

# DKS151xx Multi-user IP Door Station Operation User Manual

## Contents

<b>CHAPTER 1. SAFETY INSTRUCTIONS.....</b>	<b>3</b>
<b>CHAPTER 2. GENERAL INFO .....</b>	<b>5</b>
2.1. KEY FEATURES.....	6
2.2. PACKAGE CONTENTS.....	6
<b>CHAPTER 3. GETTING STARTED.....</b>	<b>7</b>
3.1. INSTALLATION OF ACTIVE X COMPONENTS AND AUTHORIZATION .....	7
3.2. MAIN WINDOW (LIVE VIEW) .....	11
<b>CHAPTER 4. REPLAY.....</b>	<b>13</b>
<b>CHAPTER 5. CONFIG: LOCAL CONFIG .....</b>	<b>15</b>
<b>CHAPTER 6. CONFIG: AUDIO SETTINGS .....</b>	<b>16</b>
<b>CHAPTER 7. CONFIG: VIDEO SETTINGS .....</b>	<b>17</b>
7.1. ON-SCREEN TEXT.....	17
7.2. VIDEO CODING .....	18
7.3. PRIVACY MASK .....	20
7.4. VIDEO PARAMETERS .....	21
<b>CHAPTER 8. CONFIG: NETWORK SETTINGS .....</b>	<b>24</b>
8.1. BASIC.....	24
8.2. LAN.....	25
8.3. UPNP .....	26
8.4. E-MAIL .....	26
8.5. FTP .....	28
8.6. DDNS.....	29
8.7. RTSP .....	30
8.8. HTTPS .....	30
8.9. MODBUS .....	33
8.10. HTTP EVENT.....	34
<b>CHAPTER 9: CONFIG: SIP .....</b>	<b>36</b>
9.1. SIP #1 (#2) SETTINGS .....	36
9.2. COMMON.....	38
<b>CHAPTER 10. CONFIG: STORAGE SETTINGS.....</b>	<b>39</b>
10.1. DEVICE SETTINGS.....	39
10.2. RECORD SETTINGS .....	40
10.3. SNAP SETTINGS .....	41
<b>CHAPTER 11. CONFIG: ALARM SETTINGS.....</b>	<b>42</b>
11.1. MOTION DETECTION SETTINGS .....	42
<b>CHAPTER 12. CONFIG: INTERCOM .....</b>	<b>44</b>
12.1. KMN ADDRESSING .....	44
12.2. SETTING.....	45
12.3. ALARM .....	47
12.4. APARTMENTS .....	48
12.5. RFID KEYS .....	49
12.6. DISPLAY .....	50
12.7. GATE .....	51
<b>CHAPTER 13. CONFIG: SYSTEM.....</b>	<b>52</b>
13.1. SYSTEM INFO .....	52
13.2. SYSTEM TIME .....	53
13.3. USER MANAGE .....	54
13.4. UPGRADE .....	55
13.5. RESTORE .....	57
13.6. REBOOT .....	58
13.7. SYSTEM LOG .....	59
13.8. REMOTE SYSLOG .....	60

<b>CHAPTER 14. ALARM .....</b>	<b>61</b>
<b>CHAPTER 15. RECOMMENDATIONS ON SETTING AND OPERATION OF DKS151XX .....</b>	<b>62</b>
15.1. ECHO CANCELLATION.....	62
15.2. SOUND GAIN AND VOLUME ADJUSTING.....	63
<b>APPENDICES.....</b>	<b>64</b>
APPENDIX A. FACTORY DEFAULTS.....	64
APPENDIX B. SIP SETTINGS EXAMPLE .....	64
<i>B1. Direct connection .....</i>	<i>64</i>
APPENDIX D. SIP HARDWARE AND SOFTWARE (FOR TRANSMITTING VIDEO AND SOUND VIA SIP)	
COMPATIBILITY LISTS.....	67
<i>D1. PBX Compatibility .....</i>	<i>67</i>
<i>D2. Software Compatibility .....</i>	<i>67</i>
<i>D3. Hardware Compatibility.....</i>	<i>67</i>
APPENDIX C. GLOSSARY .....	68

## **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 door

#### **ATTENTION!**

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

### **Follow this Operation User Manual.**

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

- Avoid extremely low and high temperatures (The operating temperature of this door station is -40°~+50°).
- Avoid prolonged exposure to direct sunlight, do not install near water and heat sources.
- 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 door station.
- Water or foreign matter getting inside the door station.
- The door station getting damaged:

### **Do the following:**

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

**Transportation**

Transport the door station 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 door station!

**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 door station housing.

## Chapter 2. General Info

DKS151xx Multi-user IP Door Stations are designed for organizing access control to communal entrance hallways. The IP Door Station is utilizing a 1.3 MP camera to ensure high quality video footage. Audio (Duplex) and Video are transmitted via SIP protocol. Access can be granted by using wireless marks via RFID Reader (125 KHz/ 13,56 MHz). Up to 9999 subscribers are supported, which makes the device a perfect solution for hotels or high-rise apartment houses.



Pic. 2.1

DKS151xx is an IP device with built-in microphone, speaker, video camera, IR illumination, keypad, display and RFID reader. The housing is vandal-resistant and may be mounted next to the entrance. The device is used for establishing Audio and video connection between the Guest and the Client (Subscriber); conducting video surveillance of the entrance; granting access via RFID keys and secret codes; managing of other devices, connected to the door station (e.g. electric locks, swing gates, electric switches, alarm systems etc.). IR illumination (max range – 10 meters) and the IR-filter allow for video surveillance during nighttime.

Since the device supports modern network technologies, it can be using as a part of a more complex IP-based surveillance system.

The door station is connected to the network via 10BASE-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.

If for some reason the door station breaks down, the current settings will not be lost, as they are stored in the pre-installed USB drive. Just dismount the drive and insert into a different door station and it will be the exact copy of your previous device, except for the MAC address (make sure that both devices have the same IP firmware version).

## 2.1. Key Features

- Vandal resistant housing
- Separate button for emergencies
- Supports RFID 125 kHz and 13,56 MHz
- 1.3 MP video transmission
- Audio Duplex
- Supports SIPv2 protocol
- IR Illumination (max range – 10 m.)
- Operating temperatures: -50 ~ +60°C
- Supports up to 9999 subscribers
- 8500 RFID keys
- Gain access by entering individual secret code number
- Register RFID keys by entering individual secret code number
- Up to 5 call directions per a single subscriber
- (Optional) Call via crossboard analog networks (up to 600 subscribers)
- Backup storage for 8500 RFID keys and 1500 secret codes. Used in case of updating the firmware or resetting the IP door station.
- Removable memory card with saved device settings (USB, pre-installed)
- Ready to perform basic functions (open door, call analog door phones) immediately after booting up.
- Cold-resistant LED display (8 symbols)
- Limit Switcher
- Supports 1 additional door with a 1-Wire reader.
- Remote access to entrance hall lights.

## 2.2. Package contents

- IP Door Station with pre-installed memory card and USB drive
- Terminal blocks
- Silicone cap for LAN cable and memory card box
- Package

### **ATTENTION!**

Package contents and device specification are subject to change without notice

## Chapter 3. Getting Started

### 3.1. Installation of ActiveX components and Authorization

**Step 1:** Connect the door station 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 door station, ***<PORT>*** is number of the port used for HTTP connection to the device.

**NOTE:**

Default HTTP-port is – **80**. You don't need to enter the port number if you connect via the default HTTP port.

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

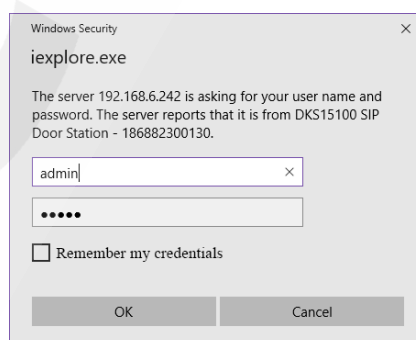
**NOTE:**

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:** Enter login and password and click OK. Default username – **admin**, default password – **admin** (*Pic. 3.1*).

**Attention!**

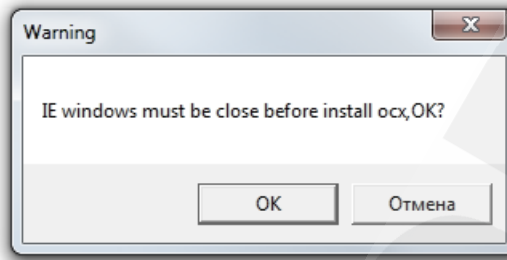
After authorization you can change login and password in **Config – System – Access Policy**. If you lose your login and password, you can reset the door station to default settings. To do so you need to press and hold the reset button 3 times for 10 seconds with 1 second pauses between each press



*Pic. 3.1*

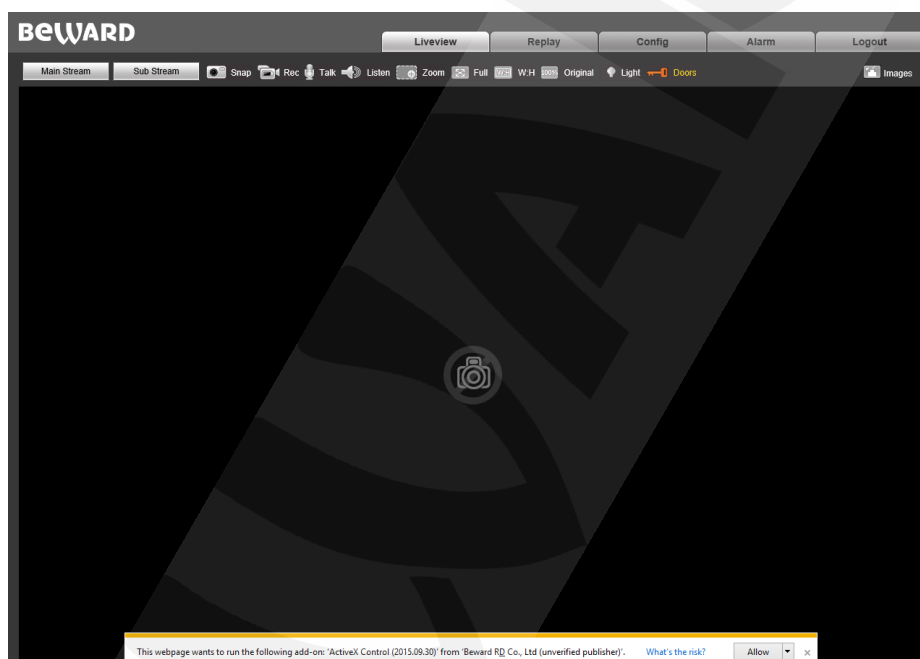
If successful, you will start receiving the videostream from the door station camera (*Pic. 3.3*).

**Step 4:** To work with the web interface you need to install the ActiveX add-on. If the necessary components are not yet installed, you will see the following message.



Pic. 3.2

Click **[OK]**. In the lower part of IE browser you will the following notification (Pic. 3.8).



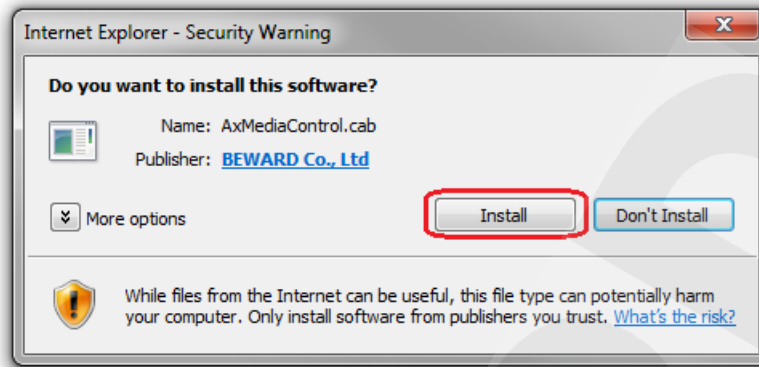
Pic. 3.3

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

#### ATTENTION!

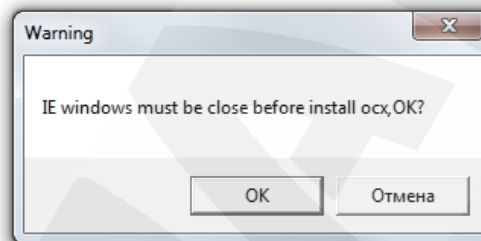
Installation of ActiveX components is only possible for 32-bit Internet Explorer..

**Step 5:** By default, the Internet Explorer security system will block the ActiveX installation. Click **[Install]** to continue (Pic. 3.4).



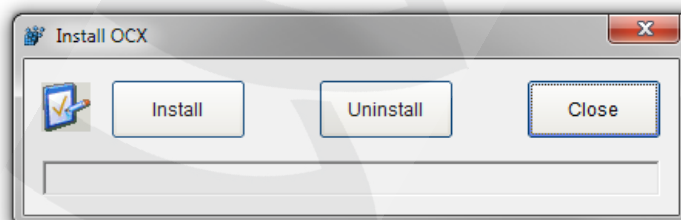
Pic. 3.4

**Step 6:** Close Internet Explorer and click **[OK]** in the Warning window (see Pic 3.4) if it pops up.



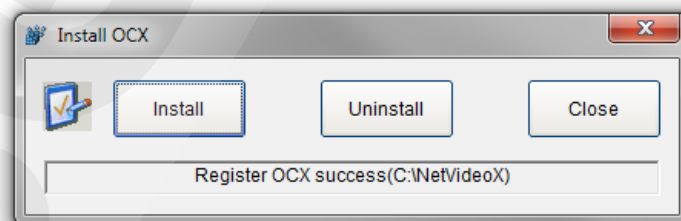
Pic. 3.5

**Step 7:** Click **[Install]**.



Pic. 3.6

**Step 8** After completing the installation you will see the following «Register OCX success(C:\)» Click **[Close]** (Pic. 3.7).



