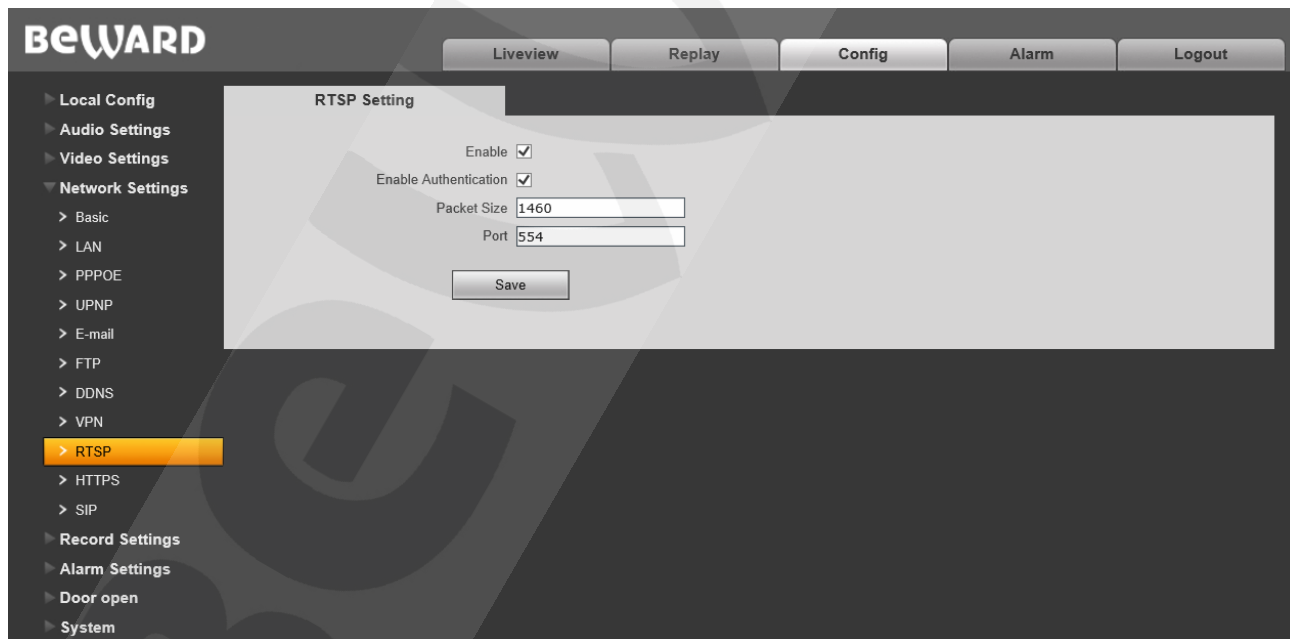
Request example: **rtsp://192.168.0.99:554/av0_0.**

The coding type for the video stream is specified in the coding settings.

NOTE:

When you connect to the device from the Internet the bitrate depends on the access channel obtained from the ISP.

The “RTSP” settings menu is shown below:



Pic. 8.9

Enable: enable\disable RTPS.

Enable Authentication: Turn on the authorization procedure when getting access to the RTSP stream. The following request must be used to gain access:
rtsp://<IP>:<PORT>/av<X>_<Y>&user=<USER>&password=<PASS>, whee **<USER>** – username, **<PASS>** – password.

Request example: `rtsp://192.168.0.99:554/av0_0&user=<admin>&password=<admin>`.

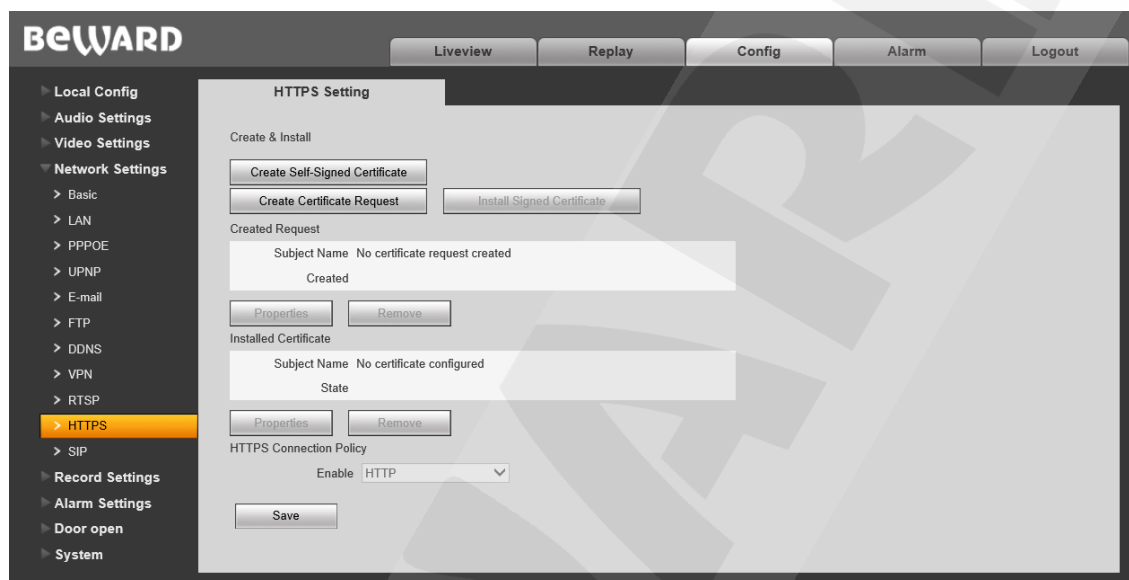
Packet Size: set the size of the data packet. Default value: 1460.

Port: RTSP port. Default vale: 554.

Press **[Save]** to apply new settings.

8.10. HTTPS

The “HTTPS” settings menu is shown below:



Pic. 8.10

Before using HTTPS connection you need to set parameters in the web interface client.

You can create a self-signed certificate or make a request to the Certification authority to create the certificate

[Create Self-Signed Certificate]: Click to create a new self-signed certificate. Fill in the fields in the pop-up window and click **[Submit]**. The created certificate will be shown in the “Installed Certificate” field.

[Create Certificate Request]: Click to make a request to the Certification authority . . Fill in the fields in the pop-up window and click **[Submit]**. The created request will be shown in the “Created request” field.

Created request: request to the Certification authority.

[Properties]: Examine the information on the certificate request that will be sent to the Certification authority.

[Remove]: remove the certificate request.

[Install Signed Certificate]: Install the certificate you received from the Certification authority in response to your prior request. Pressing this button will open a new window where you can upload your certificate. Choose the certificate file (“.pem”) and click **[Upload]**. The certificate must match the request because the data are compared during installing.

NOTE:

Change Internet Explorer security settings to be able to upload files from local folders. Go to **Tools – Internet options – Security** and click **[Custom level]**. Find «**Include local directory path when uploading files to a server**» and select «**Enable**» (*Pic. 13.5*).

