BEWARD
IP-ВИДЕОНАБЛЮДЕНИЕ

Operation User Manual

www.beward.ru

DS06A(P) IP Video Door Station

Multiaccessible User Operation
Built-in IP Video Camera
Two-Way Audio
Electronic Motorized Lock Control

Table of Contents

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 case device breakdown.

Follow this Operation Manual.

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

- Avoid extremely low and high temperatures (The operating temperature of this 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 out 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.net/.

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

2.1. BEWARD DS06A(P) door station overview

DS06A(P) IP Video Door Station is designed for organizing IP intercom systems based on already existing local networks without using any additional equipment (e.g. separate internal monitors). To start using the door station you only have to install the software from the disk and set it up. Low cost, easy installation and remote access to the device. This device is:

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

Pic. 2.1

DS06A(P) has built-in microphone, speaker, video camera, Infrared LED and a call button, as well as vandal-resistant housing. The device allows establishing video and audio connection between the *Guest* and the *Client*, conducting surveillance of the nearby territory, control of other devices that are connected to the door station (electronic locks, garage door openers, light switches, alarm systems etc.) Infrared LED (with work distance up to 10 m) and the mechanical infrared filter allow conducting video surveillance in low-light level environments. The device is supported by modern network technologies, allowing it to be used a part of a complex IP Surveillance system.

DS06A(P) Door station is connected to the network via-T/100BASE-TX Ethernet interface. Its power is supplied from a DC 12V power source. The device also supports PoE.

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

2.1.1. Key Features

- Image sensor: 1.3 MP, CMOS 1/3" SONY Exmor^{TM}, Day/Night
- Simultaneous encoding: H.264/H264, H.264/MJPEG, MJPEG /MJPEG
- Framerate: Up to 25 fps (all resolutions)
- IR Illumination (distance up to 10 m) and a mechanical IR filter
- 4GB MicroSDHC memory card installed (up to 32GB supported)
- Multistreaming: up to 10 unique streams (only one user can be in the two-way audio mode at one time)
- Built-in web server for viewing and adjusting settings
- Built-in player for recorded videos
- Build-in microphone and speaker
- Power: DC 12 , 0.5 A / PoE 802.3af Class 0 (for DS06AP only)
- Temperature: -40°C~+50°C
- Supported protocols: TCP/IP, SIP v.2.0, PPTP, HTTP, HTTPS, FTP, SMTP, DDNS, DHCP, PPPoE, RTP, RTSP, UPnP, UDP, NTP, ONVIF v.2.41, Modbus TCP, CamDrive
- ONVIF Profile S support

2.1.2. Package contents

- DS06A(P) Door station
- Bracket with mounting kit
- Security screw with L- key
- NC103 / NC103P / NC311P controller
- RJ45-S01 (2 pcs.)
- Terminal block

ATTENTION!

Package contents and device specification are subject to change without notice

2.1.3. Default Settings

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

2.2. Purpose of this Manual

BEWARD DS06A(P) door station can be used as a video surveillance device with a built-in web server and a web interface.

You can view the video broadcast by this device via the standard internet browser or via the free software that can be downloaded from App Store and Play Market.

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

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

This Manual contain the information needed to use the DS06A(P) Door Station without installing additional software.

2.3. Minimum System Requirements

Please make sure your PC meets the following minimum requirements:

Item	Requirement
CPU	2.8 Ghz Intel or AMD
Video Card	256 mb RAM or similar
RAM	1 Gb (2Gb or higher recommended)
OS	Microsoft ® Windows Vista, Windows 7, Windows 8, Windows 10
Internet Browser	Internet Explorer 11.0 or higher

ATTENTION!

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

Chapter 3. Getting Started

3.1. Installation of ActiveX components and Authorization

Step 1: Connect the 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.

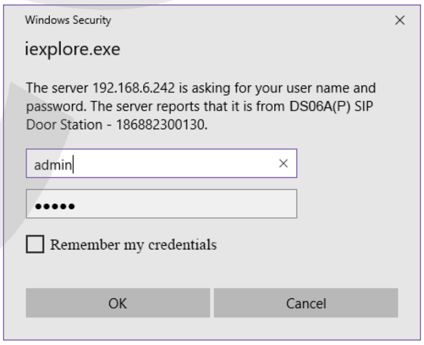
> **NOTE:**
>
> Default HTTP-port is – **80**. You don’t need to enter the port number if you connect via the default HTTP port.

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. 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



iexplore.exe

The server 192.168.6.242 is asking for your user name and password. The server reports that it is from DS06A(P) SIP Door Station - 186882300130.

admin

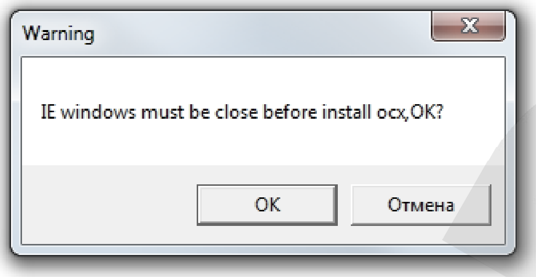
●●●●●

□ Remember my credentials

Pic. 3.1

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

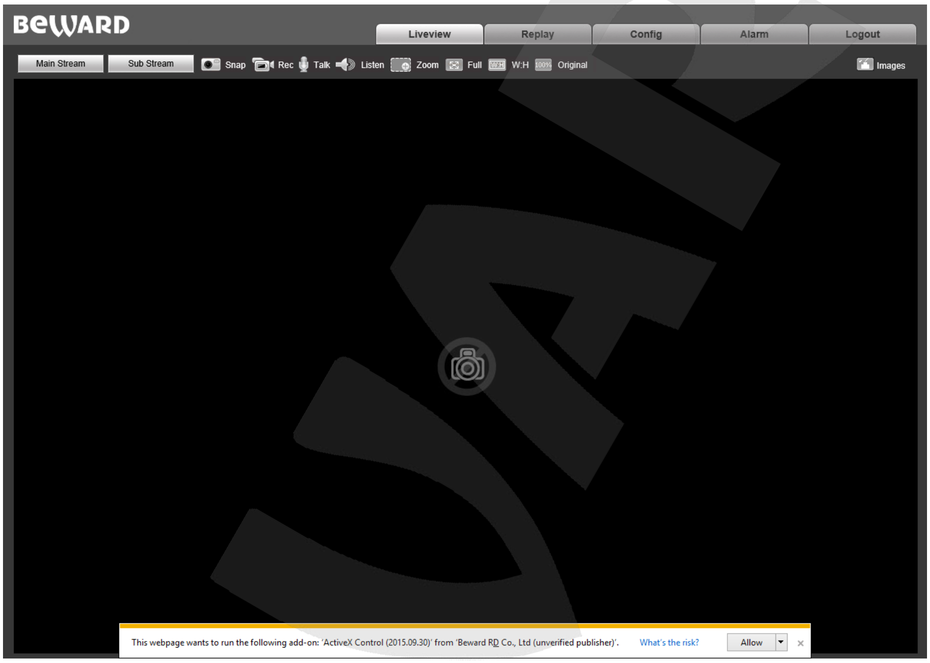
Step 4: To work with the web interface you need to install the ActiveX add-on. If the necessary components are not yet installed, you will see the following message.


Warning

IE windows must be close before install ocx,OK?

Pic. 3.2

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



This webpage wants to run the following add-on: 'ActiveX Control (2015.09.30)' from 'Beward RD Co., Ltd (unverified publisher)'.

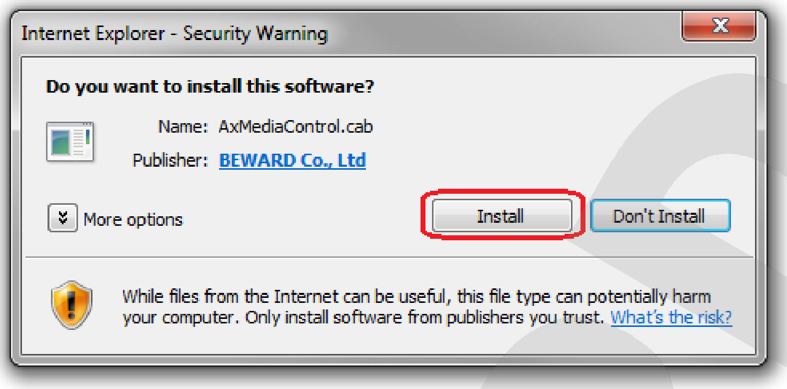
Pic. 3.3

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*).



Do you want to install this software?

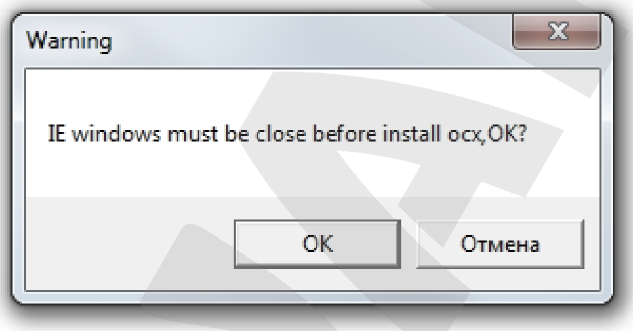
Name: AxMediaControl.cab

Publisher: BEWARD Co., Ltd

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Pic. 3.4

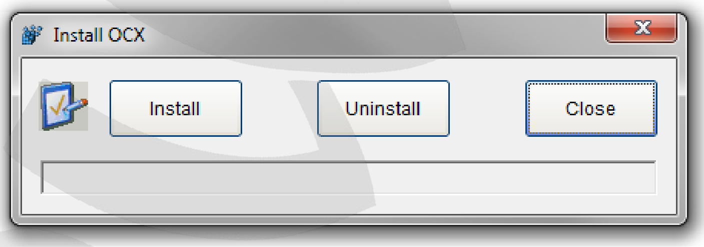
Step 6: Close Internet Explorer and click **[OK]** in the Warning window (see Pic *3.4*) if it pops up.



IE windows must be close before install ocx,OK?

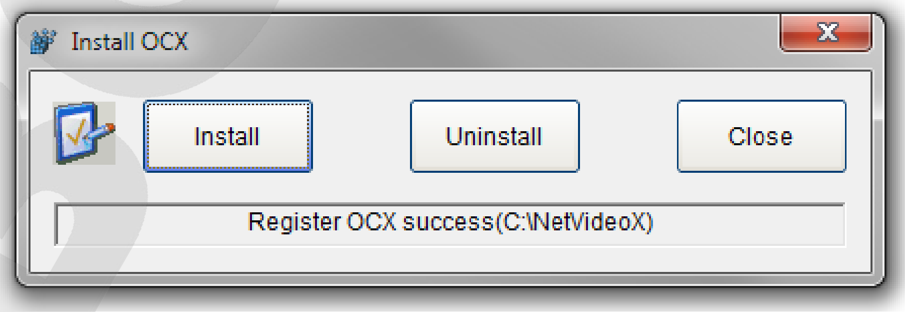
Pic. 3.5

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*).