Pic. 3.7

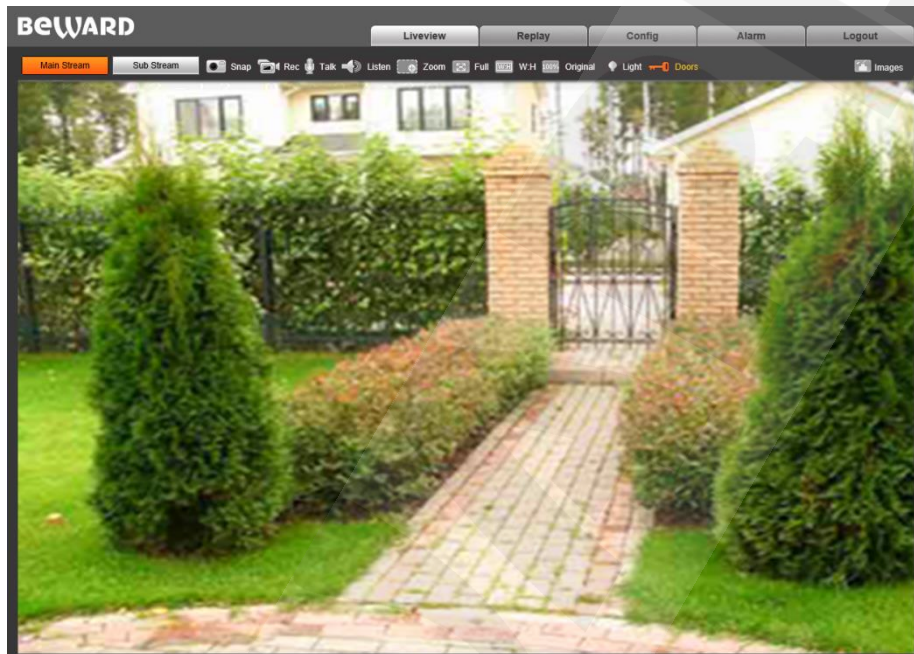
**NOTE:**

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

**NOTE:**

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

**Step 9:** Run Internet Explorer and enter the IP address of the door station in the path field..

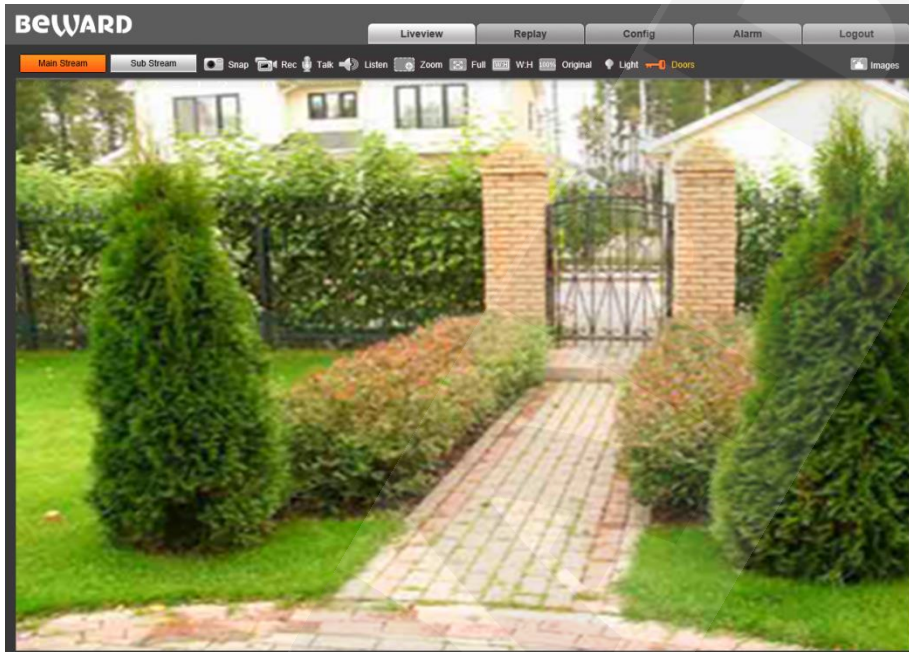


Pic. 3.8

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

### 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, Illumination, 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.

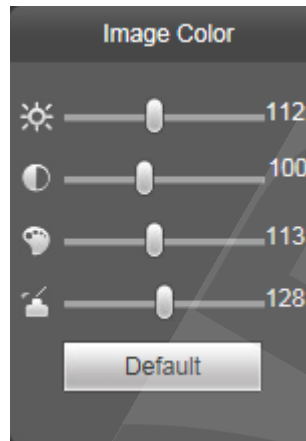
**W:H:** Press this button to apply the correct width to height ratio to the livestream display.

**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.

**Illumination:** press this button to turn on IR illumination.

**Door:** Press this button to open the main door.

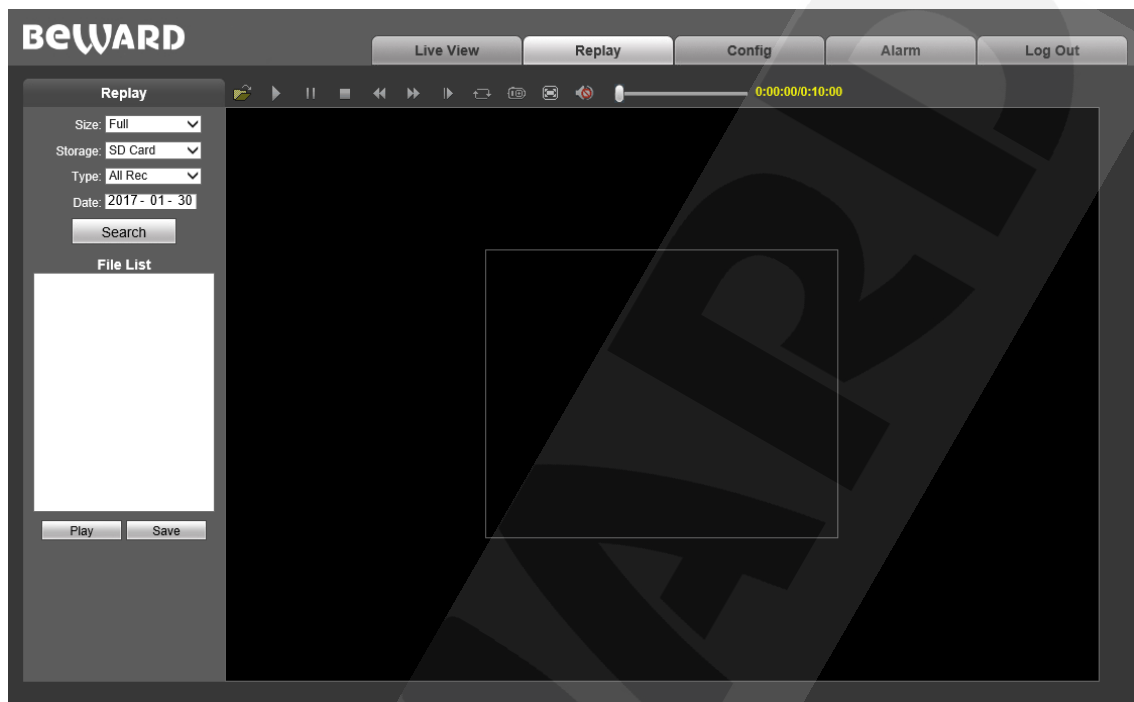
**Image:** Use this toolbar to adjust the following parameters: «Brightness», «Contrast», «Hue», «Saturation». If you want to restore to the default parameters, click **[Default]** (Pic. 3.12).



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»**.

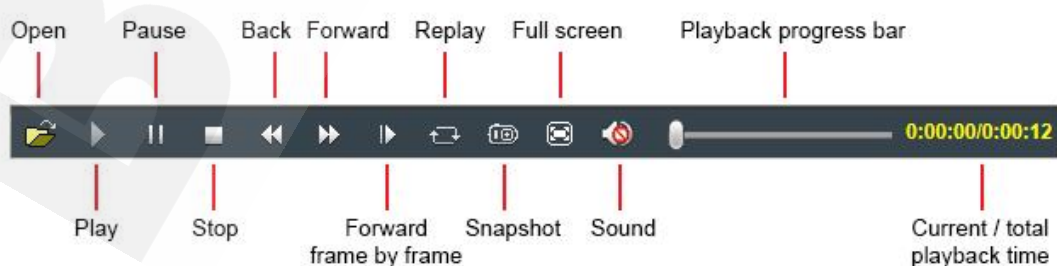
**Date:** choose the date for searching files.

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

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

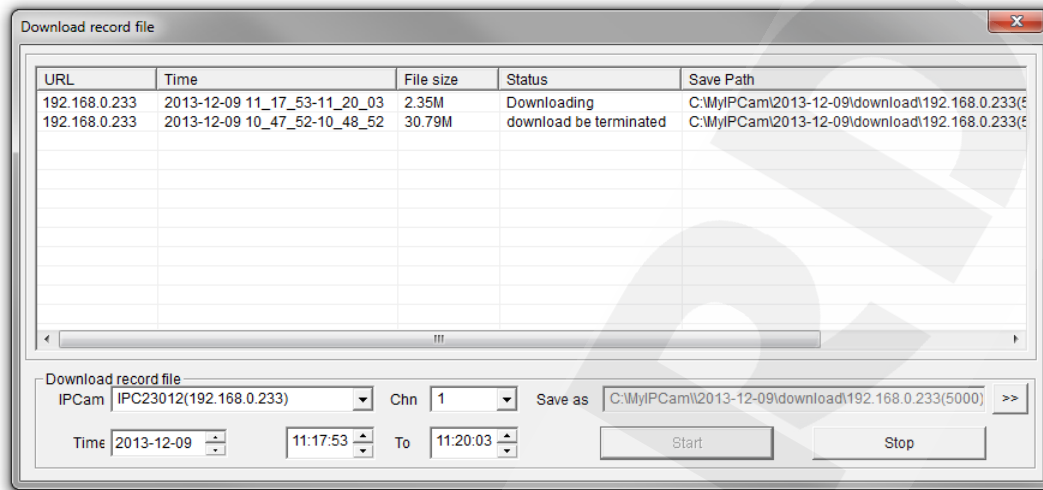
**[Play]:** Select a file in the File List and press this button to play it.

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 ID and its IP address.

**Chn:** Channel #, choose "1" for the door station

**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.

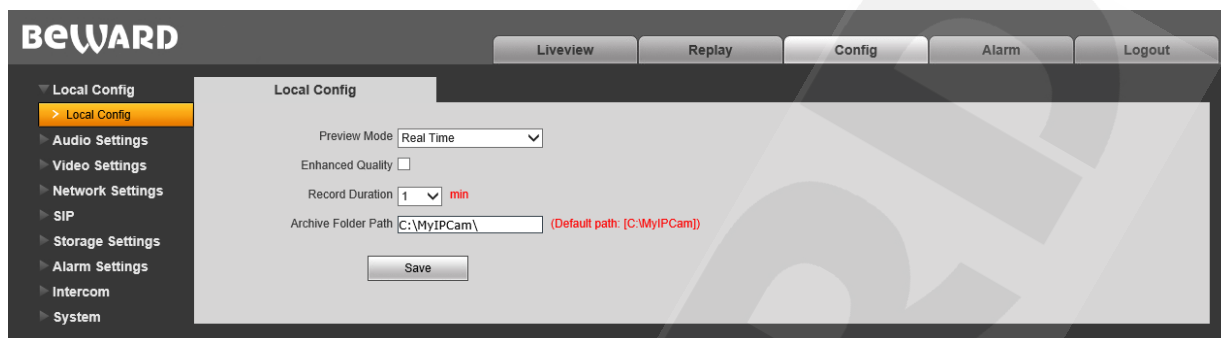
**Note!**

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 **Local Config** page of the device is seen below:



Pic. 5.1

**View 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 and G.726.

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

**IP input Volume:** Set the volume of the input signal. Available values – 0 ~ 15, default value – 8 . This option affects the speaker volume (Client side) when speaking with a guest via IP.

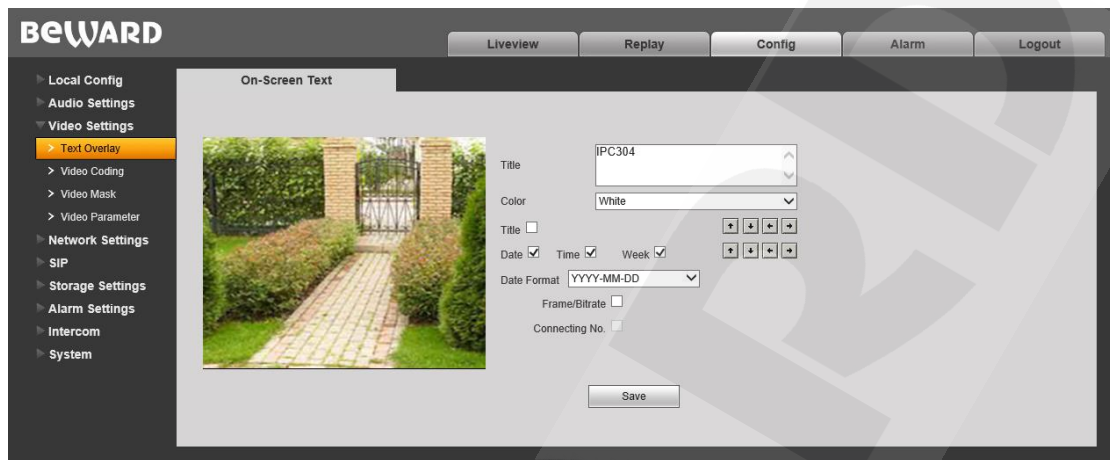
**IP output volume:** set the volume of the output signal. Available values – 0 ~ 15, default value – 8 . This option affects the speaker volume of the door station when speaking to the client via IP.