Installed Certificate: name and state of the installed certificate.

[Properties]: examine the properties of the current certificate

[Remove]: remove current certificate.

HTTPS Connection Policy: select protocol in use. Available protocols: HTTP, HTTPS, HTTP & HTTPS.

If you are using port forwarding on your router, please note TCP Port 443 is used for the HTTPS protocol.

Press **[Save]** to apply new settings.

8.11. SIP

The “SIP” settings menu is shown below:

The screenshot displays the BEWARD web interface's 'SIP configuration' menu. The interface is divided into a sidebar on the left and a main configuration area. The sidebar lists various settings categories: Local Config, Audio Settings, Video Settings, Network Settings, and Record Settings. The 'Record Settings' category is currently selected. The main configuration area is titled 'SIP configuration' and contains two columns of settings for SIP #1 and SIP #2. SIP #1 settings include Name (401), Number (401), Username (401), Password (***), SIP port (5060), and registration status (Registered). SIP #2 settings include Name, Number, Username, Password, SIP port (5060), and registration status (Not registered). Both sections have checkboxes for enabling SIP and registration, and fields for registration server, proxy server, and NAT. A 'Save' button is located at the bottom of the configuration area.

Pic. 8.11

Before using SIP connection you need to set parameters in the web interface client.

Enable SIP #1 (#2): Activate SIP account. Only a one account can be active at one time. Both accounts are disabled by default.

Name: Name of the device. Displayed during calls. This field is empty by default.

Number: Number of the device used for calls by other subscribers. This field is empty by default.

Username/Password: used to register the device in the SIP server. This field is empty by default

SIP port: Number of the port used for interactions with a SIP user agent. Default number - 5060.

Allow registration: Allow the device to be registered in the SIP server. Disabled by default.

Get the registration server by DHCP: Check to enable this option. SIP server must support this function.

Registration server/Port: The network address and port of the registration server. The network address may match the SIP server address. These fields are empty by default.

Registration status: Account status in the SIP server.

Get proxy server by DHCP: Check to enable this option. SIP server must support this function.

Proxy Server/Port: network address and port of the Proxy server.

SIP Server/Port: network address (for telephone exchange) and port (for data exchange) of the SIP server. These fields are empty by default.

NAT: the device operates via a STUN server. STUN server is one of the secure ways of getting access to devices within the network that are behind NAT. Disabled by default.

STUN IP/STUN port: network address and port of the STUN server.

ATTENTION!

STUN does not work properly with symmetric NAT. When using symmetric NAT the IP address of the STUN server will differ from the endpoint address. Therefore the NAT address seen by the STUN server will also differ from the endpoint address used for sending data to the user agent..

DTMF Mode: select DTMF signal transmission mode. Available modes:

- RFC2833 – send DTMF tones within RTP packages.
- In-Band – DTMF signals are found in the media stream; G.711 alaw/ulaw only.
- SIP INFO – send DTMF tones within INFO-messages.

Call account: call recipient(s) by pressing the “Call” button. «SIP 1» is selected by default. If SIP 1 is not available, the value switches to «SIP 2» (and vice versa).

Call abonent 1-5: Select the recipients that must be called when the “Call” on the door station is pressed. These fields are empty by default.

Stream Type: Select the type of stream transmitting during SIP sessions between the Guest and the Client. Applied for both accounts. The main stream is selected by default. “Audio only” is also available.

Door open (DTMF): set the value of the DTMF signal. The relay outputs will close when the signal is received. For example, the door will open when the specified phone button is pressed. Up to 3 DTMF symbols are available (0-9, #, *). These fields are empty by default.

Break call after door close: when the “open the door” command is received (the IP Converter receives the DTMF signal to close the relay outputs) the current SIP session ends. This function can be set up for each relay output separately. This function is disabled by default.

Use call melody: use standard call melody instead of the phone ringing sounds when calling recipient via SIP.

Repeat count: set how many times the call melody should be repeated. If the value is set to «0» the ringtone melody will play an infinite amount of times.

Click **[Save]** to apply new settings.

BEWARD

8.12 Wi-Fi

ВНИМАНИЕ!

При включенной опции «**Активировать USB для 4G модема**» в Основных LAN настройках, опция Wi-Fi отключается.

DK103MW is capable of transferring data from IP converter via WiFi standard IEEE 802.11 b/g (up to 54 Mbps). The wireless module is working in the “Infrastructure” mode. Each IP converter connects via Access Point (AP). In the “Infrastructure” mode (i.e. Client/Server), the wireless network is made up of at least a single AP (connected to the wired router) and any number of wireless end-user devices (in our case, wireless IP Converters).

The Wi-Fi settings page is shown below:

Рис. 8.12

Enable: activate Wi-Fi connection. Disabled by default.

DHCP: enable this option to automatically receive network parameters from the Wi-Fi. Make sure that DHCP server is activated in AP settings.

IP address: enter IP address manually if DHCP is disabled in AP settings.

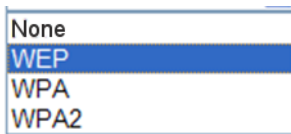
ВНИМАНИЕ!

IP address and gateway for wireless interface should not match with IP address and gateway for wired. The addresses should belong to different ! Например, вы можете установить IP адрес для проводного интерфейса 192.168.0.99 и для беспроводного 192.168.1.99, но не можете установить для проводного интерфейса IP адрес 192.168.0.99 и для беспроводного 192.168.0.100!

Subnet mask: the default value is 255.255.255.0 (it is not recommended to edit this parameter).

Gateway: set the gateway address, usually it is the IP address of a Wi-Fi access point.

SSID: (up to 32 ASCII symbols) – unique name assigned to the wireless network. Make sure it matches the SSID parameter of WiFi AP.



Encryption: set encryption parameters to ensure the wireless connection is secure. Available values – **None, WEP, WAP, WPA2**.

General information about wireless connection security

To prevent unsanctioned access to your wireless networks it is advised to pay close attention to security matters.

A wireless Access Point supports several kinds of protection of Wi-Fi networks via various encryption/identification methods and algorithms (WEP, 802.1x, 802.1x c WEP, WPA-PSK, WPA-AES and WPA RADIUS).

Using one of several encryption types will greatly decrease the chance of data interception and unsanctioned access to your wireless networks. 64 bit key WEP is the simplest and most vulnerable encryption protocol. It must be used only when it is the only supported protocol.

WEP (Wired Equivalent Privacy), WPA, WPA2 security protocols maintain a unified infrastructure for managing access, protection and encryption of data via Wi-Fi. Activate WEP or WPA to secure wireless connections.

WPA protocol, which replaced WEP, is primarily based on subset of IEEE 802.11i standard. WPA2 is based on the final revision of the IEEE 802.11.i standard. WPA utilizes several encryption methods and algorithms, including TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) to improve reliability for methods of encryption and key management. Most contemporary wireless devices are WPA compatible.