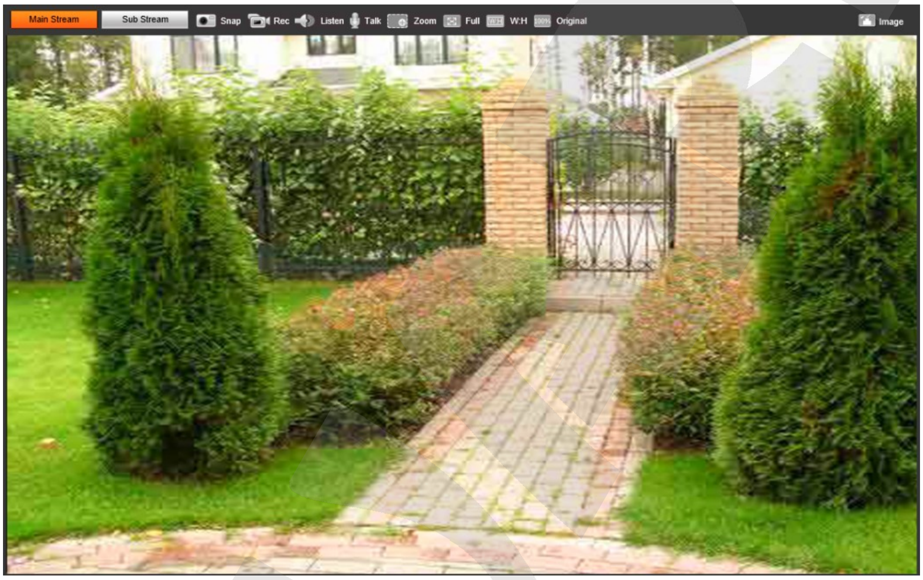
Register OCX success(C:\NetVideoX)

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..

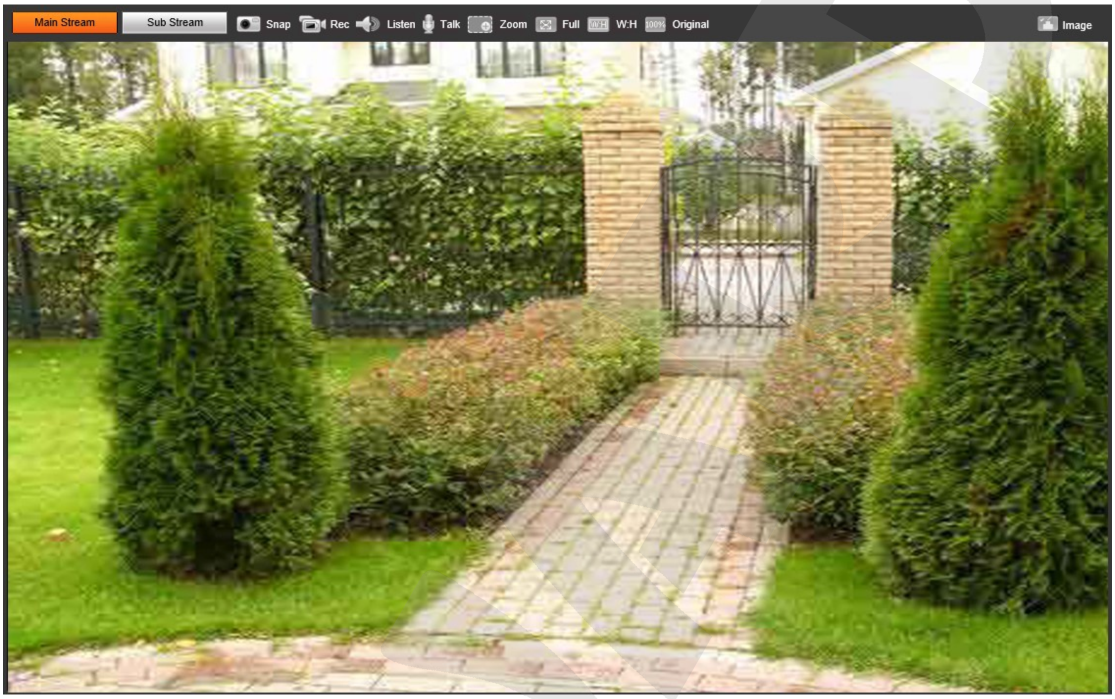


Pic. 3.8

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 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

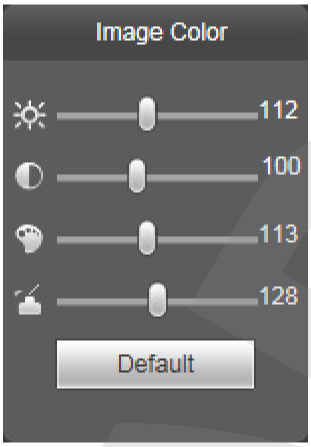
Zoom: Press this button to enlarge a specific area of the video. Press **[Zoom]**, then press and hold the left mouse button to frame the area. The enlarged area of the video will appear in a new window. Close the “Zoom In” window and press the **[Zoom]** button to disable this function.

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.

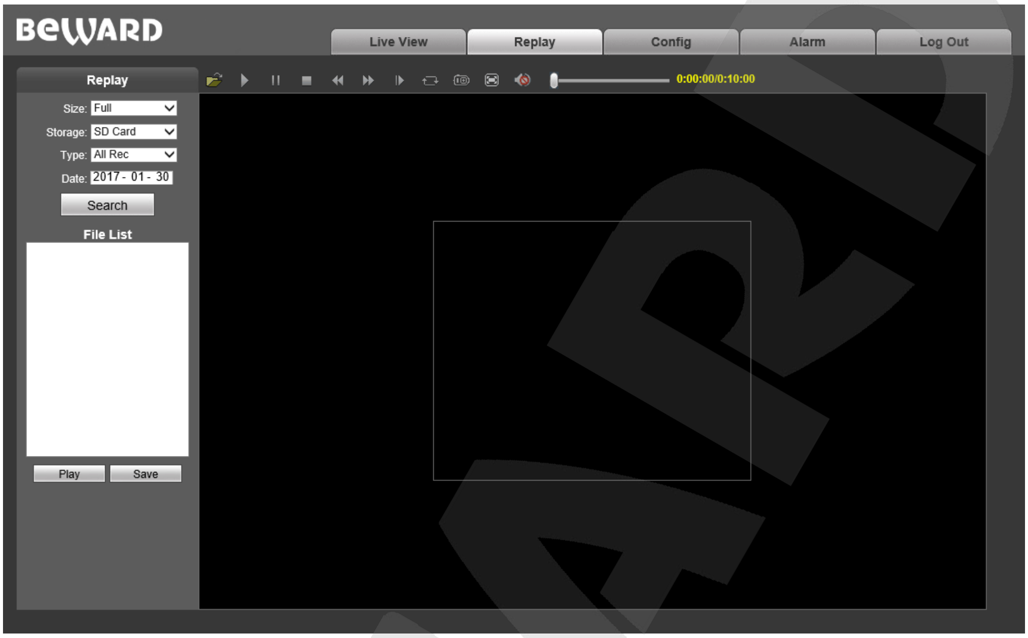
Image: Use this toolbar to adjust the following parameters: «Brightness», «Contrast», «Hue», «Saturation». If you want to restore to the default parameters, click **[Default]** (*Pic. 3.12*).



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*).



Size: Full
Storage: SD Card
Type: All Rec
Date: 2017 - 01 - 30

Pic. 4.1

Size: Change the width to heigh 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»**.

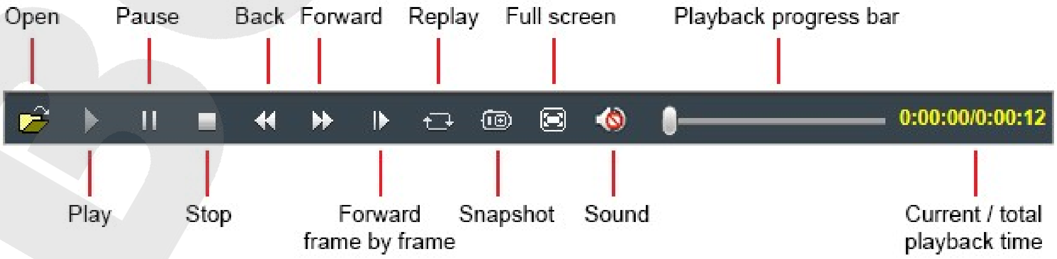
Date: choose the date for searching files.

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

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

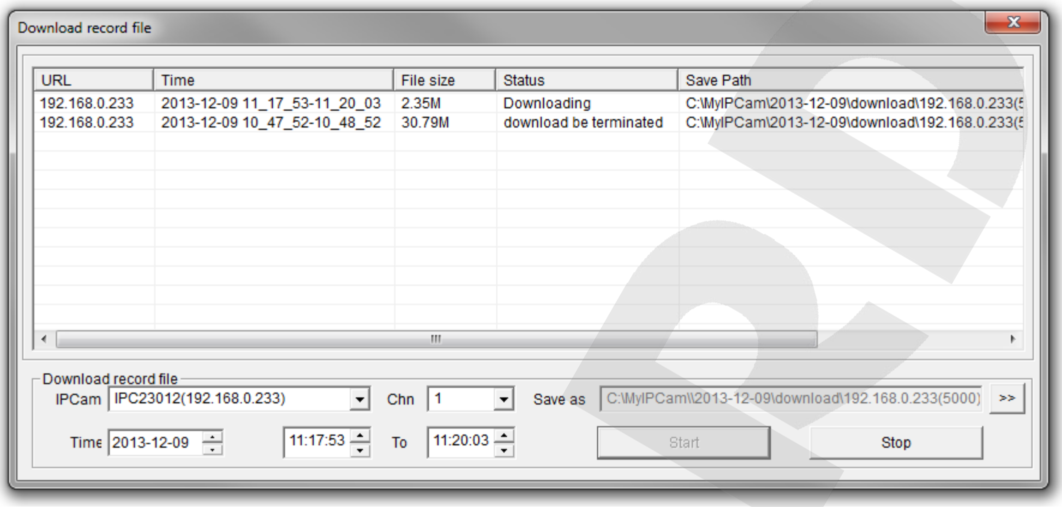
[Play]: Select a file in the File List and press this button to play it.

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*).


Download record file

URL	Time	File size	Status	Save Path
192.168.0.233	2013-12-09 11_17_53-11_20_03	2.35M	Downloading	C:\MyIPCam\2013-12-09\download\192.168.0.233(5
192.168.0.233	2013-12-09 10_47_52-10_48_52	30.79M	download be terminated	C:\MyIPCam\2013-12-09\download\192.168.0.233(5

Download record file

IPCam IPC23012(192.168.0.233) Chn 1 Save as C:\MyIPCam\\2013-12-09\download\192.168.0.233(5000)

Time 2013-12-09 11:17:53 To 11:20:03

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.

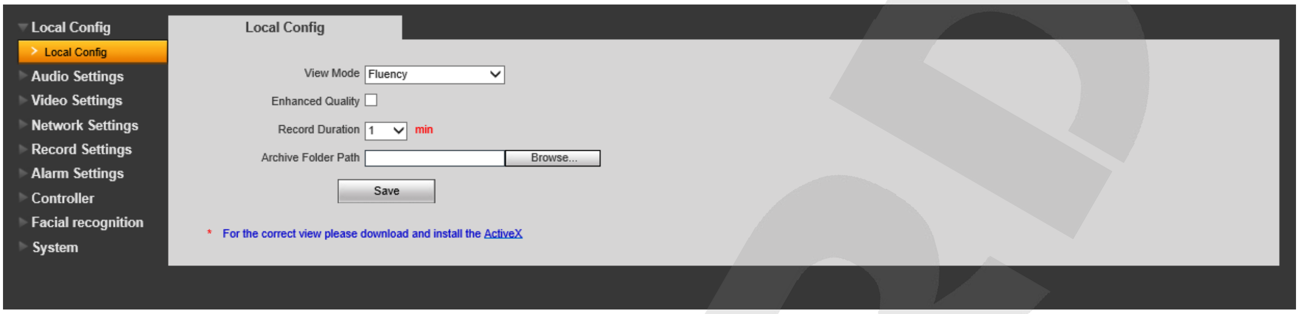
Note!

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



View Mode: Fluency

Enhanced Quality: □

Record Duration: 1 min

Archive Folder Path:

* For the correct view please download and install the ActiveX

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 cause 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 of 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).