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. door station name) that will be displayed at the bottom left corner of the screen.

**Font 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 that will be shown.

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

**Connections Number:** show/hide the number of current connections to the door station web interface (displayed in parenthesis after the title).

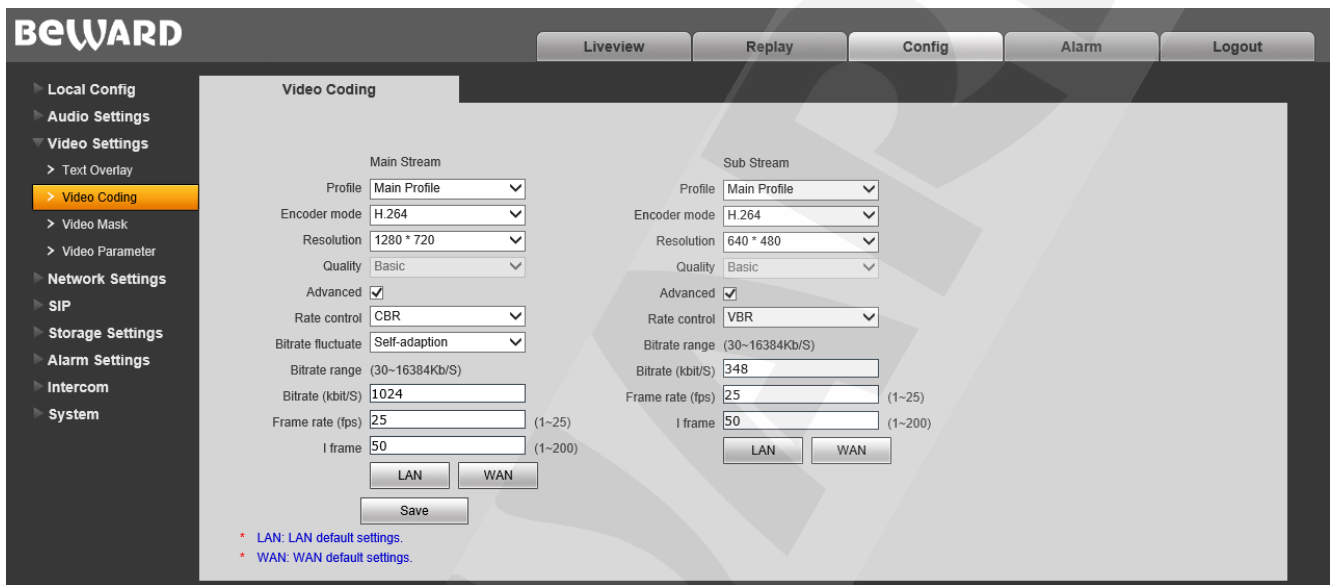
You can also change positions of the text elements. To do so use . (top row for title, bottom row for everything else).

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.



*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]:**

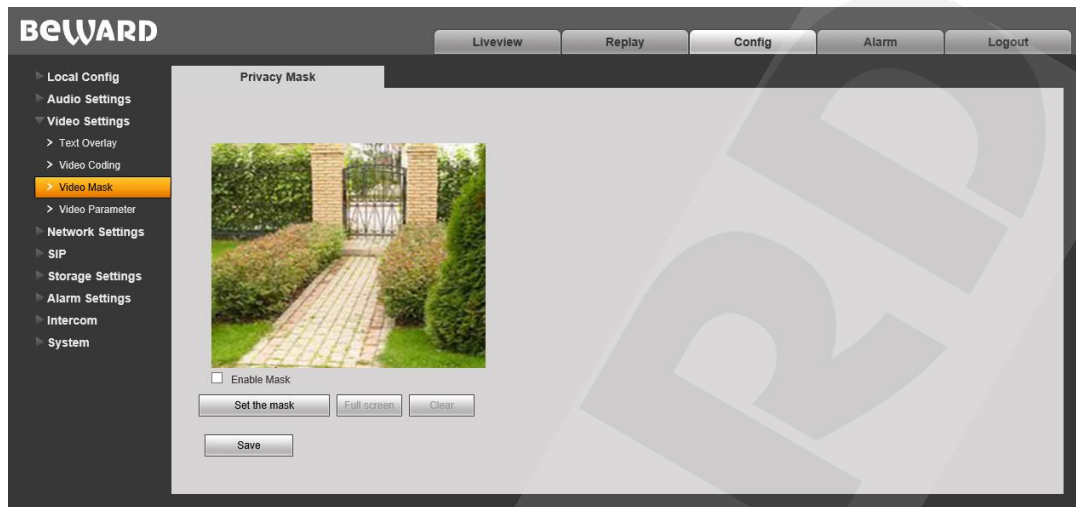
- Main stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 4096 kbit/s
- Sub stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 512 kbit/s

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

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

### 7.3. Privacy Mask

The **Privacy Mask** menu is shown in *Pic. 7.3*.



*Pic. 7.3*

**Enable Mask:** Enable\Disable privacy mask.

**[Set the mask]:** Click this button and then press and hold the left mouse button selecting the necessary area. Up to 4 mask areas can be set up.

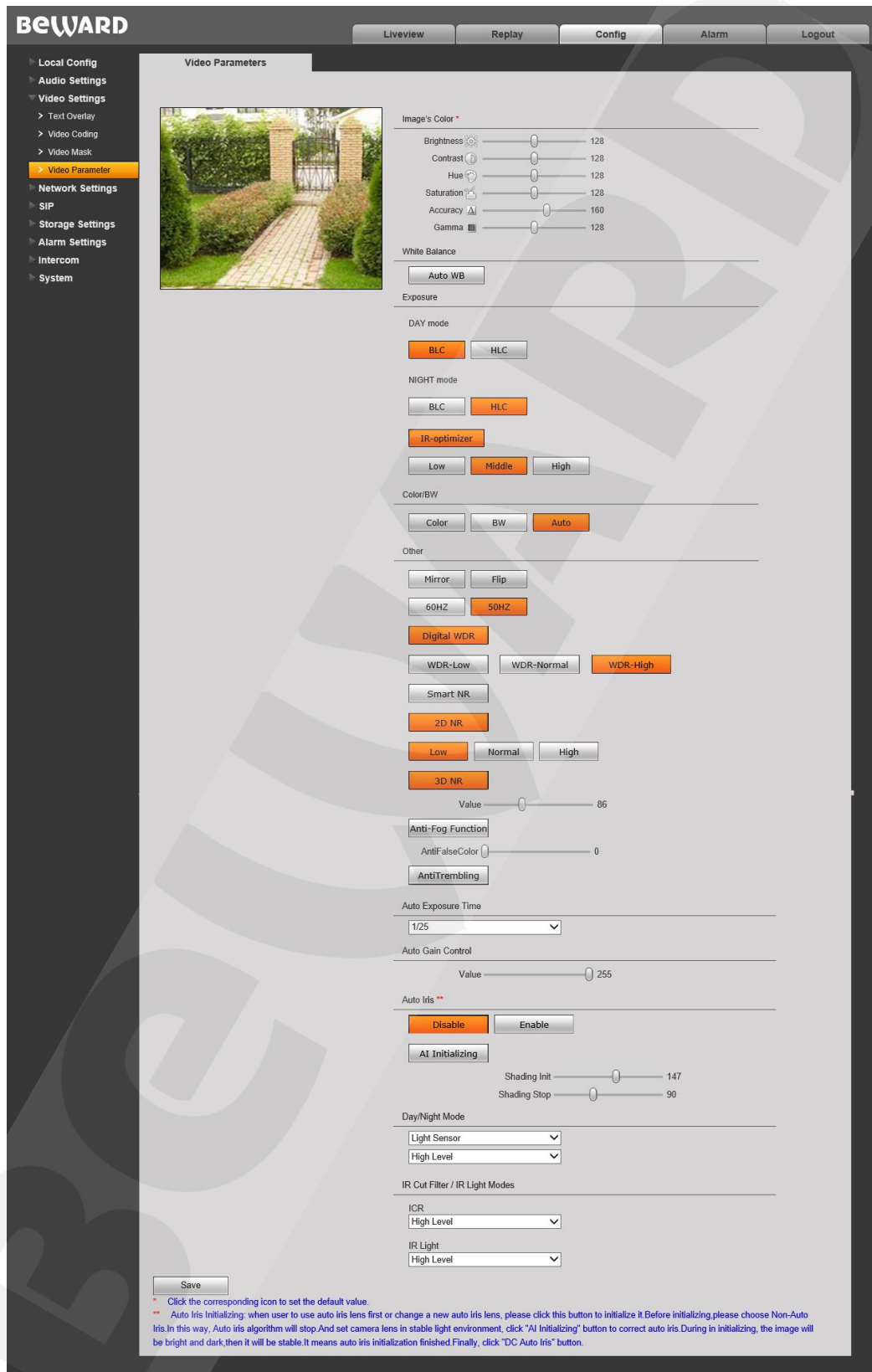
**[Full screen]:** Click to mask the whole screen.

**[Clear]:** Remove all mask area.

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

## 7.4. Video Parameters

The “Video Parameters” menu is shown on *Pic. 7.4*.



*Pic. 7.4*

**Image Parameters:** Set such parameters as brightness, contrast, hue, saturation, accuracy and gamma (available value range: 0~255). Moving the sliders will change the image immediately. To reset parameters to default, click their corresponding icons)

**White Balance:** Set automatically by default, but manual adjustment via the red, green and blue sliders is also available.

**Exposure:** This option allows brightening dark areas in **DAY and NIGHT modes**. Supports **BLC** (Backlight Compensation) and **HLC** (Highlight Compensation).

**IR Optimizer:** Use IR illumination to brighten the center area of the image, which allows for better face recognition in nighttime. Intensity levels: «Low», «Medium», «High».

**Color/BW:** Set a color mode or a black and white mode for the door station camera. The modes switch automatically by default.

**Other:** contains the following parameters:

**Mirror:** Reflect the image.

**Flip:** Flip the image.

**60HZ:** Use this mode if the light source equipment in the surveillance area connect to the 60Hz electrical grid. The exposure time is automatically set to the value divisible by 30

**50HZ:** Use this mode if the light source equipment in the surveillance area connect to the 60Hz electrical grid. The exposure time is automatically set to the value divisible by 25.

**Indoors/Outdoors:** Enable these option to partially/ completely get rid of a blinking effect in light sources via pulse-width modulation.

**DWDR:** Enable Digital Wide Dynamic Range mode. The available options are «Low»/«Normal»/«High».

**Smart NR:** This option increases 3DNR efficiency in low light conditions and reduces the blurry effect of moving objects.

**2DNR:** Reduce noise in low light conditions. The available image processing options: «Low»/«Normal»/«High».

**3DNR:** Reduce noise in low light conditions. This option does not affect the image detail, but there may be traces of moving objects depending on value you set with the slider.

**NOTE:**

3DNR only works in «Night» mode.

**Anti-Fog:** Show better details in case of fog.

**Color Correction:** Enabling this function allows for better rendition of colors by correction of hues.

**Anti-Tremble:** Reduce tremble if the device is exposed to vibrations.

**Maximum Exposure Time:** Set maximum exposure time value. Available values: «1/25»~«1/8000».

**Auto Gain Control:** Automatically increase brightness in low light conditions. Bigger AGC values result in higher noise levels

**Day/Night Mode:** Activate «Day» and «Night» presets:

- **Schedule:** «Day» and «Night» modes will switch as scheduled. When selected, you will be able to set the schedule time in additional fields.
- **Light Sensor:** «Day» and «Night» modes will switch via the built-in light sensor. Set the operation mode in the drop-down list below. “Day – Night”- Day mode in high external light levels, Night mode in low external light levels. “Night – Day” - Night mode in high external light levels, Day mode in low external light levels

**IR Cut Filter/IR Light Modes:** Set the operation modes for IR filter and IR LED

- **ICR:** Blocks infrared wavelengths for better rendition of colors.
  - «On at night»: Blocks IR spectrum during the Day Mode, transmits IR spectrum during the Night Mode
  - «On in a daytime»: Transmits IR spectrum during the Day Mode, blocks IR spectrum during the Night Mode
- **IR Light:** Use IR LED in low external light level conditions.
  - «On in a daytime»: Day mode: LED is disabled, Night Mode: LED is enabled
  - «On at night»: Day mode: LED is enabled, Night Mode: LED is disabled
  - «Disabled»: LED is always disabled.
- **IR optimizer:** Allows for facial recognition at nighttime by making sure that there is no excessive IR LED light at the center of the image.

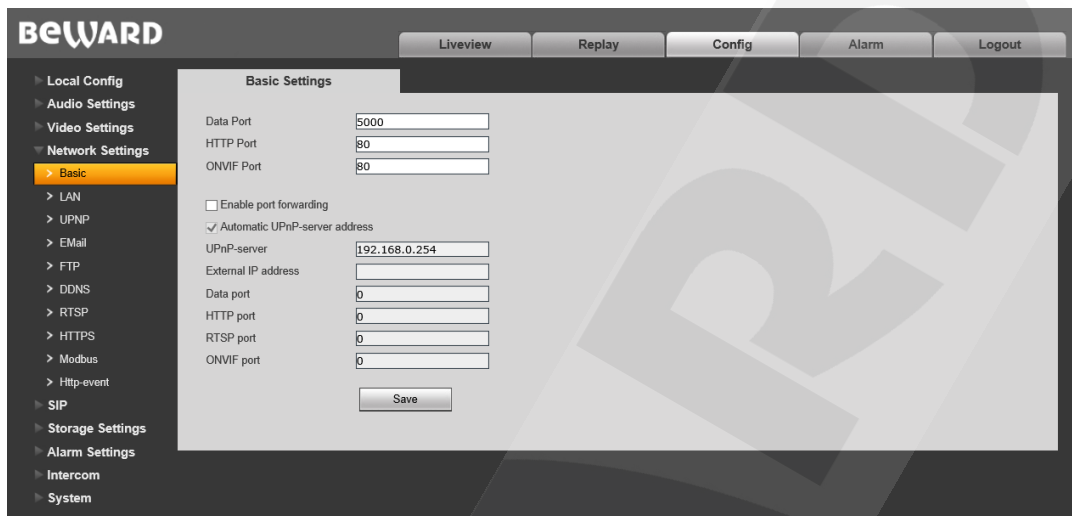
Changing the aperture setting will not affect the image, since the device does not have an aperture module. This option is displayed only because the firmware is universal for different kinds of devices.