WEP and WPA encrypt data, transferred between Access Point and remote clients. In other words, the key (a set of symbols), which is known to both AP and the client, is used to encrypt and decipher data, transferred between the two devices. If a hacker has the key, he can use it to decipher the data or establish connection to AP.

WEP's biggest drawback is that the encryption key must be entered manually on both devices.

To avoid the same weakness, WAP encryption protocol is supplemented by key management functions. Like in WEP, a key is used to encrypt data. But it is entered only once. Then WPA generates the actual encryption key. WPA regularly generates a new key. Therefore. In case of hacking the encryption key, the hacker will be able to use it only until a new key a generated automatically.

The best option is WPA Pre-Shared Key (WPA-PSK) which guarantees sufficiently reliable protection and is easy to set up.

To set up WPA-PSK you need to select the WPA Pre-Shared Key parameter. In AP, there are three WPA algorithms: TKIP, AES and TKIP+AES. TKIP is an outdated protocol, meant to solve the many problems of WEP before the next generation of WPA (WPA2) became popular. TKIP uses that same encryption algorithm as WEP, but avoid many of its issues by using a dynamically changing encryption key, encryption of configuration data (WEP uses a regular text file) and MIC (Message Integrity Checks). AES is the modern, exceptionally secure encryption algorithm, based on 802.11i and WPA2.

After selecting preferred operation mode, a WPA Shared Key must be entered. The same key must be entered for all clients that are connected to the AP. A long, hard-to-guess key is preferred. The key must be at least 8 character long, but no more than 63 ASCII symbols.

Attention! Avoid using a 20+ symbol long key, as it may severely slow down the performance of the AP.

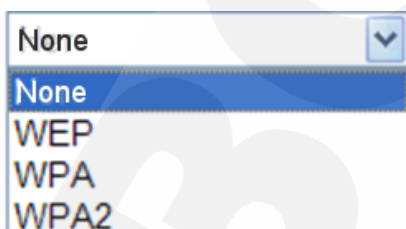
If the clients are not WPA compatible, using WEP is better than not using encryption at all. To set up WEP select Shared Key security mod in the Advanced Settings menu, select a key (1-4) as the standard encryption key and whether the WEP key is 64 bit or 128 bit in hexadecimal or ASCII formats, Fill the Key field with a corresponding standard key. For example, If the key standard is 64 bit hexadecimal, then enter a key which consists of ten hexadecimal digits. Repeat this step in all client devices.

Attention! The WEP configuration procedures varies greatly depending on the device.

From least reliable to most reliable, the encryption methods are places as follows :

- **WEP 64 bit**
- **WEP 128 bit**
- **WPA TKIP**
- **WPA2 AES**

IP Converter: Encryption of wireless connection



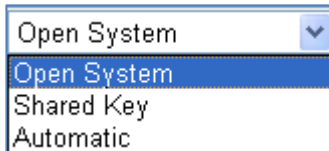
If **NONE** is selected, the device connects to an open network without encryption.

When using this option, you only need to make sure to enter a valid SSID.

WEP encryption

When this option is selected, enter the **Password** to connect to a secured network.

For this device WEP hexadecimal 128 bit key encryption is used. To enable encryption, enter the hexadecimal key into the Password field. The key must be 26 symbols long. This way, the IP device may connect to the AP that has the matching encryption key (WEP 128 bit HEX).



A screenshot of a web interface dropdown menu titled 'Identification'. The menu is open, showing four options: 'Open System' (selected), 'Open System', 'Shared Key', and 'Automatic'.

In the **Identification** menu select **Open System**, **Shared Key** or **Automatic** (recommended) authentication mode.

Attention: The following parameters should match in both the IP Converter and the AP: Encryption keys, Encryption parameters, SSID.

WPA Encryption

WPA (Wi-Fi Protected Access) provides high-grade protection for your wireless networks and data transfer. WPA uses constantly generated password-based encryption keys via TKIP protocol. No two keys are ever the same, which significantly reduces the risk of unsanctioned access.



A screenshot of a web interface dropdown menu for 'Encryption mode'. The menu is open, showing two options: 'TKIP' (selected) and 'AES'.

After selecting WPA, choose your preferred **Encryption mode** – TKIP or AES.

WPA2 Encryption

WPA (Wi-Fi Protected Access) 2 is based on IEEE 802.11i standard and is meant to replace WPA. It supports CCMP and AES encryption, which makes WPA2 even more reliable than its predecessor,

After selecting WPA2, choose your preferred **Encryption mode** – TKIP or AES. The current firmware



A screenshot of a web interface dropdown menu for 'Encryption mode'. The menu is open, showing two options: 'TKIP' (selected) and 'AES'.

uses the more reliable AES as default.

Press **[Save]** to apply new settings.

8.13 4G

IP Converter supports 4G via Huawei E3372 USB modem (purchased separately).

Attention!

If «**Activate USB for 4G modem**» is enabled (see 8.1), the option to turn on Wi-Fi becomes disabled. The tariff plan for SIM card in the modem should be able provide an external (“white”) IP address, otherwise 4G will not work.

4G settings page is shown below:.

Pic. 8.13

Enable: activate/deactivate 4G connection. If the 4G modem is connected, this option is enabled by default.

APN: (Access Point Name) — Name of the network used for data transfer via packages. Issued by the SIM card provider.

Login: Login used to access the 4G network. Issued by the SIM card provider.

Password: Password used to access the 4G network. Issued by the SIM card provider.

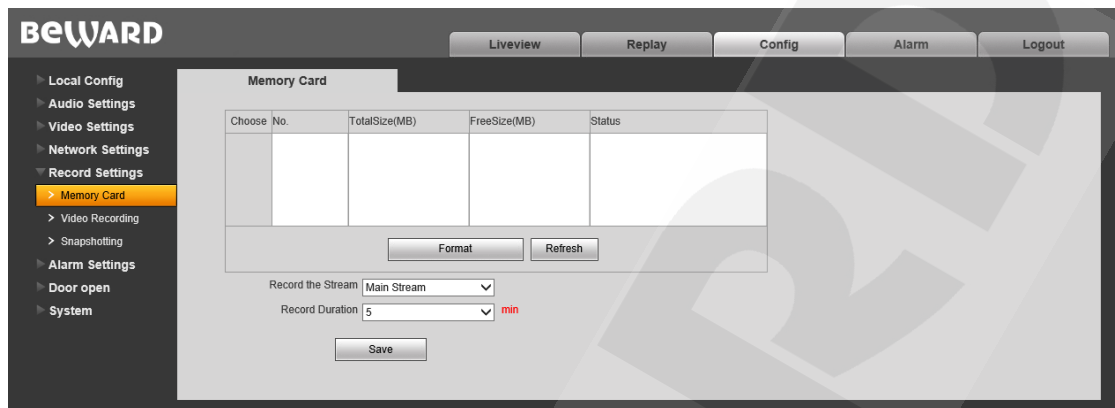
Press **[Save]** to apply new settings.