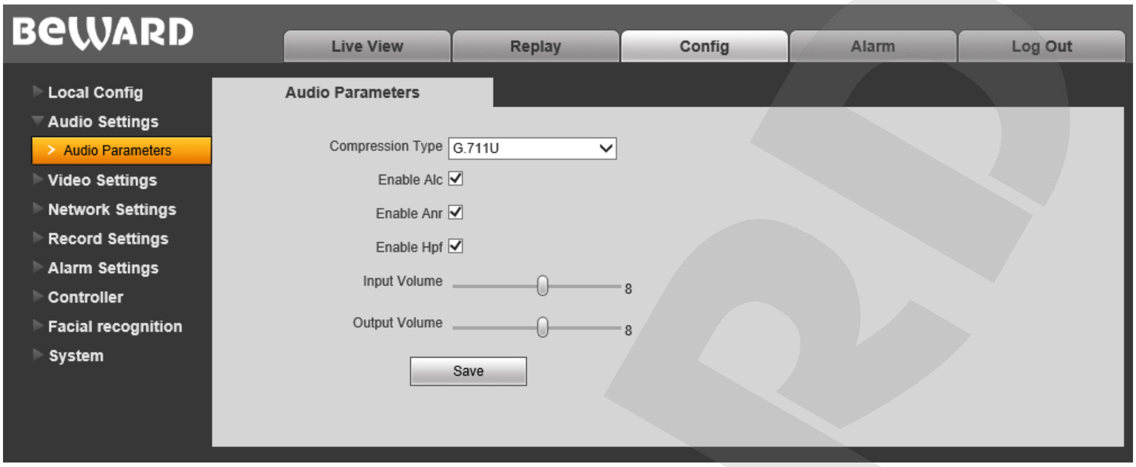
Archive Folder Path: Set the local folder to store video and image files. Default Path: **C:\MyIPCam\.**

> **NOTE:**
>
> Make sure that you 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.



Audio Parameters

Compression Type G.711U

Enable Alc ☑

Enable Anr ☑

Enable Hpf ☑

Input Volume 8

Output Volume 8

Pic. 6.1

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

Enable Alc: Turn on/off automatic level control.

Enable Anr: Turn on/off automatic noise reduction.

Enable Hpf: Turn on/off High-pass filter.

Input Volume: Set the volume level of the input audio signal. (0~15).

Output Volume: Set the volume of the output audio signal (0~15).

ATTENTION!

Adjusting the Input Volume and Output Volume parameters will affect the work of the device and may cause defects (interrupted speech, echo, etc.)

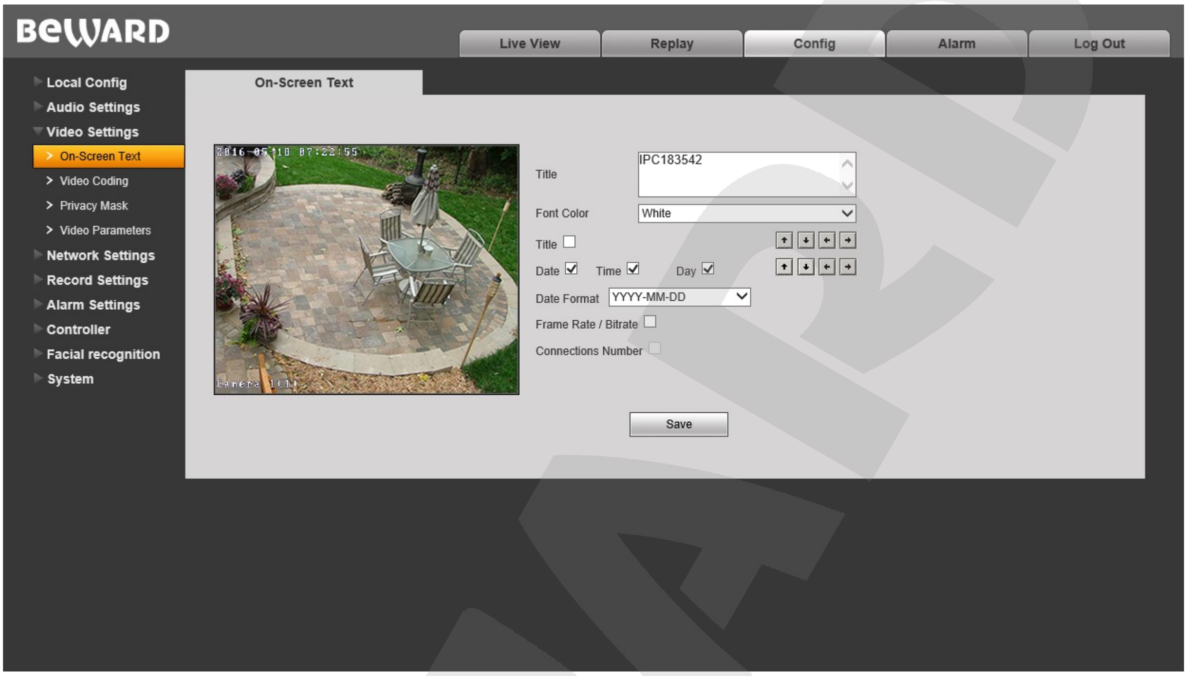
Adjust these parameters only when it is strongly necessary.

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



Title: IPC183542

Font Color: White

Title ☐

Date ☑ Time ☑ Day ☑

Date Format: YYYY-MM-DD

Frame Rate / Bitrate ☐

Connections Number ☐

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.

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).

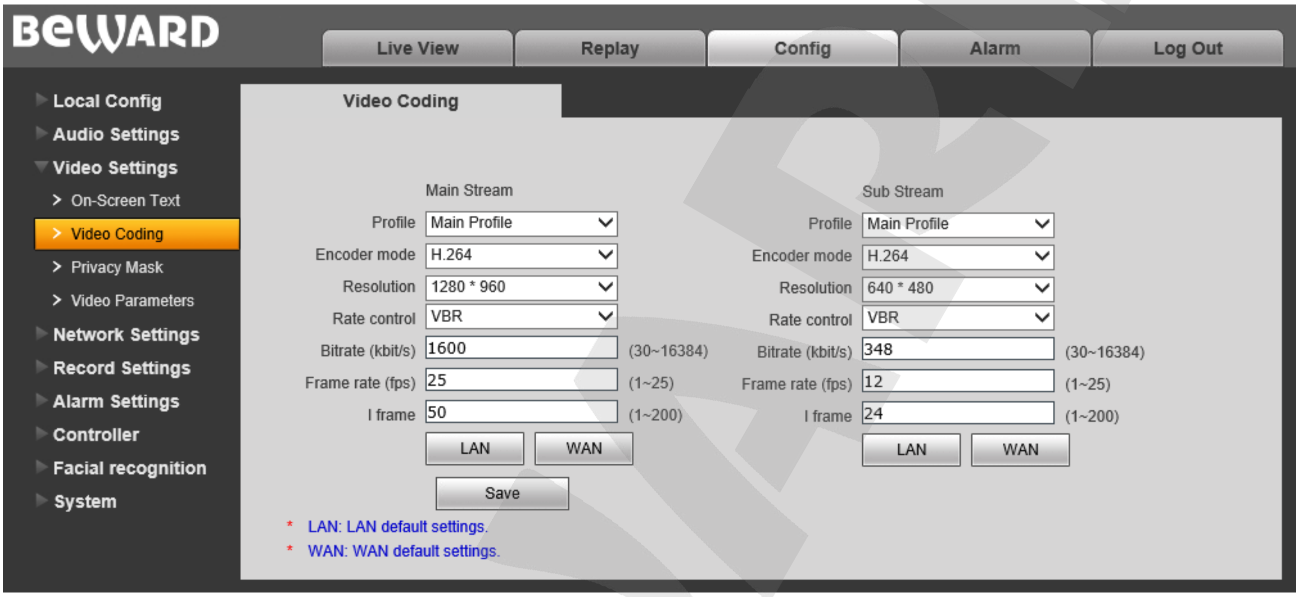
You can also change positions of the text elements. To do so use ↑↓←→. (top row for title, bottom row for everything else).

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.



Main Stream

Profile: Main Profile
Encoder mode: H.264
Resolution: 1280 * 960
Rate control: VBR
Bitrate (kbit/s): 1600 (30~16384)
Frame rate (fps): 25 (1~25)
I frame: 50 (1~200)

Sub Stream

Profile: Main Profile
Encoder mode: H.264
Resolution: 640 * 480
Rate control: VBR
Bitrate (kbit/s): 348 (30~16384)
Frame rate (fps): 12 (1~25)
I frame: 24 (1~200)

* LAN: LAN default settings.
* WAN: WAN default settings.

Pic. 7.2

Profile: Baseline, High and Main profiles 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.

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

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

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

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

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

[LAN]:

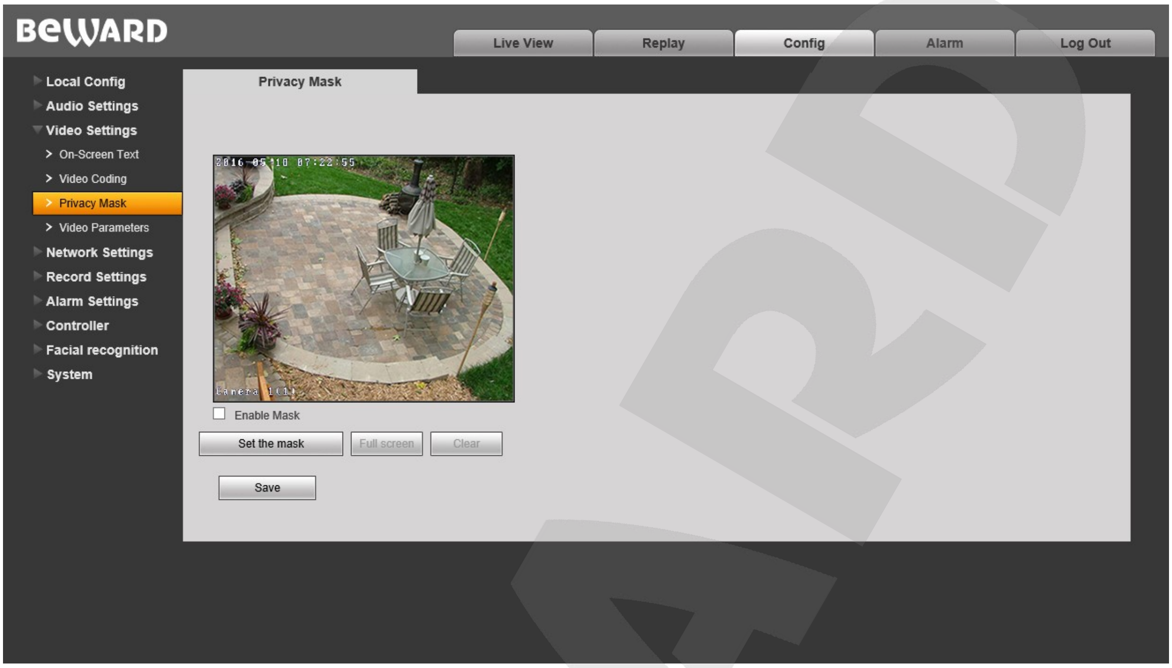
- Main stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 4096 kbit/s
- Sub stream: «I-frame» – 50, «Frame rate» – 25 fps, «Rate control» – VBR, «Bitrate» – 512 kbit/s

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

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

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*.