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

## Chapter 8. Config. Network Settings

### 8.1. Basic

The “Basic Settings” menu is shown below.



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 and 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).

**Enable port mapping** – The door station connects to the router and automatically forwards its ports behind NAT. If successful, the external ports and the IP address will be shown in fields below.

#### ATTENTION!

Your router must support map mapping in order for this function to work.

**Upnp server** – IP address of the server that will automatically forward ports behind NAT Address

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 door station 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 door station (This field is not recommended to change).

### NOTE:

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

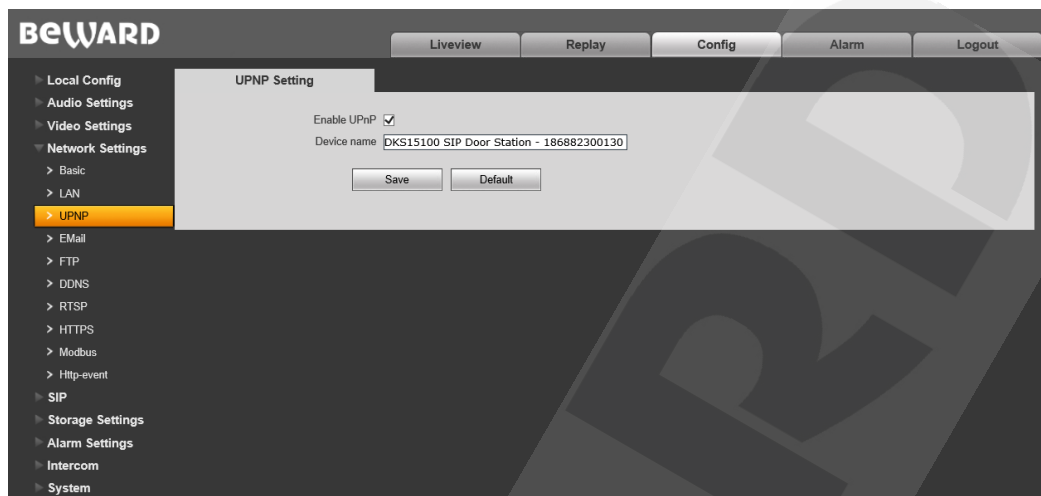
### ATTENTION!

After changing the network settings the IP door station will automatically reboot .

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

### 8.3 UPnP

The “UPnP” settings menu is shown below



Pic. 8.3

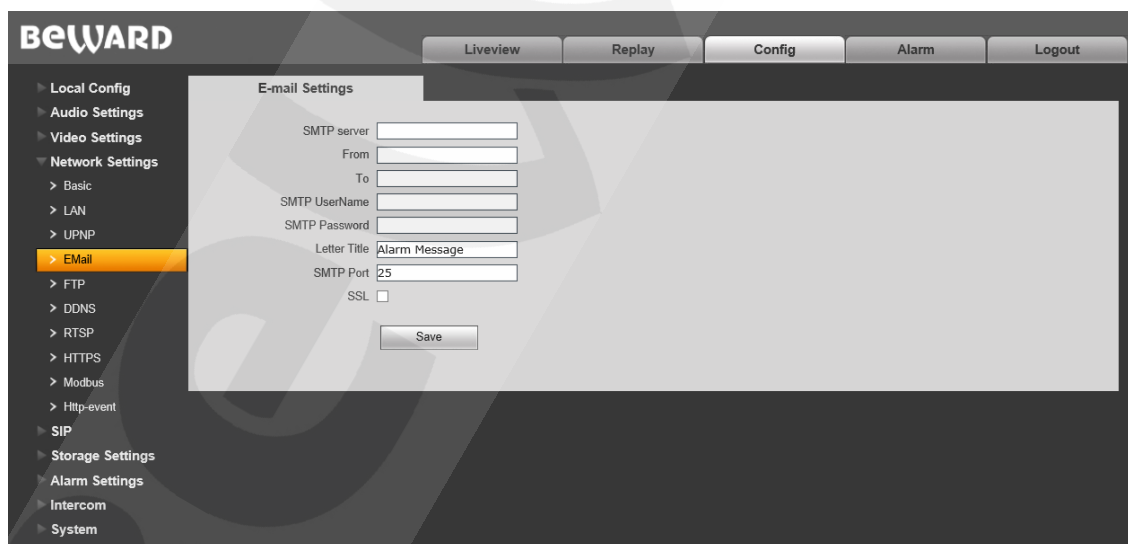
**Enable UPnP:** enable/disable network detection via UPnP

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

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

### 8.4. E-mail

The “E-mail” settings menu is shown below



Pic. 8.4

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.

## 8.5. FTP

The **FTP** settings menu is shown below:

The screenshot displays the BEWARD web interface for configuring FTP settings. The sidebar on the left lists various configuration categories, with 'FTP' under 'Network Settings' highlighted. The main content area, titled 'FTP Setting', is divided into two sections: 'Main Server' and 'Sub Server'. Each section contains input fields for 'Server URL', 'Server Port' (with a default value of 0), 'FTP Catalog', 'UserName', 'Password', 'Start Port' (with a default value of 21), and 'End Port' (with a default value of 21). A 'Save' button is located at the bottom of the form.

Pic. 8.5

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. Default value: 21.

**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.

## 8.6. DDNS

The **DDNS** settings menu is shown below:

The screenshot displays the BEWARD web interface for DDNS configuration. The top navigation bar includes 'Liveview', 'Replay', 'Config', 'Alarm', and 'Logout'. The left sidebar lists various configuration categories, with 'Network Settings' expanded and 'DDNS' selected. The main configuration area for DDNS includes an 'Enable' checkbox, a 'Service Provider' dropdown menu, and input fields for 'UserName', 'Password', 'Domain', 'Server URL', 'Server Port', 'Data port', 'HTTP port', and 'Update Interval'. A 'Save' button is located at the bottom of the form. A domain example 'test1.noip.com' is shown below the fields.

Pic. 8.6

This menu contains parameters for setting the connection via DDNS service. DDNS allows you access the door station 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 door station 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.

**External IP:** external IP address of the door station defined by your Internet provider.

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

## 8.7. RTSP

If RTSP is enabled you will be able to watch the video stream from the 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 door station has a single channel, enter “0”
- **<Y>** – command of the video stream profile: 0 – main stream, 1 – sub stream.

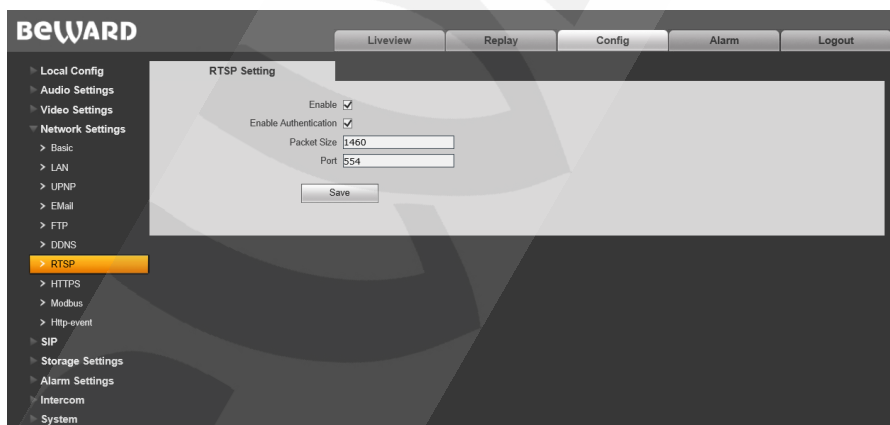
Request example: **rtsp://192.168.0.99:554/av0\_0.**

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 8.7

**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>**.

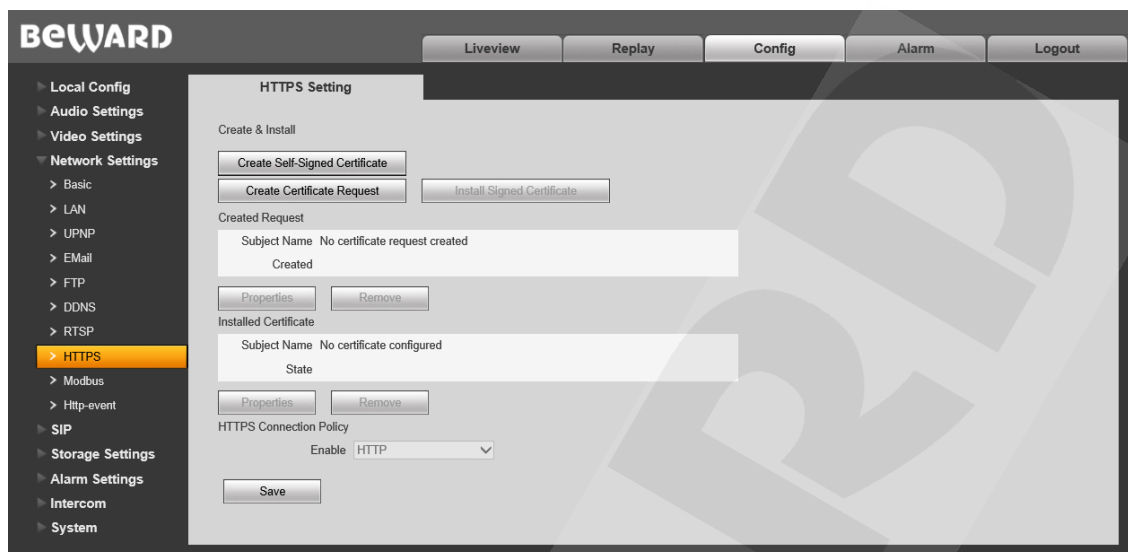
**Packet Size:** set the size of the data packet. Default value: 1460.

**Port:** RTSP port. Default vale: 554.

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

## 8.8. HTTPS

The **HTTPS** settings menu is shown below:



Pic. 8.8

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.

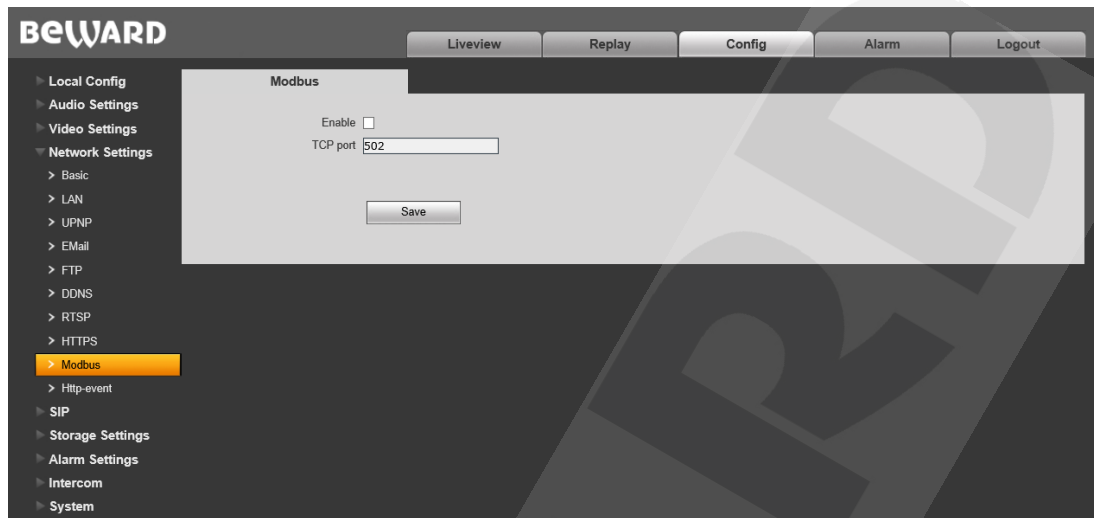
**HTTPS Connection Policy:** select protocol in use. Available protocols: HTTP, HTTPS, HTTP & HTTPS.

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.

## 8.9. Modbus

The **Modbus** settings menu is shown below:



Pic. 8.9

Use the Modbus protocol to connect to compatible equipment.

**Enable:** enable\disable Modbus.

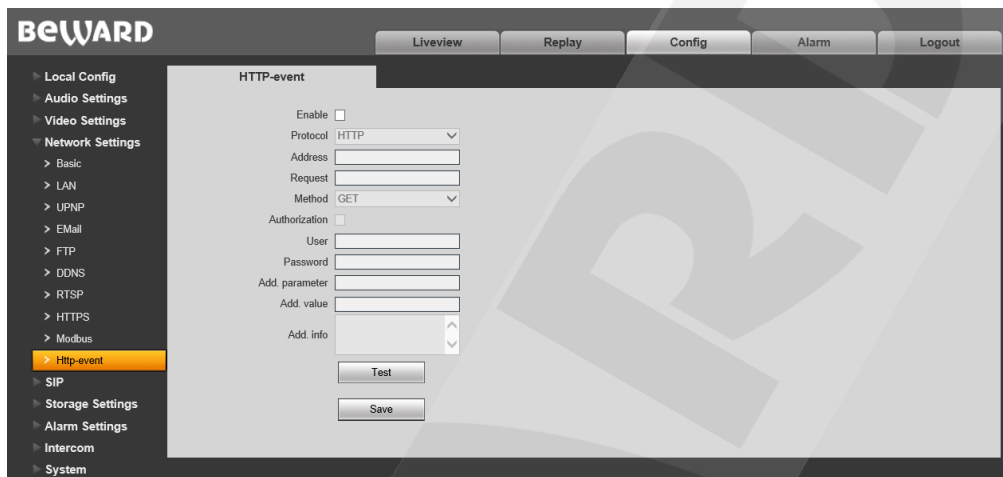
**TCP port:** number of the port for the Modbus protocol. Default number – 502.