The connection process takes about 1-2 minutes. Wait a couple of minutes and refresh your browser page to see the parameters received by the modem after connecting to the mobile provider. To access the device from any location via Internet, use **IP address**.

Chapter 9. Config: Record Settings

9.1. Memory Card

The “Memory Card” settings menu is shown below:



Pic. 9.1

This page contains information on the status of the memory card (installed/ not installed), its total capacity and free space:

[Format]: start formatting the memory card.

[Refresh]: refresh information about the current parameters of the memory card.

ATTENTION!

The hot swap of a memory card is not supported by the device and may damage the device or cause data loss!

Do not turn off the device when formatting the memory card.

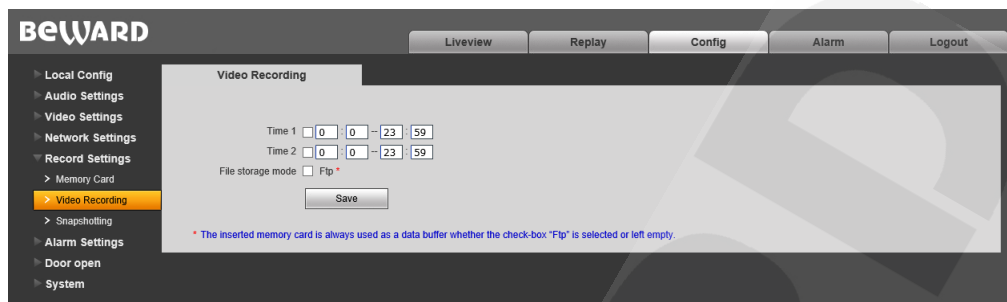
The device does not support memory cards with several partitions after formatting.

ATTENTION!

The overwrite function is enabled by default. If the memory card is full, old files are automatically deleted to make space for new files

9.2. Video Recording

The “Video Recording” settings menu is shown below:



Pic. 9.2

File storage mode FTP: Enable scheduled video recording to the FTP server. FTP server parameters can be set in the «FTP» menu (see paragraph [8.5](#)).

NOTE:

If «FTP» disabled, video files will be stored in the memory card .

ATTENTION!

The memory card installed by default also used for caching files when recording them to the FTP server.

The duration of video clips does not depend on the size of the inner buffer of the IP Converter.

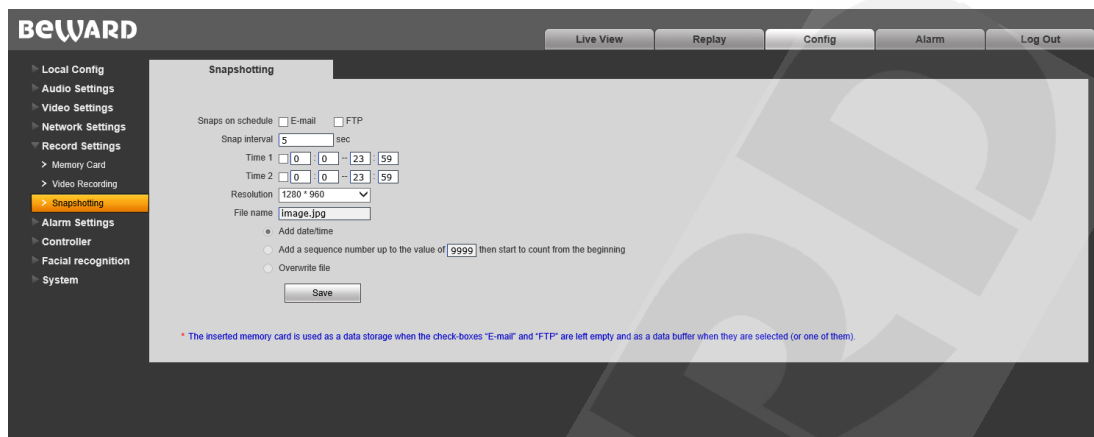
If the memory card is not installed, the inner buffer (~1MB) will be used for caching files. The duration of video clips will vary from 1 to several seconds, depending on bitrate value

Time 1/2: Set schedule for video recording. Two schedules are available.

Press [**Save**] to apply new settings.

9.3. Snapshotting

The “Snapshotting” settings menu is shown below:



Pic. 9.3

This page contains settings that allow you to set the schedule for the snapshotting function and set the snapshot folder

Snapshots on Schedule: enable scheduled snapshotting. Send snapshots to the FTP or E-mail. E-mail parameters can be set in the «E-mail» menu (see paragraph [8.5](#)), FTP-client parameters can be set in the «FTP» menu (see paragraph [8.6](#)).

NOTE:

If «FTP» and/or «E-mail» options are disabled the snapshots will be stored in the memory card,
If «FTP» and/or «E-mail» options are enabled the snapshots will be stored in the FTP server and/or sent via E-mail

Snap Interval: set the time interval between snapshots. Minimum interval – 1 second, maximum interval – 3600 seconds.

ATTENTION!

The memory card installed by default is also used for caching files when recording them to the FTP server or via E-mail. You can find the files in the memory card as well.

Time 1/2: set the schedule for snapshotting. Two schedules are available.

Resolution: select resolution for snapshots

NOTE:

«Resolution» also applies to snapshotting on alarm.

File name: choose one of the naming convention for snapshots.

Press **[Save]** to apply new settings

Chapter 10. Config: Alarm Settings

10.1. Motion Detection Settings

The “Motion Detection” settings menu is shown below:



Pic. 10.1

Here you can set motion detection parameters and conditions for sending files and notifications on motion detection triggers

[Set motion area]: set the motion detection area. Click and hold the left mouse button to frame the desired area. Up to 4 areas can be set up.

[Full screen]: set the whole image as the motion detection area.

[Clear]: clear all motion detection areas.

Sensitivity: set the motion detection trigger sensitivity. 5 levels are available: higher level leads to higher sensitivity.

Enable: enable/ disable the motion detection function.

Time 1/2: set motion detection operation by schedule. You can set 2 operating time periods.

E-mail: enable/disable e-mail notifications for motion detection triggers.

Snapshot: activate snapshotting for motion detection triggers. Specify the amount of snaps in the field to the right.

Snap interval: set the time interval between snapshots.

E-mail / FTP: set E-mail and/or FTP server as destinations for snapshots. If neither is selected, the snapshots will be sent to the memory card.

ATTENTION!

The default memory card is also used for caching files when sending them to FTP server or E-Mail, so you can find the files on the memory card

Record: enable/ disable video recording for motion detection triggers.

Record time: set the duration for video files.

FTP: set the FTP server as a destination for recorded video files. If disabled, the memory card will be used instead.

ATTENTION!