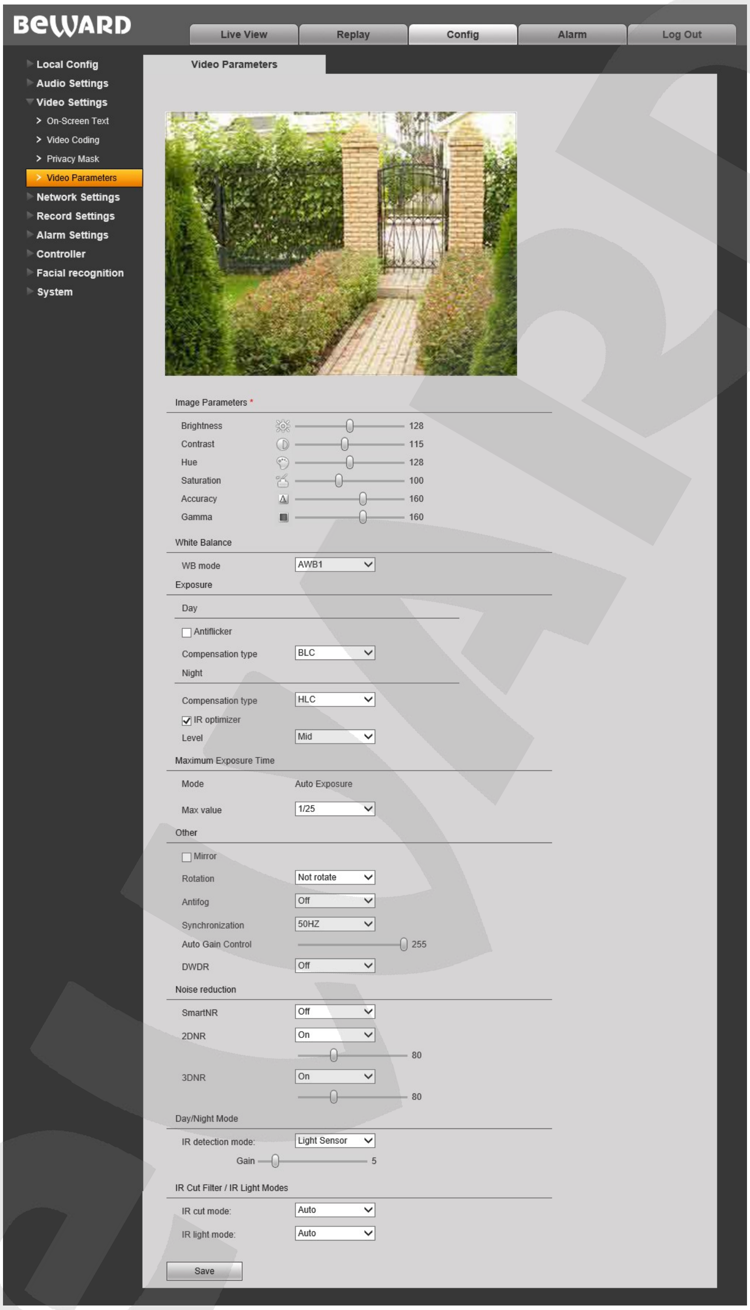


Image Parameters *

Brightness 128
Contrast 115
Hue 128
Saturation 100
Accuracy 160
Gamma 160

White Balance

WB mode: AWB1

Exposure

Day

□ Antiflicker
Compensation type: BLC

Night

Compensation type: HLC
☑ IR optimizer
Level: Mid

Maximum Exposure Time

Mode: Auto Exposure
Max value: 1/25

Other

□ Mirror
Rotation: Not rotate
Antifog: Off
Synchronization: 50HZ
Auto Gain Control 255
DWDR: Off

Noise reduction

SmartNR: Off
2DNR: On
80
3DNR: On
80

Day/Night Mode

IR detection mode: Light Sensor
Gain 5

IR Cut Filter / IR Light Modes

IR cut mode: Auto
IR light mode: Auto

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: Turn on/off different exposure settings for Day and Night modes:

Day/Night: Contains exposure parameters for day and night modes:

Antiflicker: Completely get rid of image flickering in artificial light.

Compensation Type: Choose between **BLC** and **HLC**.

- **BLC** (Back-light Compensation) optimizes brightness of the image by splitting it into several regions and applying different exposure to each region.
- **HLC** (High-light Compensation) reduces brightness of overexposed areas to improve the overall image exposure.

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. If enabled, the level of intensity can be changed (**Low**, **Mid** and **High**).

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

Other: Contains the following parameters:

Mirror: Reflect the image.

Rotate: Rotate the image by 180 degrees.

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

Synchronization:

- **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.

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

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

Noise Reduction: Contains the following parameters:

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.

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. The Gain level can be adjusted

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

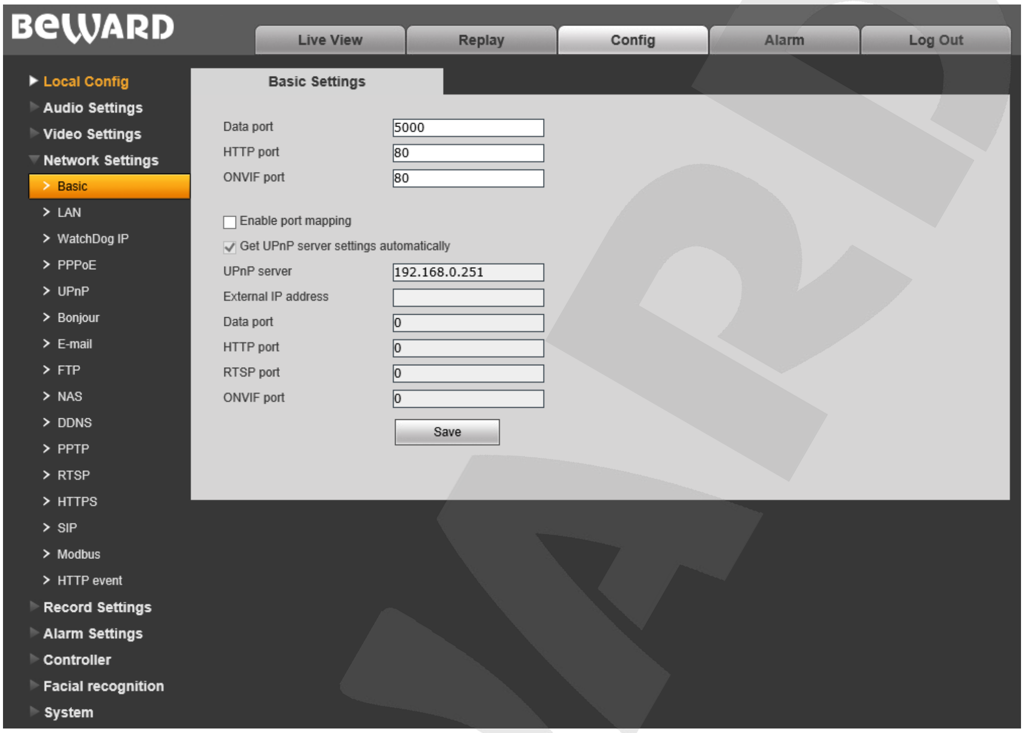
- **ICR:** Blocks infrared wavelengths for better rendition of colors.
  - **«On at night»:** Blocks IR spectrum during the Day Mode, transmits IR spectrum during the Night Mode
  - **«On in a daytime»:** Transmits IR spectrum during the Day Mode, blocks IR spectrum during the Night Mode
- **IR Light:** 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.

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

Chapter 8. Config. Network Settings

8.1. Basic

The “Basic Settings” menu is shown below.



Data port 5000
HTTP port 80
ONVIF port 80

☐ Enable port mapping
☑ Get UPnP server settings automatically

UPnP server 192.168.0.251
External IP address
Data port 0
HTTP port 0
RTSP port 0
ONVIF port 0

Pic. 8.1

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

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

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

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.

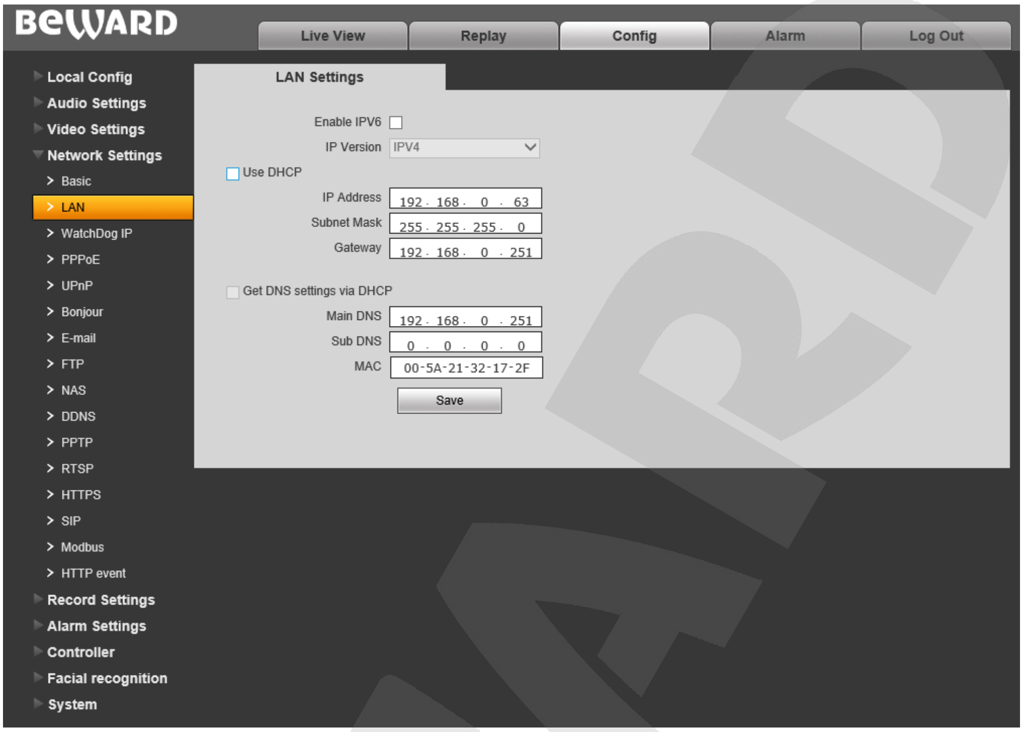
ATTENTION!
Your router must support map mapping in order for this function to work.

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.



Enable IPV6 ☐

IP Version IPV4

☐ Use DHCP

IP Address 192 . 168 . 0 . 63

Subnet Mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 0 . 251

☐ Get DNS settings via DHCP

Main DNS 192 . 168 . 0 . 251

Sub DNS 0 . 0 . 0 . 0

MAC 00-5A-21-32-17-2F

Pic. 8.2

Enable IPv6: Allows 128-bit IP addresses for door station connections. If enabled.

IP Version (available if IPv6 is enabled): Select «IPV6», to use 128-bit IP addresses

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

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.

Get DNS settings via DHCP: DHCP is used to obtain DNS settings.

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.

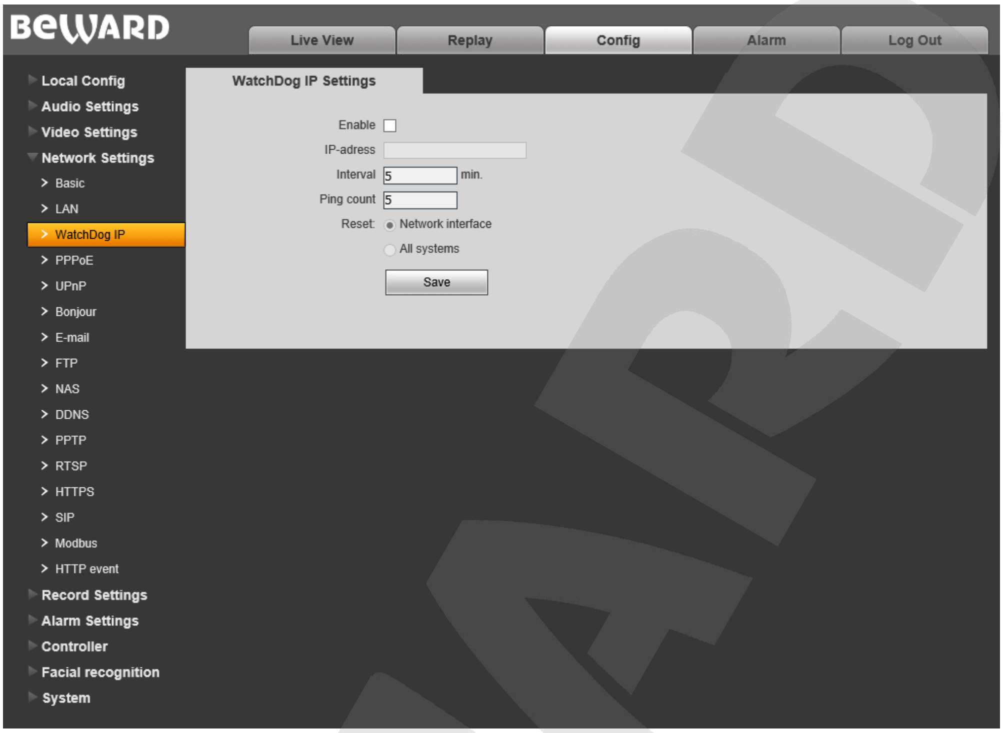
ATTENTION!