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

### 8.10. HTTP Event

This function sends commands from the door station to other network devices when motion detection is activated or when the call button is pressed.

The **HTTP event** settings menu is shown below:



Pic. 8.10

**Enable:** turn on HTTP event function.

**Protocol:** select the preferred protocol to send notifications (commands). Available protocols: HTTP, HTTPS.

**Hostname:** address and command for your HTTP event server. «&» and «=» are unsupported.

For example, For URL «http://www.eventserver.org» enter «www.eventserver.org» in the “Hostname” field.

You can also enter a port number, which will differ from the default one (e.g. enter «www.eventserver.org:81». if the port number is 81).

Default port numbers («80» for HTTP and «443» for HTTPS) are set automatically when you select the protocol.

**Request:** enter a request for your HTTP event server. For example, enter “/alarm” for the URL «http://www.eventserver.org/alarm» .

**Method:** method of sending notifications: GET or POST.

**Authorization:** enable authorization for sending notifications

**Username:** enter username for authentication. Maximum length is 20 symbols, including upper case letters and the following symbols: «!», «@», «#», «\$», «\*», «\_», «-», «,», «.».

**Password:** enter password for authentication. Maximum length is 20 symbols, including upper case letters and the following symbols: «~», «!», «@», «#», «\$», «%», «^», «\*», «(», «)», «\_», «+», «{», «}», «:», «"», «|», «<», «>», «?», «-», «;», «'», «\», «,», «.», «/».

**Additional parameter:** name of the additionally sent parameter. It is commonly required for the server when using a POST request

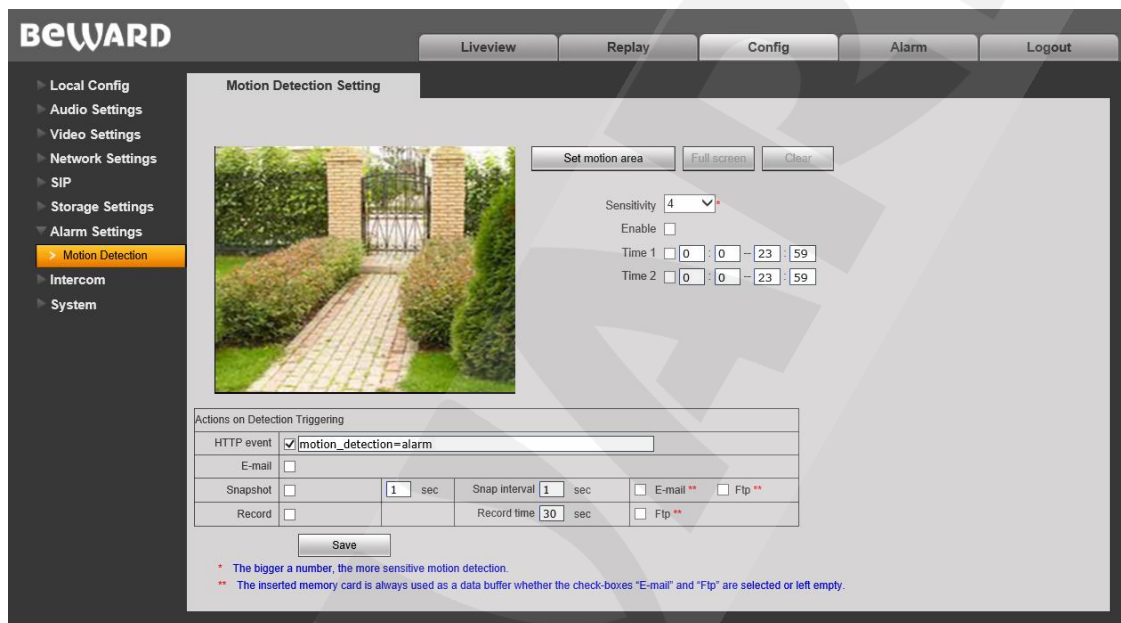
**Additional value:** enter value of the additional parameter if necessary

**Additional body:** additional information added to the body of the notification. It can be used for adding program code to send messages in online chats, blogs etc.

**[Test]:** Click to check if the data you entered is correct. The HTTP request will be sent to the specified address.

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

### HTTP event example (Motion detection) (see [11.1](#)):



Pic. 8.11

Check the “HTTP event” box and enter the required parameter. Maximum length requests is 127 symbols. «&» and «=» symbols are supported.

This parameter will be sent to the HTTP event server you entered in the settings menu (see pic. 8.15) in accordance with GET/POST methods.

Notifications will not be sent if the HTTP event server is not set or disabled

**A HTTP request with additional parameters** is made as follows:

http://<“Hostname”>?< “Additional parameter” >=< “Additional value” >&<“HTTP event”>HTTP/1.0

**A HTTP request without additional parameters** is made as follows:

http://<“Hostname”>?“HTTP event”>HTTP/1.0

## Chapter 9: Config: SIP

### 9.1. SIP #1 (#2) Settings

The SIP settings menu is shown below.

The screenshot shows the BEWARD web interface with the 'SIP #1 configuration' page. The sidebar on the left lists various configuration categories, with 'SIP' and 'SIP #1' highlighted. The main configuration area includes the following fields and options:

- ☒ Enable SIP #1
- Name:
- Number:
- Username:
- Password:
- SIP port:
- ☐ Enable registration
- ☐ Get registrar by DHCP
- Registration server:  Port:
- Registration status:
- ☐ Get proxy by DHCP
- Proxy:  Port:
- SIP server:  Port:
- ☐ NAT
- STUN IP:
- STUN port:
- STUN nort:
- 

Pic. 9.1

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.

**Registration status:** Account status in the SIP server.

**Name:** Name of the door station. Displayed during calls. This field is empty by default.

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

**Username/Password:** used to register the door station 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 door station to be registered in the SIP server. Disabled by default.

**(SIP #1 only) Get the address of a registration server via 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.

**(SIP #1 only) Get the address of a proxy server via 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 door station 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!**

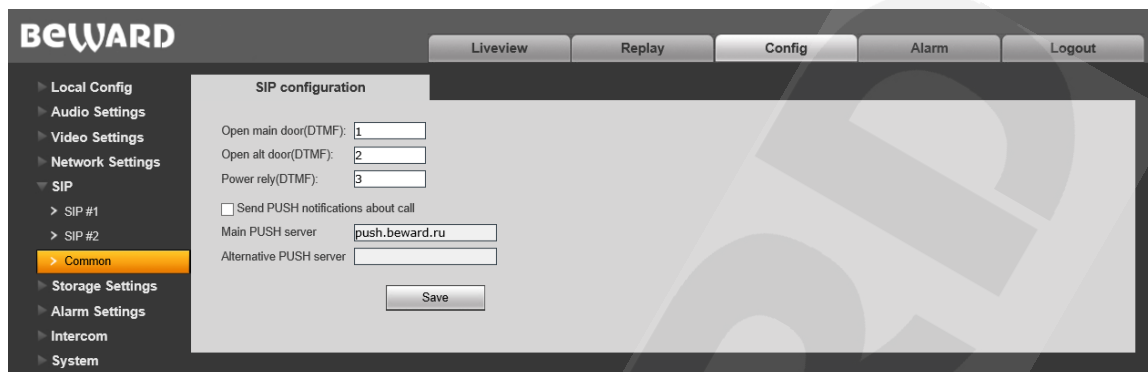
STUN does not work properly with symmetric NAT. When using symmetric NAT the IP address of the STUN server will differ from the endpoint address. Therefore the NAT address seen by the STUN server will also differ from the endpoint address used for sending data to the user agent..

**Stream type:** Select the stream type, which will be broadcast when the client and the guest are speaking. Mainstream is selected by default. Audio only option is available as well.

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

## 9.2 Common

The **Common** SIP settings menu is shown below.



The screenshot shows the BEWARD web interface with the 'Config' tab selected. On the left, a sidebar lists various settings categories: Local Config, Audio Settings, Video Settings, Network Settings, SIP, Storage Settings, Alarm Settings, Intercom, and System. Under the 'SIP' category, 'Common' is highlighted. The main content area displays the 'SIP configuration' form with the following fields: 'Open main door(DTMF)' with value '1', 'Open alt door(DTMF)' with value '2', 'Power rely(DTMF)' with value '3', a checkbox for 'Send PUSH notifications about call' which is unchecked, 'Main PUSH server' with value 'push.beward.ru', and 'Alternative PUSH server' which is empty. A 'Save' button is located at the bottom of the form.

Pic 9.2

**Open main door (DTMF):** set the value of the DTMF signal that opens the main door. Up to 3 DTMF symbols are available (0-9, #, \*).

**Open alt door (DTMF)** set the value of the DTMF signal that opens the secondary door. Up to 3 DTMF symbols are available (0-9, #, \*).

**Power Relay (DTMF):** set the value of the DTMF signal that closes the relay output. Up to 3 DTMF symbols are available (0-9, #, \*).

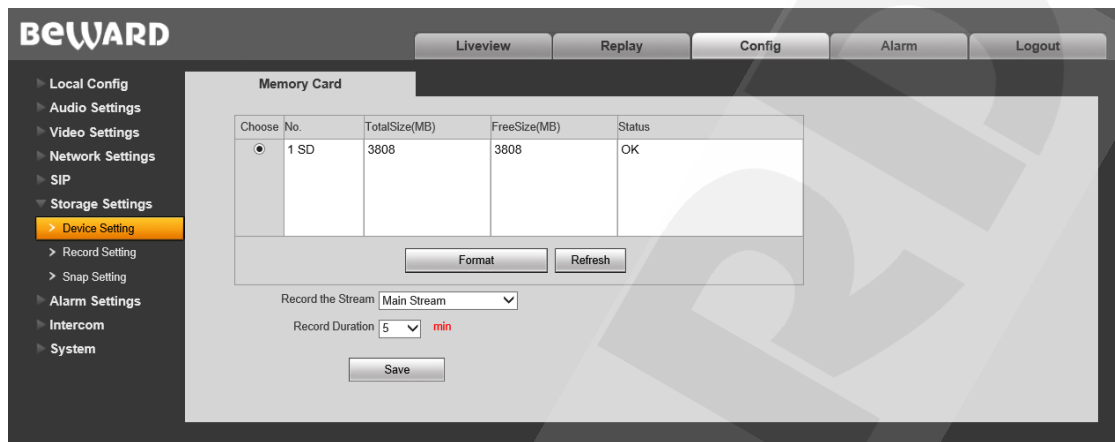
**Send PUSH notifications about call:** Enable this option to receive PUSH notifications via third-party service. Make sure to enter the address of the main PUSH server.

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

## Chapter 10. Config: Storage Settings

### 10.1. Device Settings

The **Device Settings** menu is shown below



Pic. 10.1

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.

**Record the Stream:** select the preferred videostream that will be recorded. Main stream is used by default.

**Record Duration:** Select the duration of the recorded video clips. Available values – 1 ~ 60 minutes.

#### ATTENTION!

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

Do not turn off the door station when formatting the memory card.

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

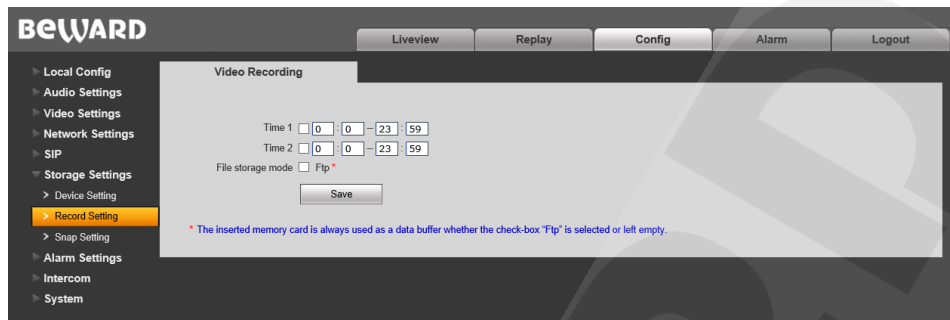
#### ATTENTION!

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

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

## 10.2. Record Settings

The **Record Settings** menu is shown below:



Pic 10.2

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

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

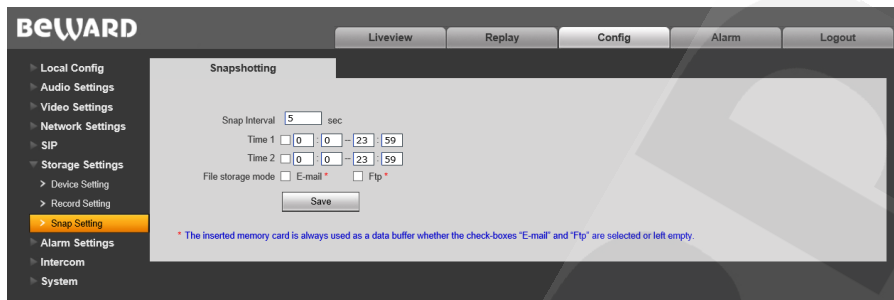
**NOTE:**

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

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

### 10.3. Snap settings

The **Snapshotting** settings menu is shown below



Pic. 10.3

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

**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.

**Snaps 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 [8.4](#)), FTP-client parameters can be set in the «**FTP**» menu (see paragraph [8.5](#)).