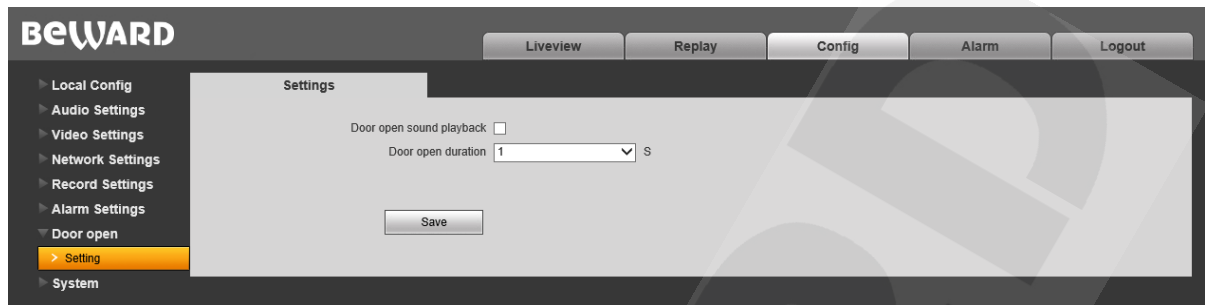
The default memory card is also used for caching files when sending them to FTP server. The duration of video files is not limited by the size of the inner buffer of the IP Converter

If there is no memory card installed, the inner buffer (~1mb) of the IP Converter will be used instead. The duration of video files will vary from 1 to several seconds, depending on the bitrate value

Press **[Save]**.to apply new settings

Chapter 11. Config: Door open

The “Door open” settings menu is shown below:



Pic. 11.1

Door open sound playback: Upon receiving “Open door” command, the door station speaker (connected to the IP Converter) plays sound signals when opening the door.

Door open duration: set the duration for the closed/open door status(depending on the type of the lock and its controller).

Press [**Save**].to apply new settings

Chapter 12. Config: System

12.1. System Info

The “System Information” menu is shown below:

The screenshot displays the BEWARD web interface for System Information configuration. The left sidebar lists various settings categories, with 'System' and 'System Info' highlighted. The main content area shows the following fields:

Field	Value
Device Name	IPC195179
Video Standard	NTSC
Language	English
Device ID	195179
Device model	DK103M
Firmware Version	3.1.0.0.4.18
Build Time	Mar 19 2018 11:01:00
WEB UI Version	2.1.3.7(20170302)

A 'Save' button is located below the fields. A red asterisk note at the bottom states: "It is necessary to close and open again the browser to apply a language changing."

Pic. 12.1

Device Name: change the device name for its easy identification.

Video Standard: choose the standard of video broadcasting (PAL/NTSC).

Language: it is possible to upload different localization files in the “FW Upgrade” menu (see paragraph [12.4](#)).

Device ID: unique ID number of the device

Device Model: Model of the device for easy identification when connection to the device remotely..

Firmware Version: the current installed version of firmware for this device.

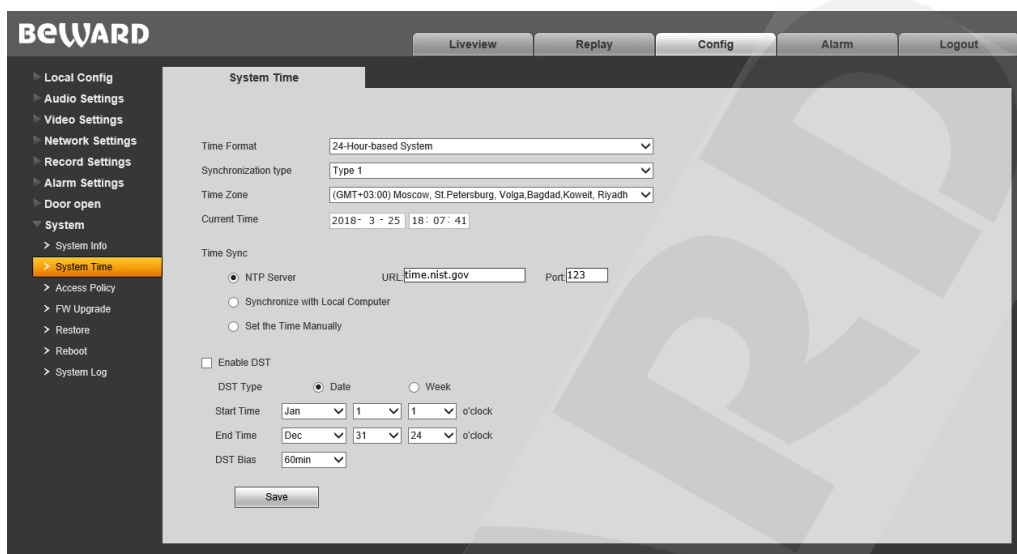
Build Date: the date when the firmware was built.

Web UI Version : the current installed version of the web interface.

Press [**Save**] to apply new settings

12.2. System Time

The “System Time” settings menu is shown below:



Pic. 12.2

Time Format: choose the time displaying format – 12- or 24-hour.

Synchronization Type: choose the type of IP Converter/door station synchronization in accordance with appropriate time standard (CST/GMT/UTC).

Time Zone: choose the time zone in accordance with location of the device.

Current Time: these fields contain current date and time entered manually or synchronized via an NTP server.

NTP Server: tick off this option to obtain time and date from a standard time server (by default – *time.nist.gov*) in Internet, using the NTP (Network Time Protocol). You can enter web address and port of an NTP server in the fields to the right.

- **Manual/Auto:** the two ways an NTP server can be selected.

Set “Manual” to enter address and port of the NTP server in the fields to the right.

Set “Auto” to let the device try to use NTP servers from the list by default till the moment of successful synchronization. The fields to the right will not be available. The list of NTP servers by default is given in the [Appendix A](#).

Synchronize with Local Computer: press this button to set date and time according to time settings of the PC which is used for work with the web interface of the device.

Set the Time Manually: choose it to set date and time manually in the “Current Time” field.

DST Type: you can choose the specific date of time advancing (“Date” type) or a day of the week (“Week” type).