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

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

8.3. WatchDog IP

The Watchdog IP settings menu is shown below.



WatchDog IP Settings

Enable ☐

IP-adress

Interval 5 min.

Ping count 5

Reset: ● Network interface

○ All systems

Save

Pic. 8.3

Watchdog IP automatically restarts the device in case of system jams

Enable: Enable/disable Watchdog IP.

IP address: IP address of the server that will be periodically pinged to check the system status

Interval: Enter the time interval (in minutes) between pings.

Ping: Enter the number of pings that will be sent each time.

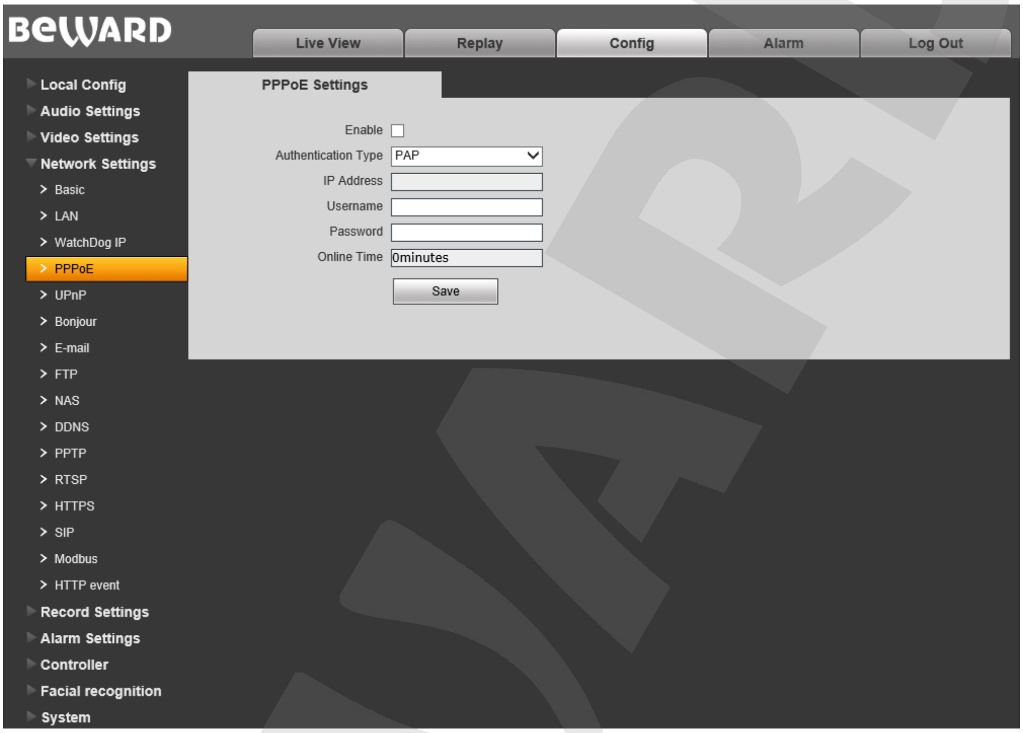
Choose whether only the **Network Interface** will restart, or **All systems.**

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

8.4. PPPoE

The “PPPoE” settings menu is shown below.

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



PPPoE Settings

Enable □
Authentication Type PAP
IP Address
Username
Password
Online Time 0minutes

Pic. 8.4

Enable: Enable/disable PPPoE.

Authentication Type: choose the authentication protocol.

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

Username: Enter your username for the PPPoE connection.

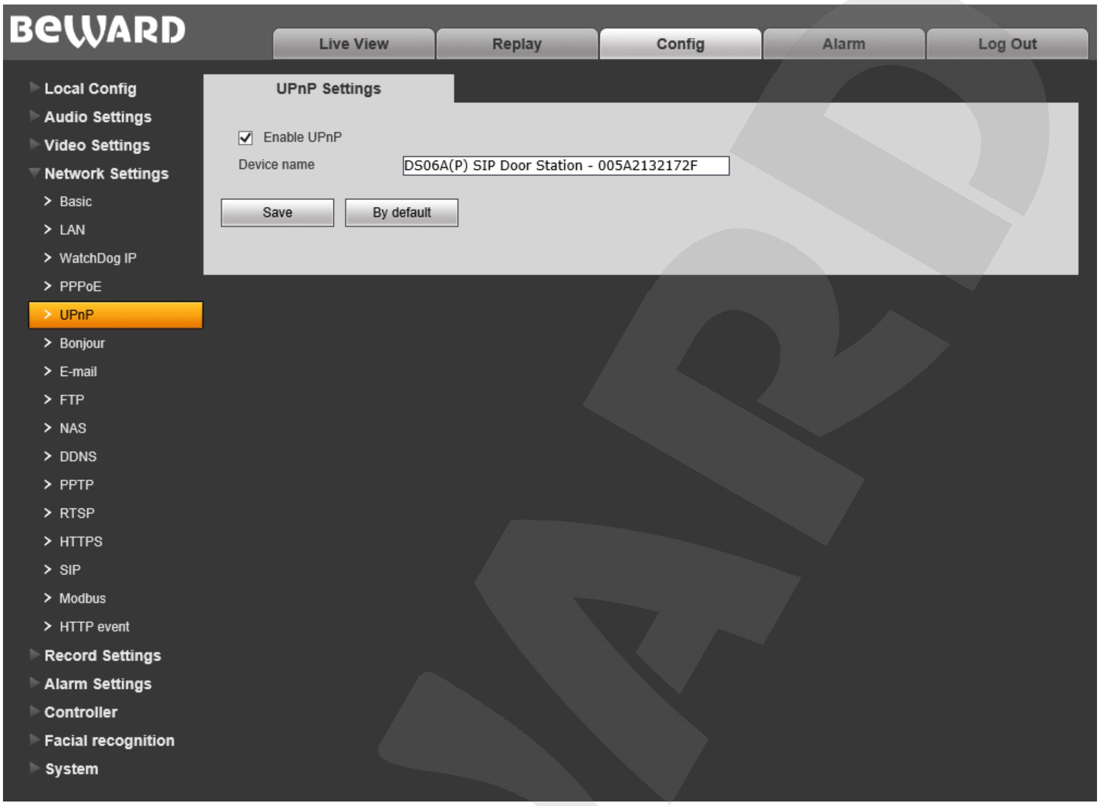
Password: Enter your password for the PPPoE connection.

Online Time: Duration of connection.

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

8.5. UPnP

The “**UPnP**” settings menu is shown below



☑ Enable UPnP

Device name DS06A(P) SIP Door Station - 005A2132172F

Pic. 8.5

Enable UPnP: Enable\disable network detection via UPnP

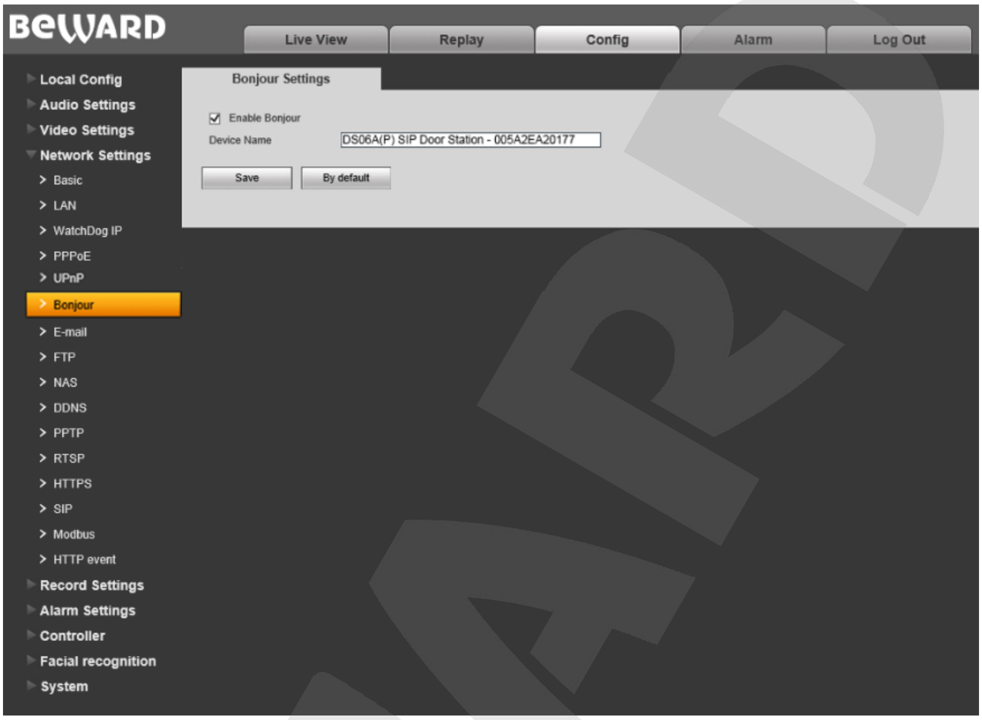
Device name: Name that will be displayed in UPnP search results.

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

Press **[By Default]** to reset to default parameters.

8.6. Bonjour

The “**Bonjour**” settings menu is shown below



☑ Enable Bonjour

Device Name: DS06A(P) SIP Door Station - 005A2EA20177

Pic. 8.6

Enable Bonjour: enable/disable network detection via Bonjour.

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

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

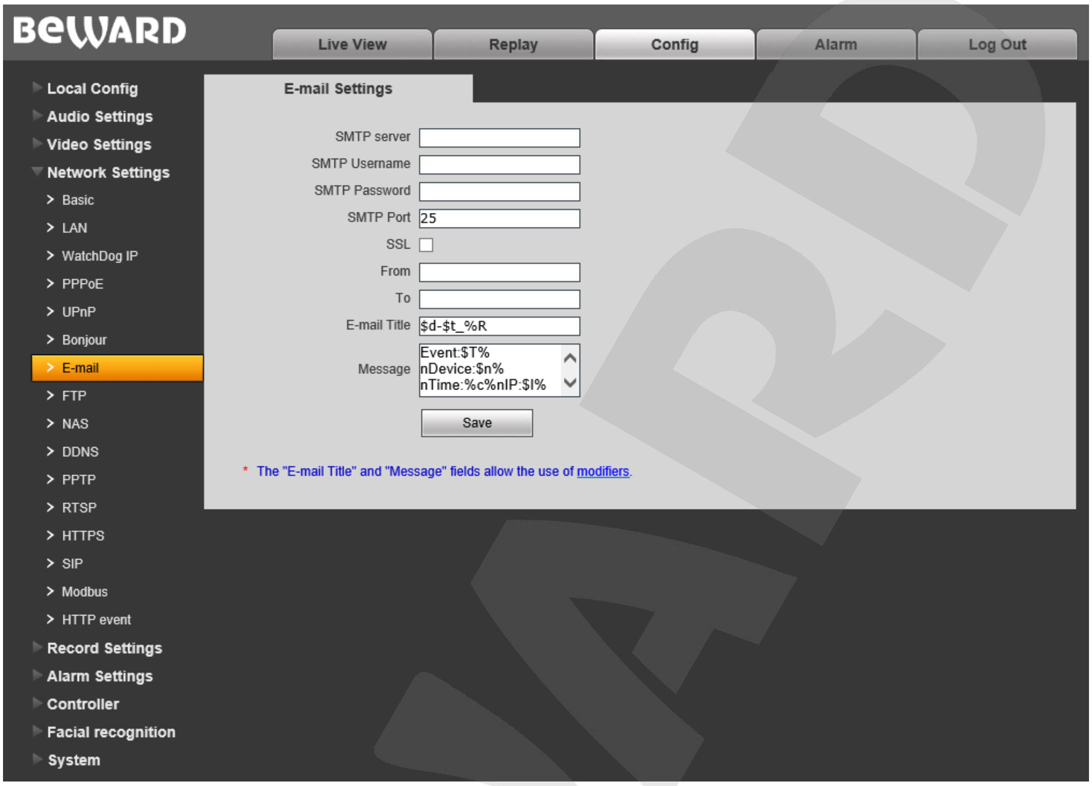
Press **[By default]** to reset to default parameters.