#### NOTE:

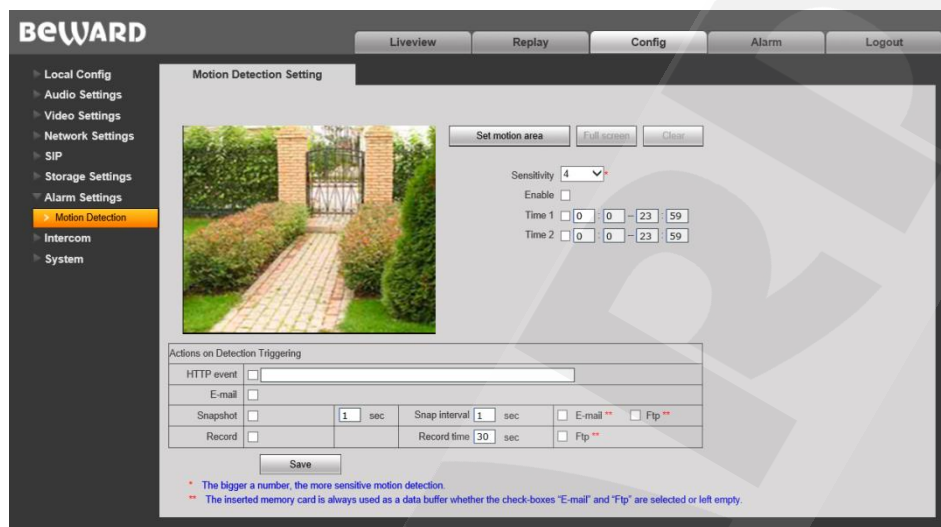
If «**FTP**» and/or «**E-mail**» options are disabled the snapshots will be stored in the memory card,  
If «**FTP**» and/or «**E-mail**» options are enabled .the snapshots will be stored in the FTP server and/or sent via E-mail

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

## Chapter 11. Config: Alarm Settings

### 11.1. Motion Detection Settings

The **Motion Detection** settings menu is shown below:



Pic. 11.1

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.

**HTTP event:** enable and set the necessary parameter in the text field. The parameters will be sent to the HTTP server (see **Config – Network settings – HTTP event**) when the motion detection trigger activates.

Maximum length – 127 symbols. «&» and «=» symbols are not supported.

If the HTTP/HTTPS event server is not set or enabled, notifications will not be sent.

**E-mail notification:** 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 door station

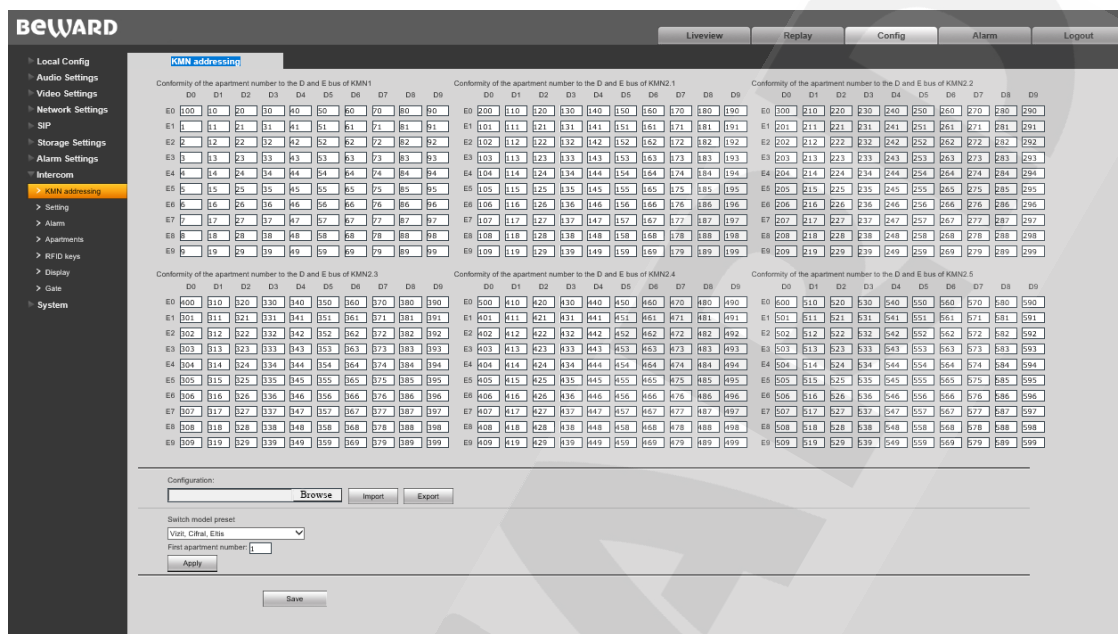
If there is no memory card installed, the inner buffer (~1mb) of the door station will be used instead. The duration of video files will vary from 1 to several seconds, depending on the bitrate value

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

## Chapter 12. Config: Intercom

### 12.1. KMN addressing

The KMN addressing settings menu is shown below:



Pic.12.1

Majority of the space is taken up by the mapping table, where apartment numbers correspond to D (first digit) and E (second digit) bus wires of the crossboard switches. Up to 6 crossboard switches can be used at once. Users can manually enter apartment numbers in the table cells.

**Configuration:** Import and export existing KMN configurations.

To Import existing KMN configurations, click **[Browse]**, select the configuration file and press **[Import]**.

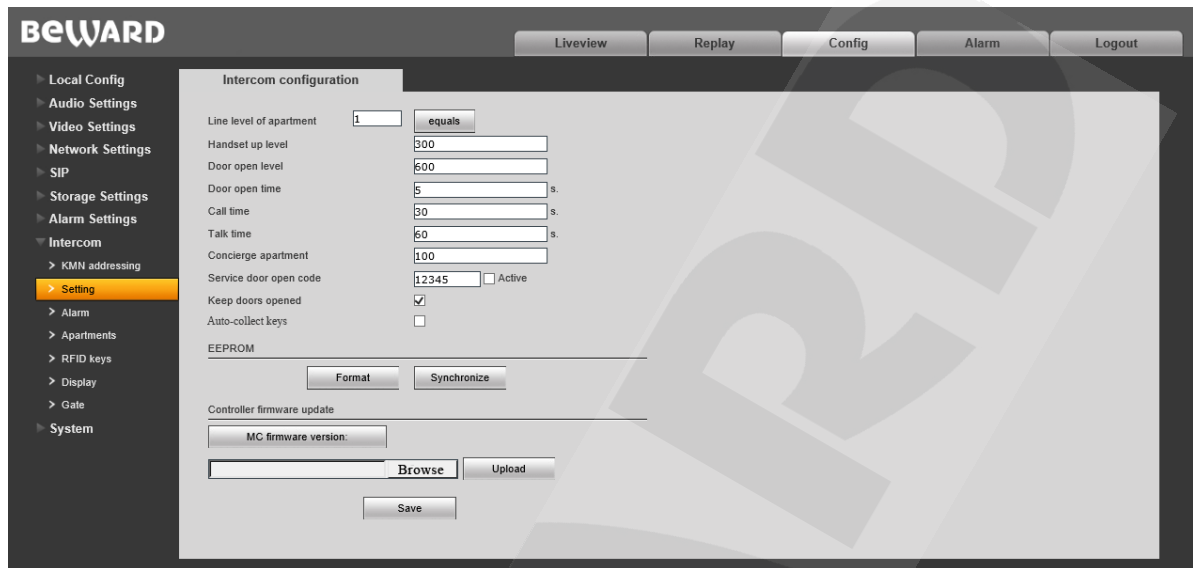
To export the currently used KMN settings, press **[Export]**. The configuration will be downloaded as a .csv file.

**Switch model preset:** Choose one of the standard presets for autofilling the mapping table, depending on the currently used crossboard switches. Available values – «Visit, Cifral, Eltis», «Metacom 80 100 160 220» and «Metacom 25». Set the number of the first apartment (default value – 1) and click **Apply** to initiate the autofilling process.

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

## 12.2. Setting

The **Intercom Configuration** menu is shown below:



Pic.12.2

Set the voltage level values by doing the following steps:

**Step 1:** Enter the apartment number. Make sure that the door phone is not picked up and press the **[Equals]** button. A number will appear (e.g. 250), Memorize it or write it down on a piece of paper.

**Step 2:** Pick up the door phone and the **[Equals]** button. A number will appear (e.g. 450),. **Headset up level** can be calculated by using the following formula:  $(450-250)/2+250$ .

**Step 3:** Press and hold the door opening button. Press the **[Equals]** button. A number will appear (e.g. 650), Deduct 50 from that number and put the result in the **Door open level** field.

**Door open time:** Set the duration of the door being opening after pressing the door opening button. Range of values – 5 ~ 30 s..

**Call time:** Set the maximum duration of a call. Range of values – 1 ~ 255 s..

**Talk time:** Set the maximum duration of a conversation between a client and a guest. Range of values – 1 ~ 63655 s.

**Concierge:** Set the number of the apartment that will receive calls when the **Concierge** button is pressed.

**Service door open code:** enter a 5-digit code via the key dial to open the door. Enter the code and press **Activate**.

**Keep doors opened:** Enable this option to keep the door open indefinitely (e.g. while the door station is being configured).

**Auto-collect keys:** automatically remember RFID keys after putting them on the RFID reader.

**EEPROM:** Microchip inside the door station. Acts as a backup storage during firmware upgrades and rebooting of the device. Can store up to 8500 RFID keys and 1500 codes.

**Format:** format the EPPROM device.

**Synchronize:** Update EPPROM data.

### Controller firmware update:

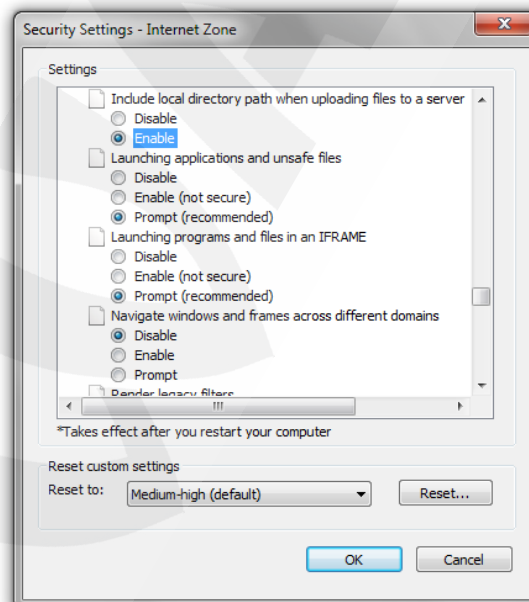
Press «**MC firmware version:**», to see the current version of the microcontroller firmware.

To update the microcontroller:

1. Click [**Browse**]. Select the update file and click [**Open**].
2. Press [**Upload**] to start update process.

### 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. 12.3).



Pic. 12.3

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

## 12.3 Alarm

The **Intercom Alarm** menu is shown below:

Pic. 12.4

The **Doors** parameters allow users to configure alarms for the main door and the additional door separately.

To change the time period, after which the notification about the open door will be sent, enable the **Long open** option and set the duration. Range of values – 100 ~ 1000 s. Set the number (SIP account) that will receive the notifications.

**Door break in:** enable this option to receive notifications whenever somebody is trying to break in the door. Set the number (SIP account) that will receive the notifications.

**SOS button:** enable this option to receive notifications whenever the **SOS** button is pressed. Set the number (SIP account) that will receive the notifications.

### Note!

The SOS signal has the highest priority and will override any other signal. For example, SOS button press will stop the on-going call between a client and a guest.

**Intercom break-in:** Enable the «**Send e-mail**» option. During any attempt to break in the Door Station, a Break-in notification will be sent to the E-mail address, set in **Config – Networks Settings – E-mail** ([see 8.4](#)).

### Long door open notification/ Door break-in notification:

Users can change the default notification sounds to custom ones (mono only).

### Note!

Supported format - .wav 8kHz mono. Max file size – 32 Kbyte

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

## 12.4 Apartments

The Apartments Configuration menu is shown below:

**Select:** Use **Previous** and **Next** buttons to select the apartment. Enable **Hide empty** to skip all apartments with empty settings fields.

**Search:** find the desired apartment by using the following parameters: **Apartment #, Door code, Registration code, RFID , Phone**

**Clear apartments:** Clear the parameters of the apartments within the set range.

Apartment parameters are listed below:

**Apartment number:** number of the currently selected apartment. Enable the **Clear** option and press the **Save** button to clear this parameter.

**Door open code:** unique code for opening the door. Must be entered via the keydial of the door station.

**RFID registration code:** unique code for registering the RFID key directly via the RFID reader. Enter this code via the dial of the door station, press the Bell button and put the RFID key to the reader to open the door. The RFID key will be added to the database.

### Note!

Enable the **Activate** options to activate Door open code and RFID registration code. To randomly generate new codes, enable the **Regenerate** option and press **Save**.