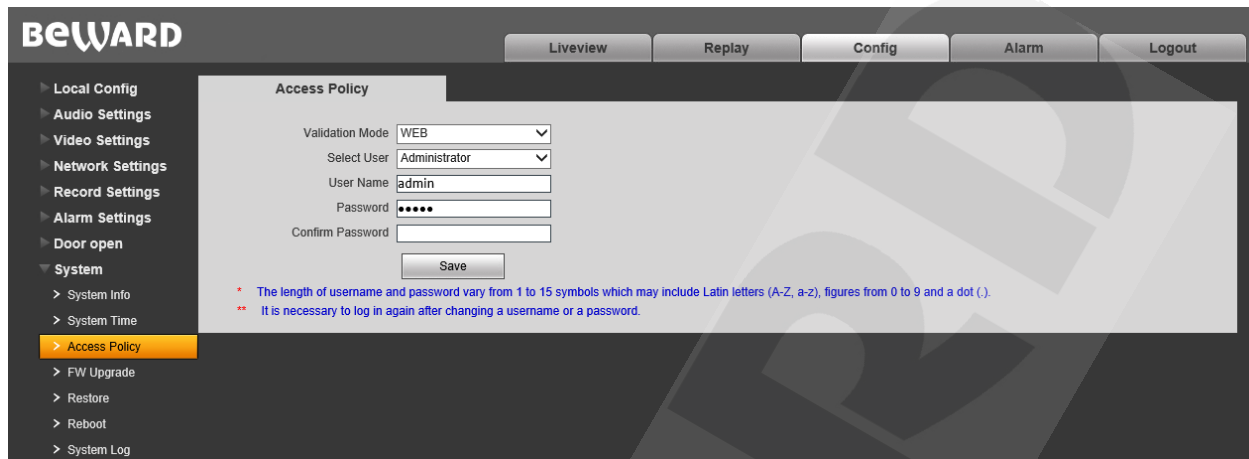
Start / End Time: set the time of advancing and backward adjusting.

DST Bias: set a size of the time shift.

Press the **[Save]** button to apply new settings.

12.3. Access Policy

The «Access Policy» settings menu is shown below:



Pic. 12.3

Validation Mode – WEB: this mode determines that username and password for IP Converter access are entered in the authorization window.

By default the device has 3 user accounts:

- **“Administrator”** has username and password as **“admin / admin”**. This is the main user account so it has no limits of access rights.
- **“User1”** has username and password as **“user1 / user1”**.
- **“User2”** has username and password as **“user2 / user2”**.

The following parts of the web interface are only available for the users authorized as **“User1”** and **“User2”**: **“Live View”**, **“Replay”** and **“Local Config”**.

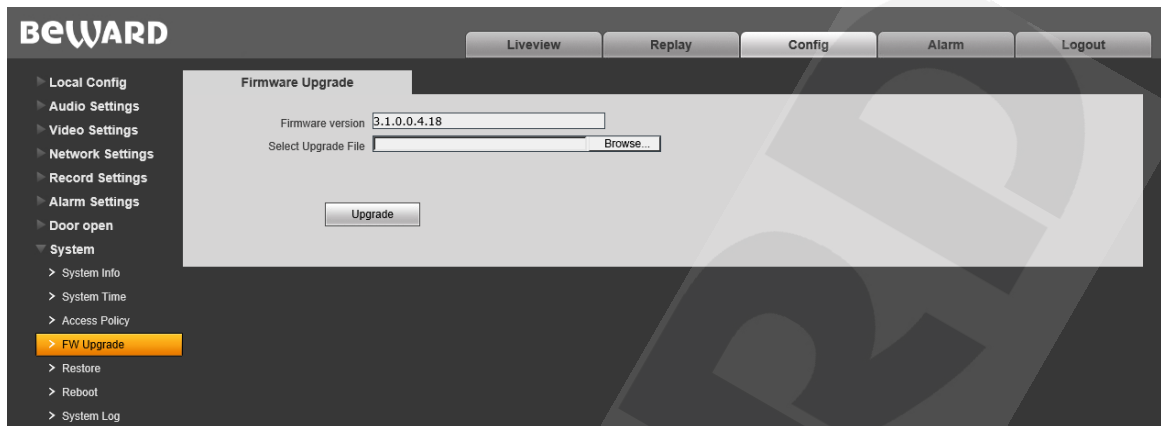
Press the **[Save]** button to apply new settings.

NOTE:

When entering the username and password, pay attention to the size of symbols. Both uppercase and lowercase letters are available. The length of username and password vary from 1 to 15 symbols which may include Latin letters (A-Z, a-z), figures from 0 to 9 and a dot (.).

12.4. FW Upgrade

The “File Uploading” menu is shown below:



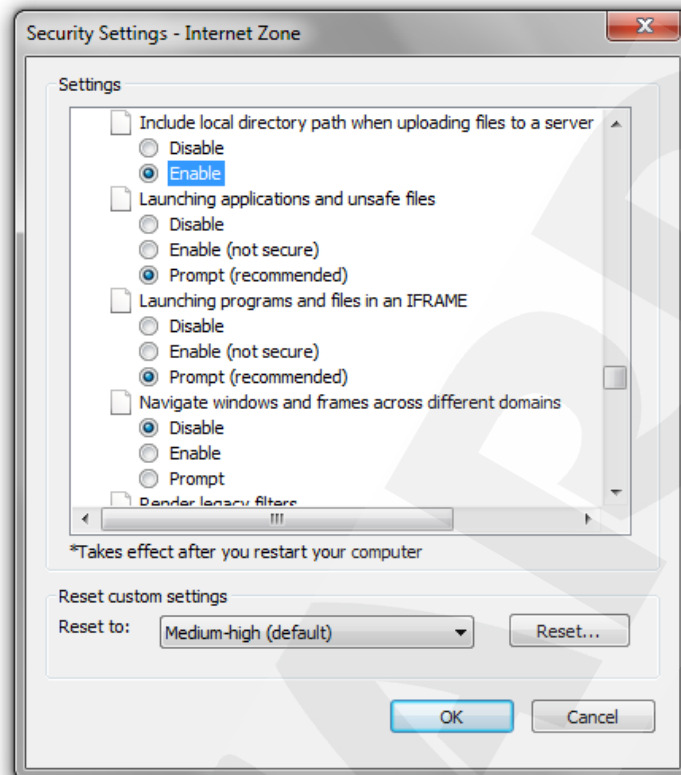
Pic. 12.4

To upgrade the device firmware or upload a localization file do the following:

1. Press the **[Browse]** button. Choose the appropriate file in the opened File Explorer window and press the **[Open]** button.
2. Press the **[Upload]** button to start upgrading. The IP Converter is automatically rebooted after upgrading procedure completing.

NOTE:

It is necessary to change Internet Explorer security settings to permit uploading files from the local folder. For this purpose, go to the menu **Tools – Internet options – Security** and press the **[Custom level]** button. Find the item “**Include local directory path when uploading files to a server**” in the opened window and select “**Enable**” (Pic. 12.5).



Pic. 12.5

3. Set IP Converter parameters by default (see paragraph [12.5](#)).

ATTENTION!