Note!

For more information about using the Bonjour protocol in Windows OS, please visit the official Apple website.

8.7. E-mail

The “**E-mail**” settings menu is shown below



SMTP server
SMTP Username
SMTP Password
SMTP Port 25
SSL □
From
To
E-mail Title $d-$t_%R
Message Event:$T% nDevice:$n% nTime:%c%nIP:$I%

* The "E-mail Title" and "Message" fields allow the use of modifiers.

Pic. 8.7

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.

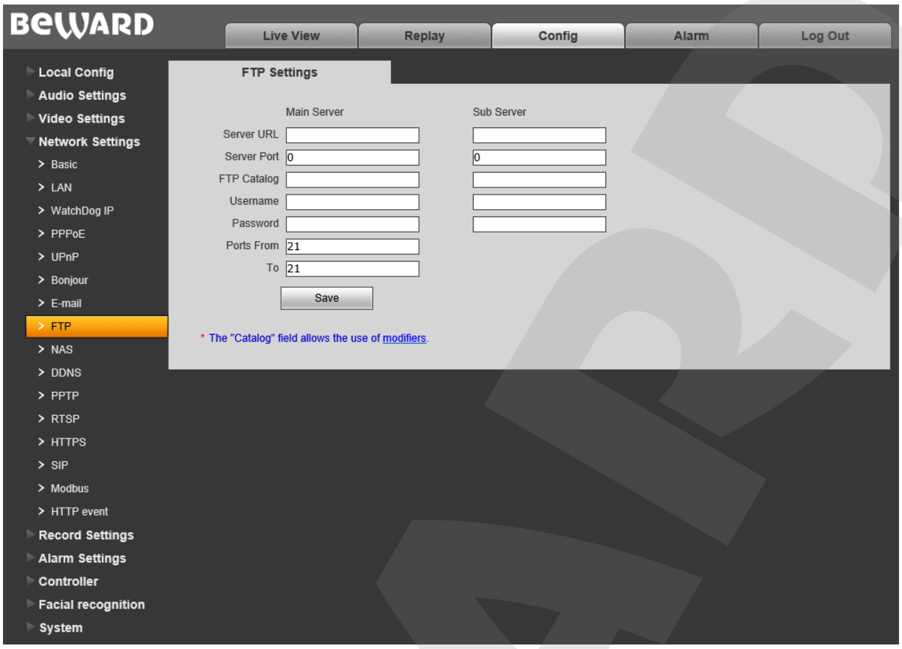
SMTP port: Enter the port number of the SMTP server (default value – 25).

SSL: Enable if your Internet provider requires SSL.

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

8.8. FTP

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



	Main Server	Sub Server
Server URL		
Server Port	0	0
FTP Catalog		
Username		
Password		
Ports From	21	
To	21	

* The "Catalog" field allows the use of modifiers.

Pic. 8.8

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.

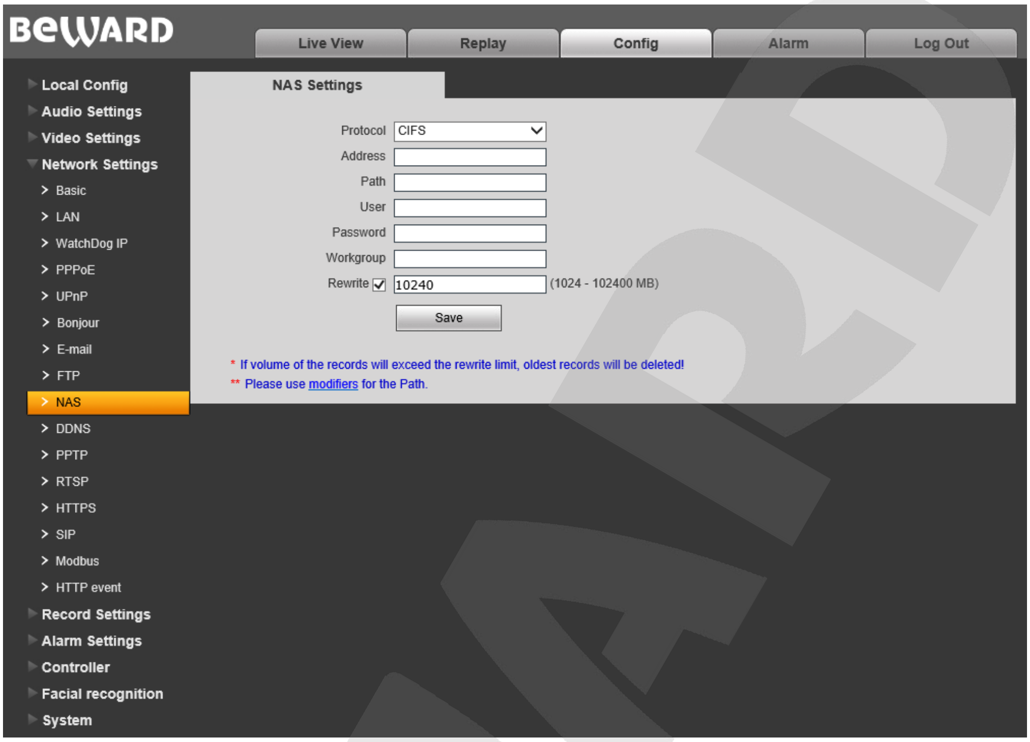
Port from /to: Range of ports to access the FTP server.

> **NOTE:**
>
> Make sure you have enough rights to save files to the FTP server in use

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

8.9. NAS

The “**NAS**” settings menu is shown below:



Protocol: CIFS

Address:

Path:

User:

Password:

Workgroup:

Rewrite ☑ 10240 (1024 - 102400 MB)

* If volume of the records will exceed the rewrite limit, oldest records will be deleted!

** Please use modifiers for the Path.

Pic. 8.9

This menu contains parameters used for sending video footage and snapshots to the NAS server.

Protocol: Select the access protocol for the NAS server. **CIFS** is for Windows OS-based storages, while **NFS** is for Unix-based systems (for example, Linux OS).

Address: IP address of the NAS server.

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

> **NOTE:**
> In the **Path** field, modifiers can be added to the filename. Too see the full list of available modifiers, please click the “modifiers” hyperlink.

> **NOTE:**
> If you are using a Windows OS storage, the path should look like this: **//IP/Folder**, where **IP** is the IP address of the network storage or PC folder with open access, **Folder** is the folder which is used to record files within the network storage.
> If you are using a Unix-based system, the path should look like this: **IP:/Folder**

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

Workgroup: Set the name of the workgroup for the Windows networks.

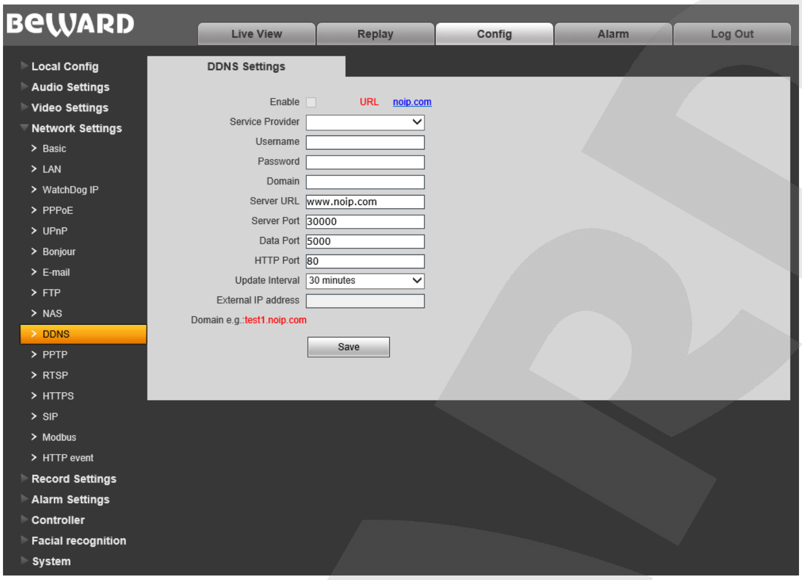
Rewrite: Set the maximum size in megabytes. If the stored files start to exceed it, the older files will start to be overwritten.

> **NOTE:**
> Make sure you have the appropriate rights to save files to the NAS server in use

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

8.10. DDNS

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



DDNS Settings

Enable □ URL noip.com
Service Provider
Username
Password
Domain
Server URL www.noip.com
Server Port 30000
Data Port 5000
HTTP Port 80
Update Interval 30 minutes
External IP address
Domain e.g.:test1.noip.com

Pic. 8.9

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.

Server Provider: 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.

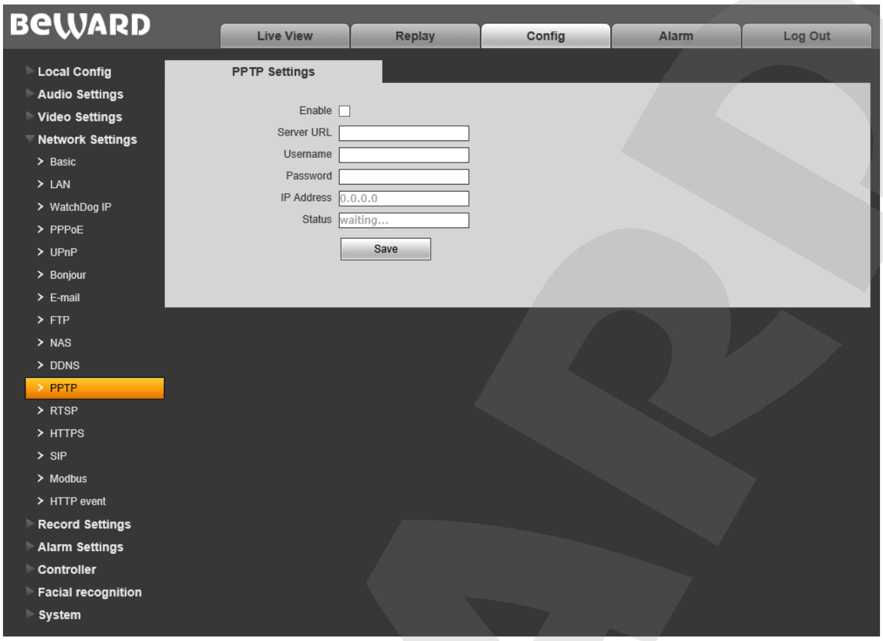
Update Interval: Set the interval at which the device will update IP address on the DDNS server after IP address change.

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

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

8.11. PPTP

The “**PPTP**” settings menu is shown below:



Enable □

Server URL

Username

Password

IP Address 0.0.0.0

Status waiting...