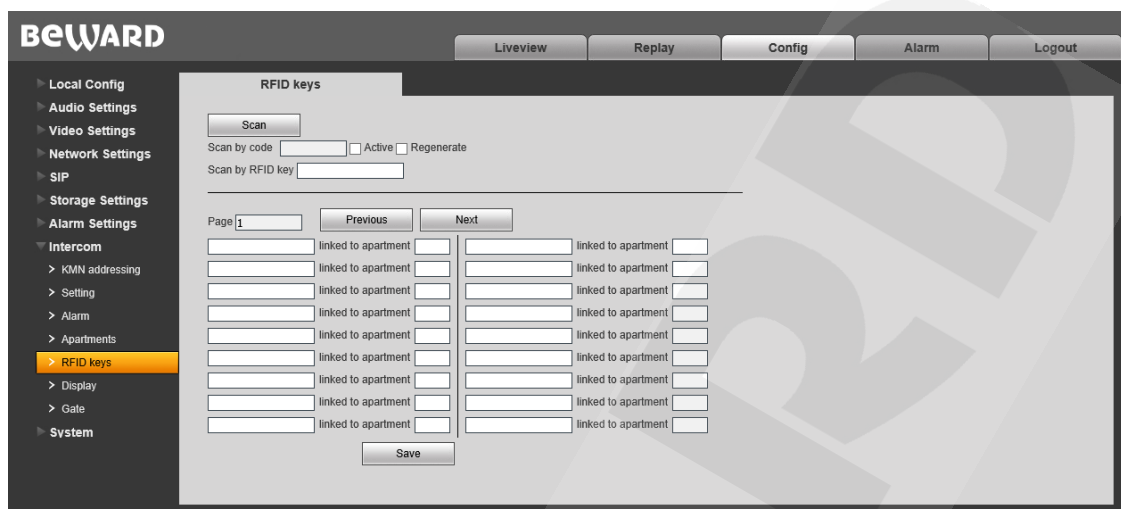
**Block KMN handset call:** the call will ignore analog door phones and go directly to IP/SIP addresses.

**Phone numbers:** IP/SIP addresses that will receive calls. Up to 5 number are available.

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

## 12.5 RFID keys

The **RFID keys** menu is shown below:



Pic.12.6

The Door Station supports up to 8500 RFID keys. The keys are scanned and added to the table as follows:

*[Name of RFID key] linked to apartment [number of the apartment].*

**Scan:** press this button scan a RDIF key and add it to the database.

**Scan by code:** The scanning mode will activate after entering the specified code via the keydial of the door station.

**Scan by RFID code:** specify the Master Key. Putting the Master Key to the RFID reader will activate the scanning mode.

The RFID keys will also be added to the database when the Autocollect keys option is enabled. (see [12.2](#)).

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

## 12.6 Display

The **Display** menu page is shown below:

The screenshot shows the BEWARD web interface. The top navigation bar includes 'Liveview', 'Replay', 'Config', 'Alarm', and 'Logout'. The left sidebar menu lists various configuration categories, with 'Display' currently selected and highlighted in orange. The main configuration area for 'Display' includes a 'Ticker' text field with an 'Active' checkbox, a 'Switch symbols timeout' field set to '1000', and five 'String' fields (String 1 to String 5), each with an 'Active' checkbox. A 'Save' button is located at the bottom of the configuration area.

Pic.12.8

Here users can configure text, shown on the LED display of the door station.

Two modes are available: Ticker and String Switching

To activate the ticker mode, perform the following steps:

**Step 1:** Enter any text into the **Ticker** field. Up to 48 characters.

**Step 2:** Enable the **Active** option.

**Step 3:** Set the **Switch symbols timeout**. Range of values (milliseconds) : 100 ~ 1000.

**Step 4:** Click **Save**.

To activate the String Switching mode, perform the following steps:

**Step 1:** Enter any text into the **String 1-5** fields. Up to 8 characters per string.

**Step 2:** Enable the **Active** option for necessary strings.

**Step 3:** Set the **Switch lines timeout**. Range of values (milliseconds) : 1000 ~ 9000.

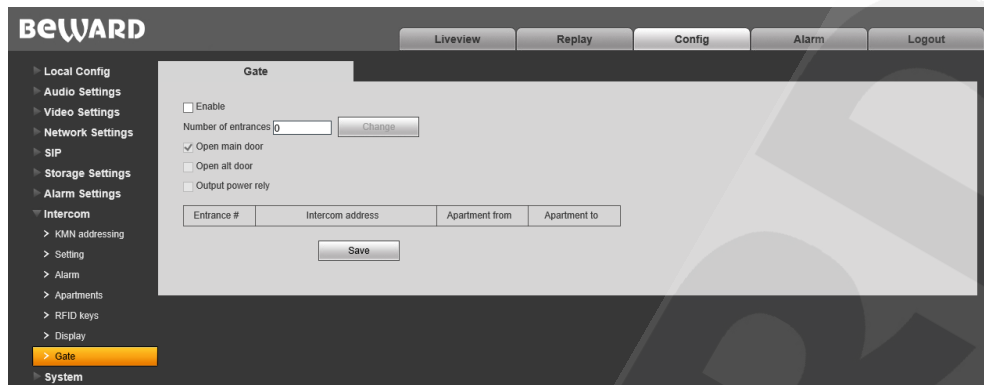
**Step 4:** Click **Save**.

### Note!

The LED display supports up to 8 characters at once (Capital letters (Russian/English), digits, some symbols).

## 12.7 Gate

The **Gate** menu page is shown below:



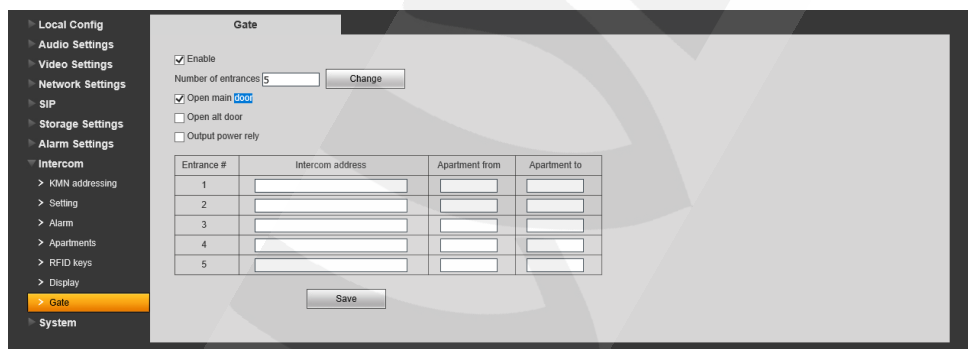
Pic. 12.8

The **Gate** mode is used to integrate several multi-user door stations, installed within a single gated housing complex, with a door station, installed on the gate.

To set up the Gate mode, perform the following steps:

**Step 1:** Press **Enable**

**Step 2:** Set the number of internal multi-user door stations, installed within the housing complex (max value - 50). Press **Change**.



Pic. 12.9

**Step 3:** Enter the SIP/IP addresses of internal door stations in **Intercom address** fields.

**Step 4:** Enter the range of apartments, assigned to each internal door station. Use the **Apartment from** and **Apartment to** fields.

**Step 5:** Click **Save**.

**Open main door:** One of the internal door stations will send an **Open door** command to the door station on the gate to open the main door.

**Open alt door:** One of the internal door stations will send an **Open door** command to the door station on the gate to open the secondary door.

**Output power relay:** One of the internal door stations will send an **Open door** command to the door station on the gate to activate the power relay contacy. The relay can be used to operate the swing gates.

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

## Chapter 13. Config: System

### 13.1. System Info

The **System Information** menu is shown below:

The screenshot displays the BEWARD web interface's 'System Information' configuration page. The left sidebar contains a menu with options like Local Config, Audio Settings, Video Settings, Network Settings, SIP, Storage Settings, Alarm Settings, Intercom, and System. The 'System' menu is expanded, showing 'System Info' as the selected option. The main content area contains a form with the following fields and values:

Device Name	IPC304
Video Standard	PAL
Language	English
Device serial number	304
Device model	DKS15100
Firmware Version	3.1.0.0.3.18.5
Build Time	Jun 15 2018 14:43:41
WEB UI Version	2.1.3.7(20180607)
UpTime	00:36:51

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

Pic. 13.1

**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 “**Upgrade**” menu (see paragraph [13.4](#)).

**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

## 13.2. System Time

The **System Time** settings menu is shown below:

Pic. 13.2

**Time Zone:** choose the time zone in accordance with location of the door station.

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

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

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

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

**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.

**Synchronize with PC:** 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 door station.

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

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

### 13.3. User Manage

The «Access Policy» settings menu is shown below:

Pic. 13.3

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

By default the door station 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”**.

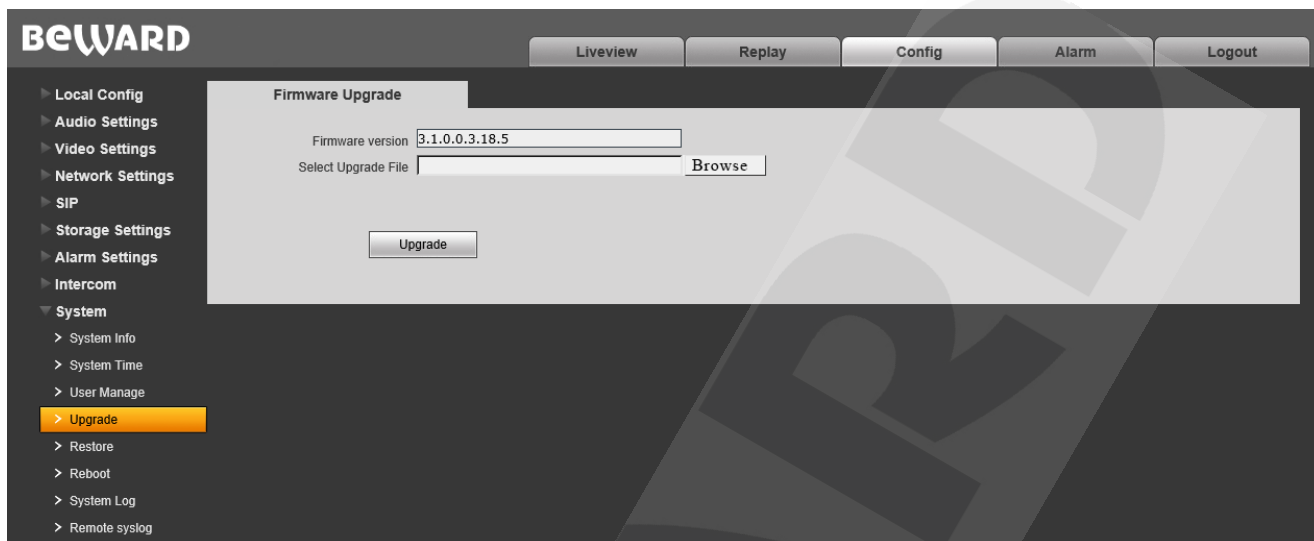
Press the **[Save]** button to apply new settings.

#### 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 (.).

## 13.4. Upgrade

The **Firmware Upgrade** menu is shown below:



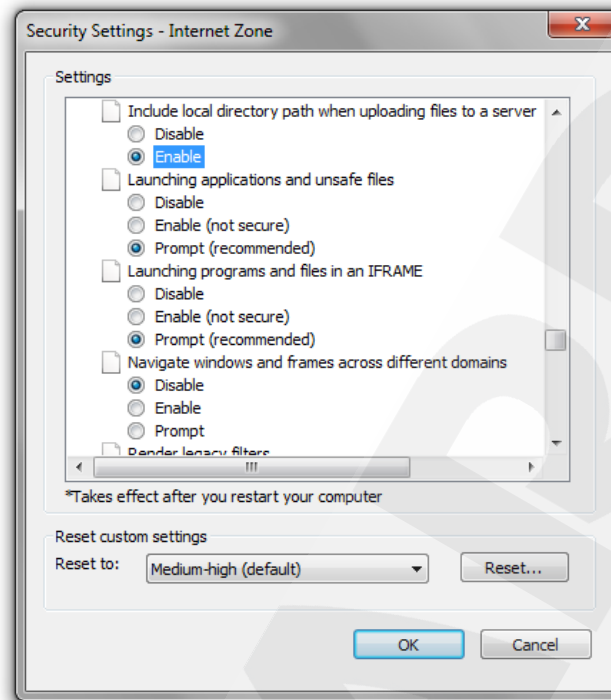
Pic. 13.4

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

3. Press the **[Browse]** button. Choose the appropriate file in the opened File Explorer window and press the **[Open]** button.
4. Press the **[Upload]** button to start upgrading. The door station 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. 13.5).



Pic. 13.5

1. Set door station parameters by default (see paragraph [13.5](#)).

**ATTENTION!**

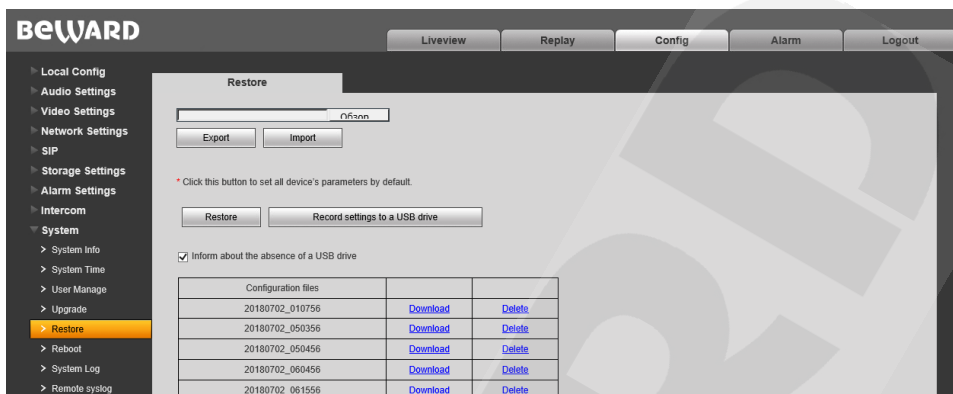
Use only appropriate firmware files which are compatible with the device model! The device may operate incorrectly and be damaged in case of using an unsuitable firmware file.

Do not disconnect the device from the network while the firmware is upgraded.

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

### 13.5. Restore

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



Pic. 13.6

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

**[Export]:** click to save door station settings as a file with the “.bak” extension. The file name contains the date and the time of saving (according to the door station 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 door station parameters by default. 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 door station (**Network Settings – LAN**) without changing.