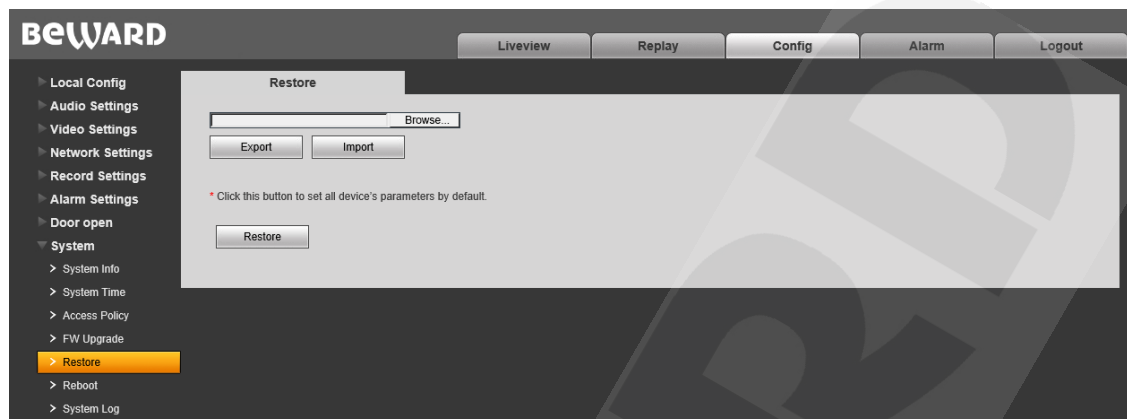
Use only appropriate firmware files which are compatible with the device model! The device may operate incorrectly and be damaged in case of using an unsuitable firmware file.

Do not disconnect the device from the network while the firmware is upgraded. The device will have the IP address 192.168.0.99 after restoring to default settings.

The device breakdown caused by incorrect firmware upgrading is not covered by the warranty

12.5. Restore

The «**Restore**» settings menu is shown below:



Pic. 12.6

Here you can set the IP Converter to factory default settings in case of some problems or after firmware upgrade. Moreover, you can save the main IP Converter settings as a file to reset them later.

[Export]: click to save IP Converter settings as a file with the “**.bak**” extension. The file name contains the date and the time of saving (according to the device clock).

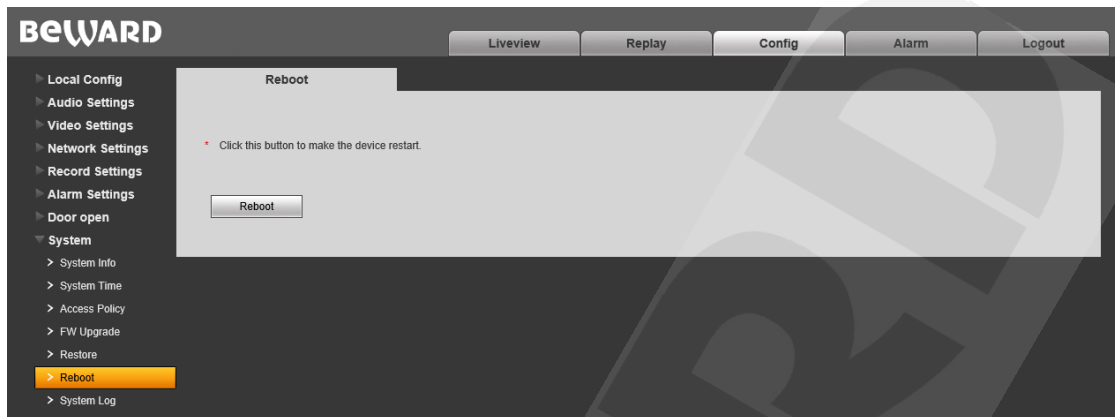
[Import]: click to reset the settings from the “**.bak**” file. Click **[Browse]**, choose the file and click **[Import]**. After restoring the settings the device will be rebooted.

[Restore]: press this button to set IP Converter parameters to default settings. Enter the administrator password and press the **[OK]** button to confirm restoring in the opened window. Press **[X]** to cancel restoring. Here you can also put a tick “**Save network settings**” to keep LAN settings of your IP Converter (**Network Settings – LAN**) without changing.

The IP Converter will be automatically rebooted after restoring the default settings. All the parameters, including an IP address and a current date, are set by default.

12.6. Reboot

The “**Reboot**” menu is shown below:.

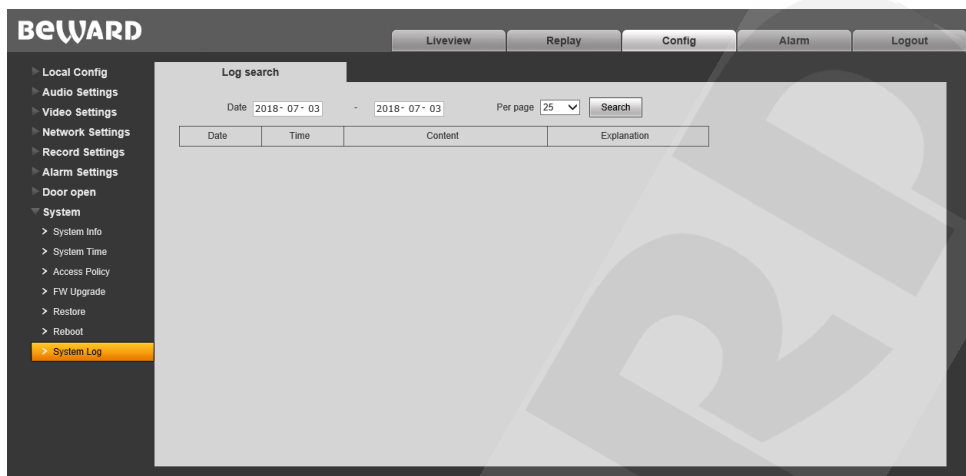


Pic. 12.7

[Reboot]: press this button to reboot the device. This procedure may last 1-2 minutes. Enter the administrator password and press the **[OK]** button to confirm rebooting in the opened window. Press **[X]** to cancel rebooting.

12.7. System Log

The “System Log” menu is shown below:



Pic. 13.8

The system log contains information about changes of the IP Converter settings and the system events that happened. The log starts recording information automatically after the device is switched on.