Pic. 8.11

Enable: Enable/disable PPTP.

Server URL: Enter the IP address or the domain name of the PPTP server.

Username: Enter your username to access the PPTP server.

Password: Enter your password to access the PPTP server.

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

Online Time: PPTP connection status.

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

8.12. 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.

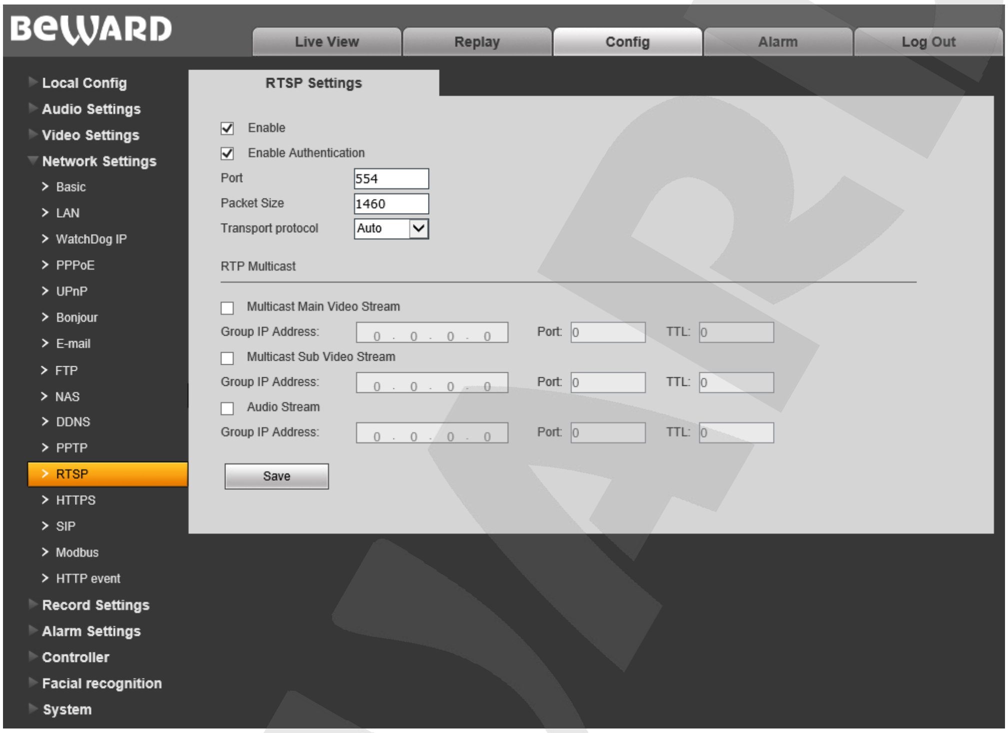
Request example: **rtsp://192.168.0.99:554/av0_0**.

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:



RTSP Settings

☑ Enable

☑ Enable Authentication

Port 554

Packet Size 1460

Transport protocol Auto

RTP Multicast

□ Multicast Main Video Stream

Group IP Address: 0 . 0 . 0 . 0 Port: 0 TTL: 0

□ Multicast Sub Video Stream

Group IP Address: 0 . 0 . 0 . 0 Port: 0 TTL: 0

□ Audio Stream

Group IP Address: 0 . 0 . 0 . 0 Port: 0 TTL: 0

Save

Pic. 8.12

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>.*

Port: RTSP port. Default vale: 554.

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

RTP multicast: Broadcast settings for audio and video streams in multicast networks

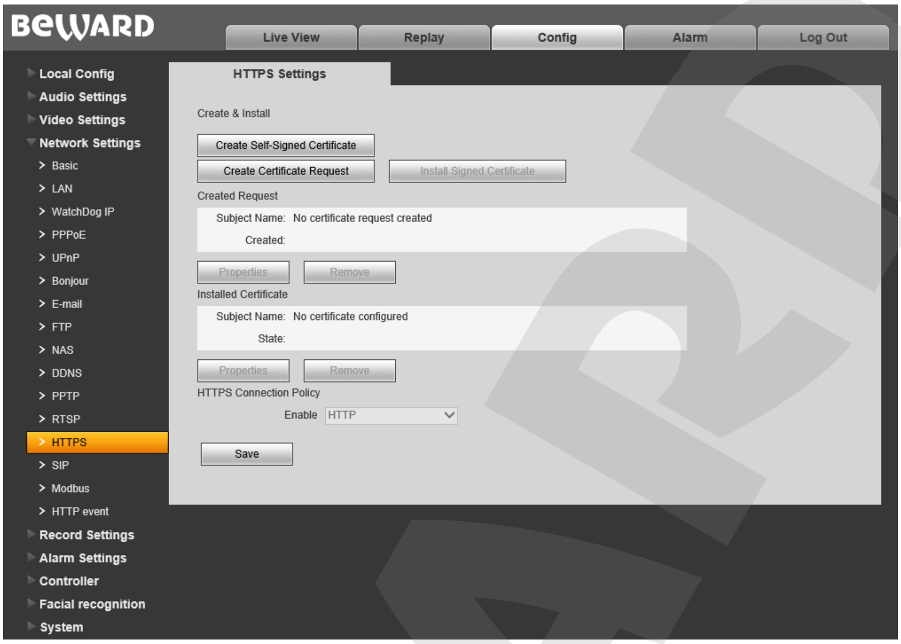
Press **[Save]** to apply new settings.

ATTENTION!

RTP multicast should be supported by your router.

8.13. HTTPS

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



Subject Name: No certificate request created
Created:

Subject Name: No certificate configured
State:

Enable HTTP

Pic. 8.13

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»**.

Installed Certificate: Name and state of the installed certificate.

[Properties]: Examine the properties of the current certificate

[Remove]: Remove current certificate.

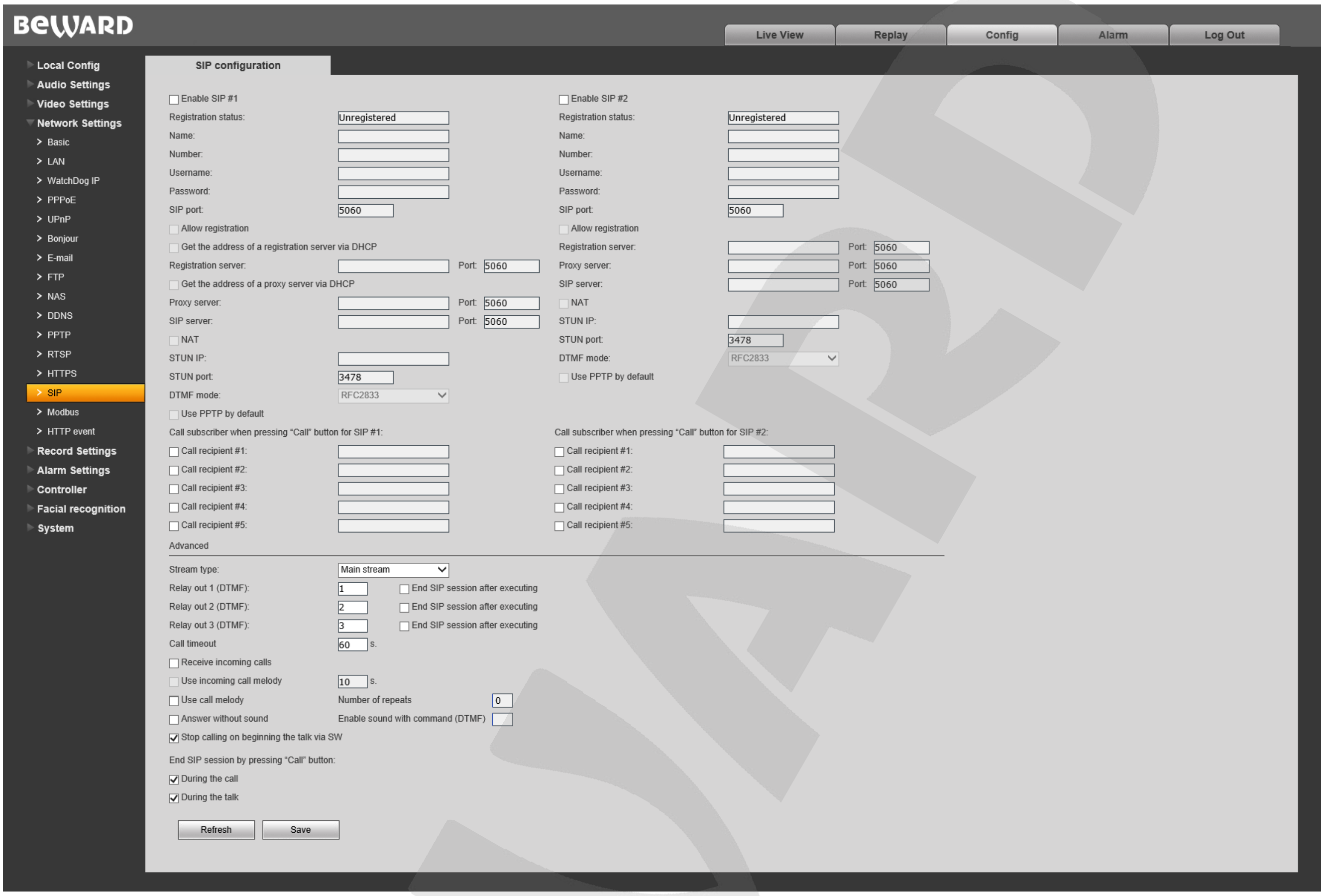
HTTPS Connection Policy: Select protocol in use. Available protocols: HTTP, HTTPS, HTTP & HTTPS.

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.

8.14. SIP

The **“SIP”** settings menu is shown below:



SIP configuration

☐ Enable SIP #1

Registration status: Unregistered

Name:

Number:

Username:

Password:

SIP port: 5060

☐ Allow registration

☐ Get the address of a registration server via DHCP

Registration server: Port: 5060

☐ Get the address of a proxy server via DHCP

Proxy server: Port: 5060

SIP server: Port: 5060

☐ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

☐ Use PPTP by default

Call subscriber when pressing “Call” button for SIP #1:

☐ Call recipient #1:

☐ Call recipient #2:

☐ Call recipient #3:

☐ Call recipient #4:

☐ Call recipient #5:

☐ Enable SIP #2

Registration status: Unregistered

Name:

Number:

Username:

Password:

SIP port: 5060

☐ Allow registration

Registration server: Port: 5060

Proxy server: Port: 5060

SIP server: Port: 5060

☐ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

☐ Use PPTP by default

Call subscriber when pressing “Call” button for SIP #2:

☐ Call recipient #1:

☐ Call recipient #2:

☐ Call recipient #3:

☐ Call recipient #4:

☐ Call recipient #5:

Advanced

Stream type: Main stream

Relay out 1 (DTMF): 1 ☐ End SIP session after executing

Relay out 2 (DTMF): 2 ☐ End SIP session after executing

Relay out 3 (DTMF): 3 ☐ End SIP session after executing

Call timeout 60 s.

☐ Receive incoming calls

☐ Use incoming call melody 10 s.

☐ Use call melody Number of repeats 0

☐ Answer without sound Enable sound with command (DTMF)

☑ Stop calling on beginning the talk via SW

End SIP session by pressing “Call” button:

☑ During the call

☑ During the talk

Pic. 8.14

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.

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.

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..

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

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

Call subscriber when pressing “Call” button: Call recipient by pression the “Call” button on the door station panel. This function is disabled if no Call recipient is selected.

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

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

Relay Out 1-3 (DTMF): Set the value of the DTMF signal. The relay outputs will close when the signal is received. For example, the door will open when the specified phone button is pressed. Up to 3 DTMF symbols are available (0-9, #, *). These fields are empty by default.

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

Call timeout: The amount of time during which the door station will call the subscriber. Available values: 10~300 s.