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

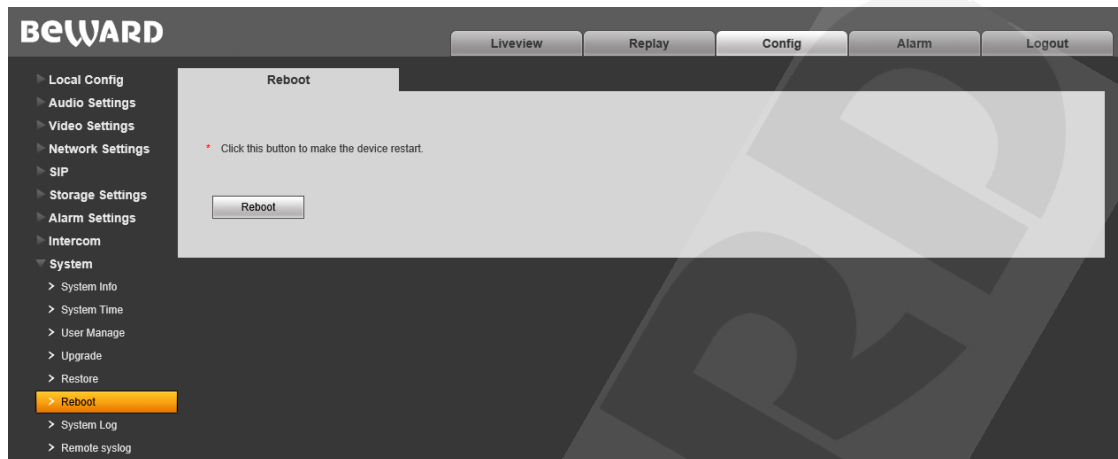
**[Record settings to a USB drive]:** save current Intercom settings to the installed USB drive.

Use **Configuration files** list to download and deleted saved Intercom parameters.

**Inform about the absence of a USB drive:** If this option is enabled, the message about the absent USB drive will be shown on both the LED display and WEB UI’s OSD.

### 13.6. Reboot

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

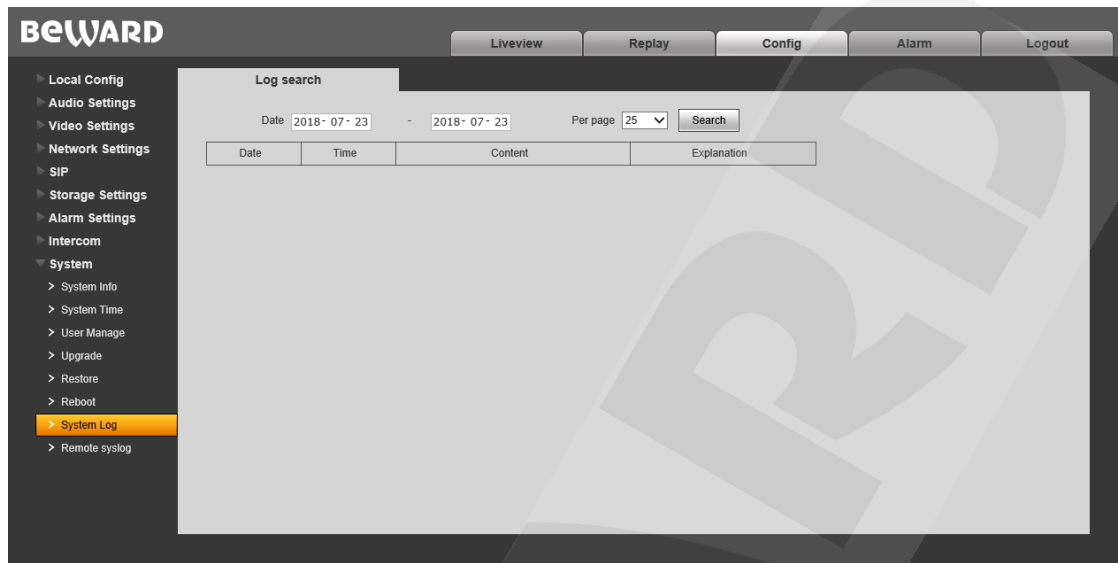


Pic. 13.7

**[Reboot]**: press this button to reboot the door station. 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.

### 13.7. System Log

The “System Log” menu is shown below:



Pic. 13.8

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

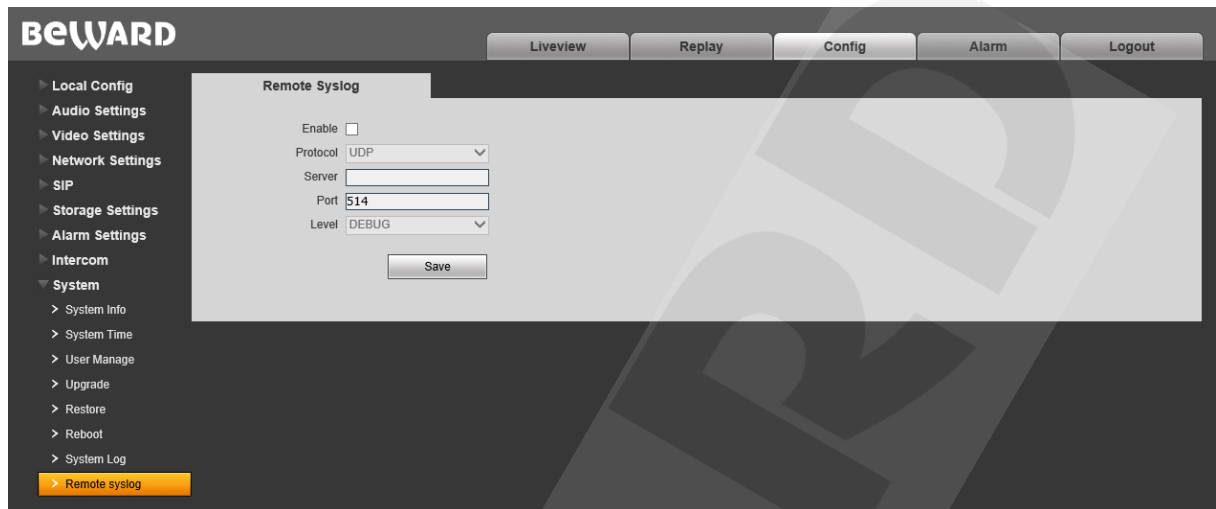
**Date:** specify the necessary search period.

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

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

### 13.8 Remote syslog

The Remote syslog menu is shown below:



Pic. 13.9

Use this menu to set up syslog parameters, that are responsible for sending notifications about IP network events.

**Enable:** activate this option to receive logs about the ongoing events.

**Protocol:** Select either UDP or TCP.

**Server/Port:** Specify the address/port of the currently used Syslog server.

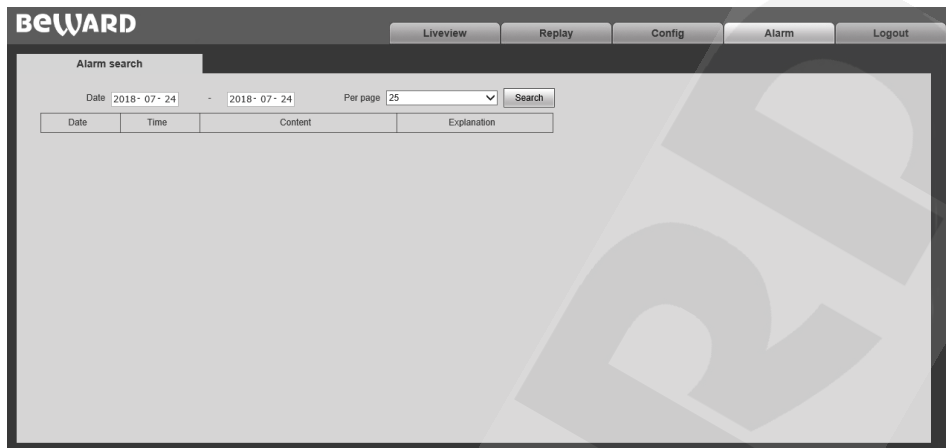
**Level:** Specify the urgency level of event messages.

<b>EMERGENCY</b>	System is unusable.
<b>ALERT</b>	Action must be taken immediately.
<b>CRITICAL</b>	Critical conditions, such as hard device errors
<b>ERROR</b>	Error conditions.
<b>WARNING</b>	Warning conditions.
<b>NOTICE</b>	Normal but significant conditions.
<b>INFO</b>	Informational messages.
<b>DEBUG</b>	Debug-level messages.

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

## Chapter 14. Alarm

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



Pic. 14.1

This menu has a similar look and functionality as the “**System Log**” menu (see paragraph [13.7](#)), except this menu is used for searching alarm events only .

## Chapter 15. Recommendations on Setting and Operation of DKS151xx

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.

### 15.1. Echo Cancellation

When using the door station 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 door station 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](#)).

## 15.2. 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

Factory default parameters are shown below:

Parameter	Value
IP address	DHCP
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. SIP settings example

#### B1. Direct connection

Setting the SIP direct connection using the MicroSIP application is given for example. In case of using other applications the setting is done in a similar way.

#### ATTENTION!

It is necessary to provide a connection channel between the devices (door station and PC with the application) for the direct connection. Pay attention that the Port 5060 is only used for establishing connection, but data are transferred via RTP (the range of port numbers by default is 1024-65535). The devices need be accessible via these ports for correct SIP operation.

Install and run MicroSIP. The application window is shown below:



Pic. B1

Go to the door station web interface menu for setting SIP connection.

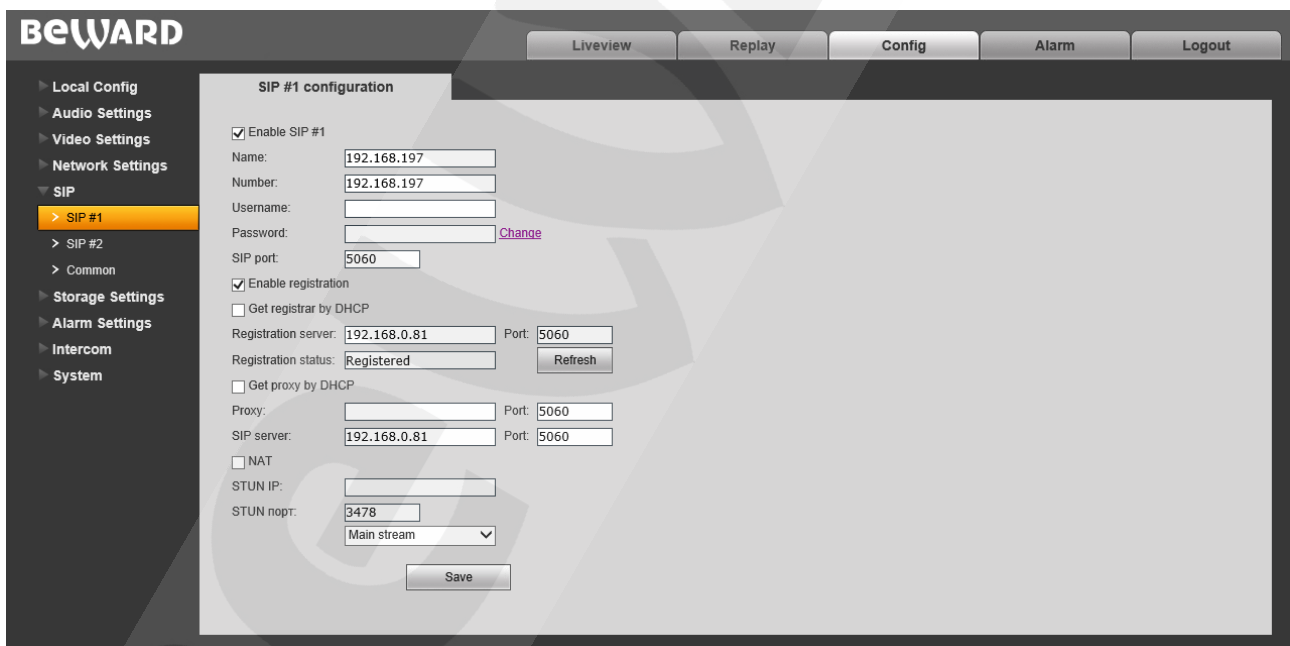
You only need specify the following parameters for the SIP direct connection:

**Enable SIP #1:** enable the SIP option.

**Name:** enter a device name for its easy identification.

**Number:** enter the door station IP address.

To apply new settings click **[Save]** (Pic. B2).



Pic. B2

Go to **Config - Intercom – Apartments**

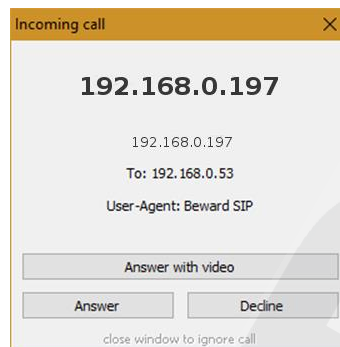
Select an apartment

Make sure that the Phone Numbers option is enabled. Enter the SIP account number into one of the **Phone #** fields.

Click **Save**.

If the settings are correct then you will see the following window after pressing the apartment number and the bell button of a door station:

:



*Pic. B3*

You can answer or cancel the call.

Setting the SIP direct connection is finished

## **Appendix D. SIP Hardware and Software (for transmitting video and sound via SIP) Compatibility Lists**

### **D1. PBX Compatibility**

- 3CX
- Asterisk 11
- Asterisk 12

### **D2. Software Compatibility**

- Jitsy 2.8.5426 (Windows Desktop, Mac OS X, Linux)
- MicroSIP 3.12.1 (Windows Desktop)
- Linphone 3.9.1 (Windows Desktop, Android)
- Grandstream Wave (Android, iOS)

### **D3. Hardware Compatibility**

- Grandstream GXV3240, GXV3275 videophones
- Yealink SIP VP-T49G

## 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.