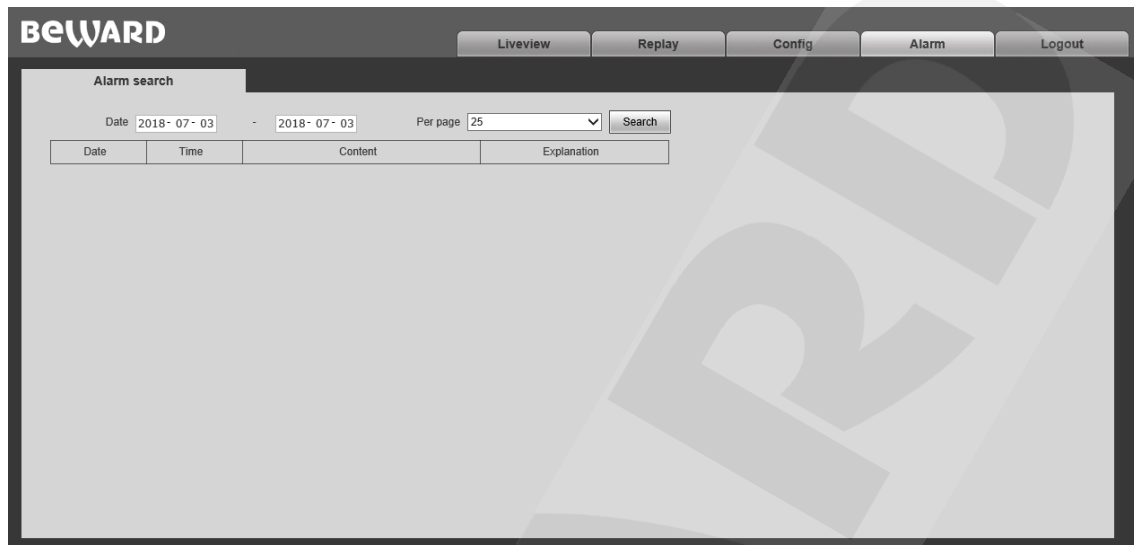
Date: specify the necessary search period.

Per page: specify the number of lines per a log page.

Press the **[Search]** button to start searching the events.

Chapter 13. Alarm

The “**Alarm Log**” menu is shown below:



Pic. 13.1

This menu has a similar look and functionality as the “**System Log**” menu (see paragraph [12.7](#)), except this menu is used for searching alarm events only .

Chapter 14. Recommendations on Setting and Operation of DKS103M

IP intercom systems include different types and configurations of equipment (PCs, laptops, microphones, speakers, etc.). Consequently, correct operation of the whole system depends on proper setting of each device used taking into account the peculiarities of their joint operation.

14.1. Acoustic Echo Cancellation

When using the IP Converter the [Client](#) or the [Guest](#) may hear an echo feedback from their PC speakers or the door station speaker accordingly.

The echo feedback on the Guest side (door station speaker) depends on settings of audio output equipment of Client's PC as well as on audio settings in the operating system on Client's PC.

The echo feedback on the Client side (PC speakers) depends on the door station settings.


The echo feedback may occur when one or more of the following conditions are taken place:

- Microphone Boost level is too high;
- The speakers are too close to the microphone;
- The speaker volume is turned up so as the microphone hears the speakers;
- The microphone sensitivity is too high.

The most efficient method to remove the echo feedback effect on the Client side is use of headphones or a hands-free unit by the Client for a conversation with the Guest. If this is impossible according to some reasons, follow the recommendations below.

There are two main ways of reducing the echo feedback effect: **change of audio settings in the operating system** and **change of audio settings of the door station**.

1. To reduce the echo feedback effect on the Guest side (door station speaker) by changing settings of the operating system do as follows:

- go to **Control Panel – Sound – Recording**, double-click the recording device set by default (microphone) and ensure that the “**Listen to this device**” option is disabled on the **Listen** tab.
- go to **Control Panel – Sound – Playback**, double-click the playback device set by default and ensure that the “**Microphone**” option is disabled on the **Levels** tab (button .

It is also possible to reduce the echo feedback effect by selecting the **Enhancements** tab on the microphone properties page and enabling one of the following options:

- Enable Noise Suppression
- Enable Acoustic Echo Cancellation

NOTE!

These settings are audio hardware and software specific and may not be available for all microphones.

•

NOTE!

The names of options in the OS menus may differ from the ones mentioned above.

2. Some features of functionality of the IP Converter can be effectively used to reduce the echo feedback effect on the Client side (PC speakers). In the Web User Interface menu go to **Config – Audio Settings – Audio Parameters** and put a tick near **“Echo Cancellation”**. (to get access to the Web User Interface please refer to paragraph [3.1](#)).

14.2. Sound Gain and Volume Adjusting

1. If the Client can't hear the Guest well or his voice is interrupted, or if the Guest hears his echo, then change your operating system settings as follows:

- go to **Control Panel – Sound – Recording**, double-click the recording device set by default (microphone) and reduce microphone boost level and volume level (if necessary) on the **Levels** tab. It is recommended to set microphone boost level to 0 dB, volume level to 100. It is also necessary to ensure that the **“Listen to this device”** option is disabled on the **Listen** tab.
- reduce volume level of the PC speakers to the minimal appropriate level. If it is too high, then the microphone may receive the audio waves from the speakers and, therefore, the Guest may hear his echo as well as the Client may hear the Guest with interrupts.
- place the PC microphone farther from the speakers and closer to Client's face.

Moreover, you can adjust the gain of sound transmitted from the door station microphone to the PC speakers in the Web User Interface. Go to **Config – Audio Settings – Audio Parameters** and change the **“Input Volume”** parameter to the appropriate value. The lower **“Input Volume”** value, the quieter Guest's voice and his echo, and vice versa.

2. If the Guest can't hear the Client well or his voice is interrupted, then change your operating system settings as follows:

- go to **Control Panel – Sound – Recording**, double-click the recording device set by default (microphone) and increase microphone boost level on the **Levels** tab. Then, set appropriate volume level. It is recommended to set microphone boost level to 0 dB, volume level to 100. Values of the parameters may vary depending on the PC microphone type.
- ensure that the **“Listen to this device”** option is disabled on the **Listen** tab.
- reduce volume level of the PC speakers to the minimal appropriate level.

Moreover, you can adjust the gain of sound transmitted from the PC microphone to the door station speaker in the Web User Interface. Go to **Config – Audio Settings – Audio Parameters** and change the **“Output Volume”** parameter to the appropriate value. The lower **“Output Volume”** value, the quieter Client's voice and his echo, and vice versa.

Appendices

Appendix A. Factory Defaults

You can see some of the factory default parameters below.

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
Data port	5000
RTSP port	554
ONVIF port	2000
NTP-server	time.nist.gov time.windows.com time-nw.nist.gov time-a.nist.gov time-b.nist.gov

Appendix B. Maintenance

It is recommended to clean the camera lens once a month by using a cotton swab (3mm) soaked in industrial alcohol



Pic. B1

If regular cleaning is not performed the image quality will deteriorate.

Appendix C. Glossary

Client is person who controls a door station using computer.

Door Station Controller is used for powering the door station, network connection, processing the signal of door opening and signals of other devices that can be connected to the door station.

Guest is a person who presses the call button on a door station installed outside.

IP Video Door Station is a device which is used for controlling the access to some territory or building and provides video surveillance functions due to a built-in IP video camera. The call from the Guest (as he presses the call button) is sent from the door station to the Client's PC or laptop with the installed application. The Client can see the Guest on the monitor of his PC and talk with him using a microphone and speakers / headphones. The Client can control the electronic door lock and some other devices connected to the door station controller.

PoE Injector is a device that stands between a regular Ethernet switch and the powered device (for example, door station PoE supported controller), injecting power and transferring the data via the same cable.

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 user name 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 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 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 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.