Receive incoming calls: Automatically receive incoming calls using the SIP account(s). If the receiving account is not available the door station cancels the call and send the cancel message to the caller.

Use Incoming call melody: Define the duration of the melody that plays during incoming calls. Available values: 1~30 s.

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

Number of repeats: Set how many times the call melody should be repeated. If the value is set to «0» the ringtone melody will play an infinite number of times.

Answer without sound: When enabled the call recipient will see and hear the guest but the guest will not be able to hear the recipient or be aware that the connection has been established.

Enable sound with command (DTMF): Set the value of the DTMF command (available symbols: 0-9, #, *) used to enable sound transmission from the recipient to the guest.

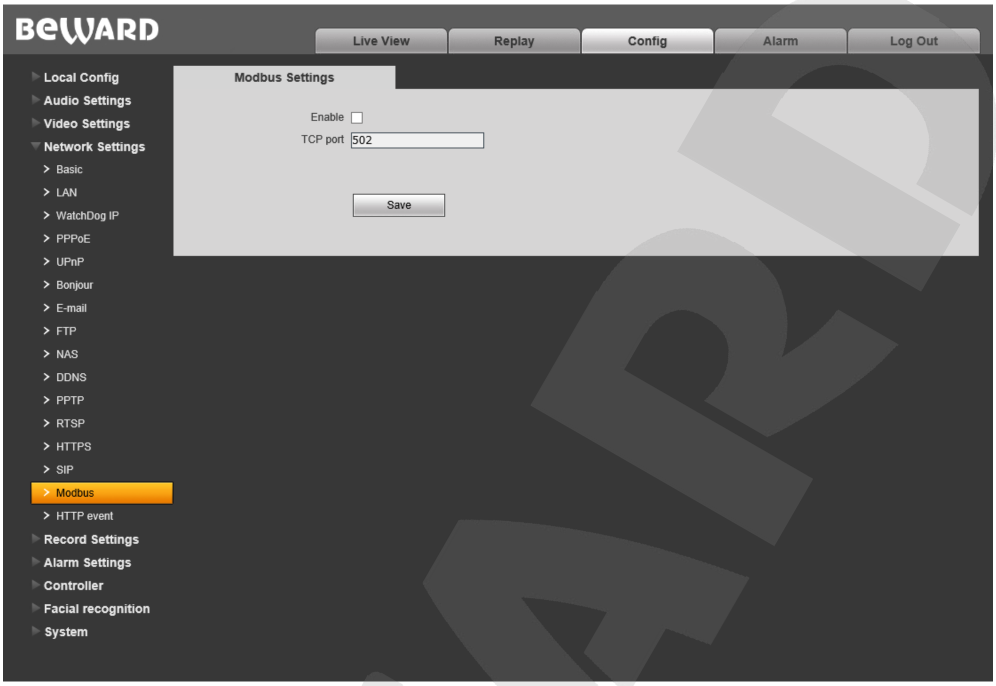
Stop calling on beginning the talk via SW: Automatically end calls, if the recipient answered with the use of Beward software or compatible applications**.**

End SIP session by pressing "Call" button: Enables the subscriber on the door station side to end the SIP session by pressing the "Call" button. This option can be used **during the call** or **during the talk**. Both options are enabled by default.

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

8.15. Modbus

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



Modbus Settings

Enable □

TCP port 502

Pic. 8.15

Use the Modbus protocol to connect to compatible equipment.

Enable: Enable\disable Modbus.

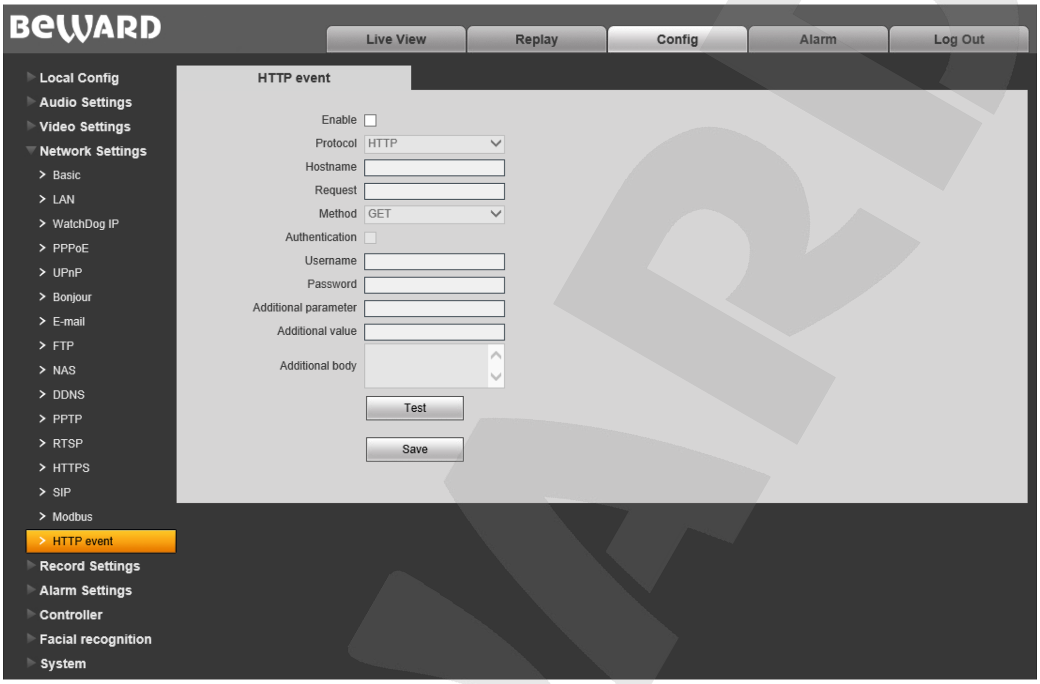
TCP port: Number of the port for the Modbus protocol. Default number – 502.

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

8.16. 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:



HTTP event

Enable □
Protocol HTTP
Hostname
Request
Method GET
Authentication □
Username
Password
Additional parameter
Additional value
Additional body

Pic. 8.16

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. «&» и «=» 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 theURL «http://www.eventserver.org/alarm».

Method: Method of sending notifications: GET or POST.

Authentication: 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

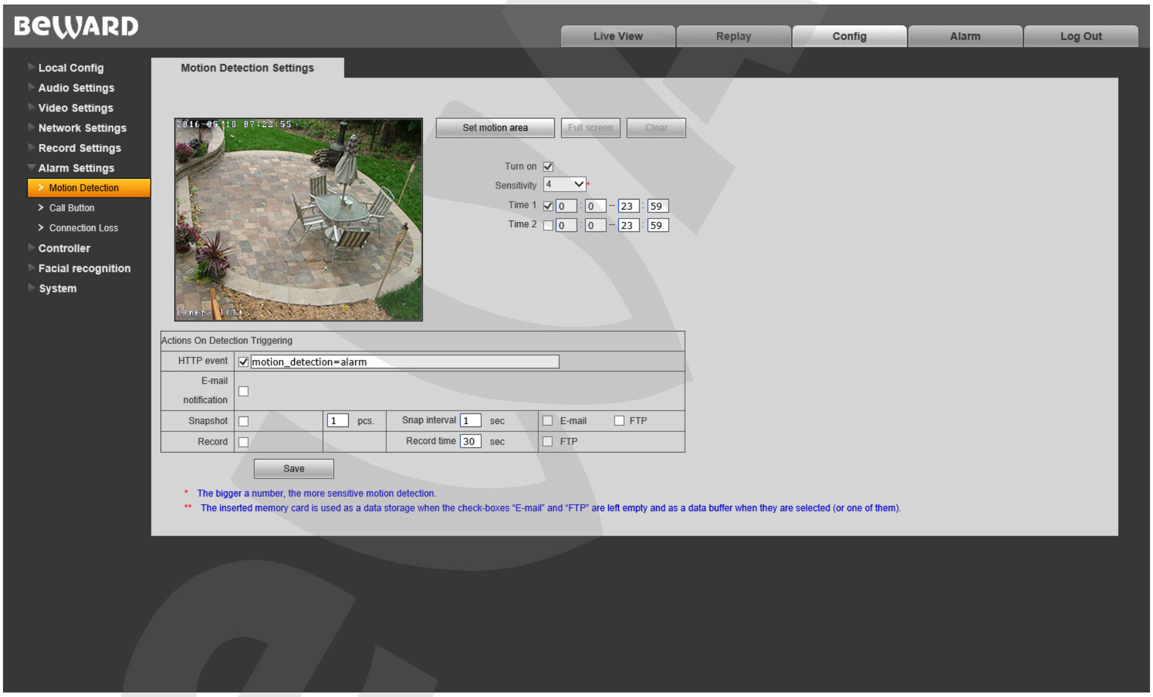
Additional body: Additional information added to the body of the notification. It can be used for adding program code to send messages in online chats, blogs etc.

[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 examples

1) When motion detection is activated (see paragraph 10.1):



Turn on ☑
Sensitivity 4 *
Time 1 ☑ 0 : 0 -- 23 : 59
Time 2 □ 0 : 0 -- 23 : 59

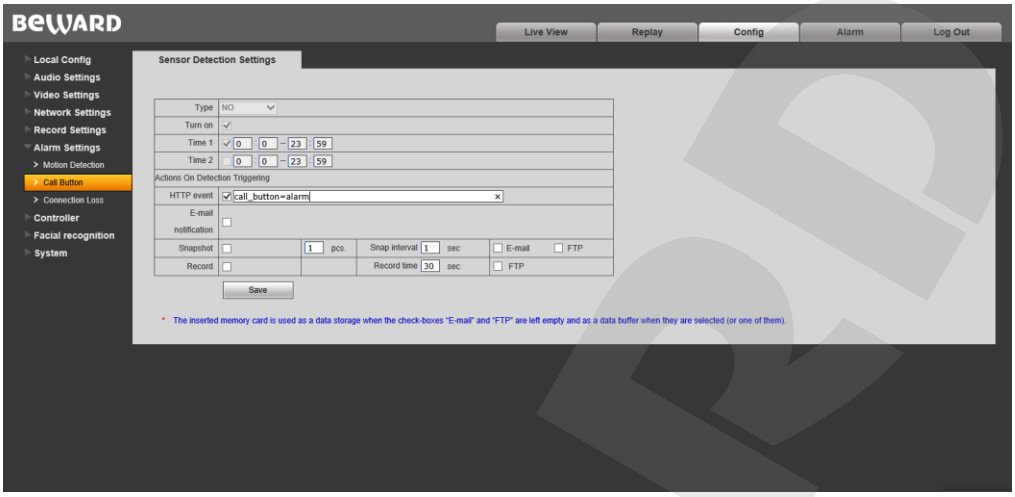
Actions On Detection Triggering				
HTTP event	☑ motion_detection=alarm			
E-mail notification	□			
Snapshot	□	1 pcs.	Snap interval 1 sec	□ E-mail □ FTP
Record	□		Record time 30 sec	□ FTP

* The bigger a number, the more sensitive motion detection.

** The inserted memory card is used as a data storage when the check-boxes "E-mail" and "FTP" are left empty and as a data buffer when they are selected (or one of them).

Pic. 8.17

2) When the “Call” button is pressed (see paragraph 10.2):



Type	NO			
Turn on	☑			
Time 1	☑ 0 : 0 – 23 : 59			
Time 2	□ 0 : 0 – 23 : 59			
Actions On Detection Triggering				
HTTP event	☑ call_button=alarm			
E-mail notification	□			
Snapshot	□	1 pcs.	Snap interval 1 sec	□ E-mail □ FTP
Record	□		Record time 30 sec	□ FTP

* The inserted memory card is used as a data storage when the check-boxes "E-mail" and "FTP" are left empty and as a data buffer when they are selected (or one of them).

Pic. 8.18

In both cases you must 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. *8.16)* 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

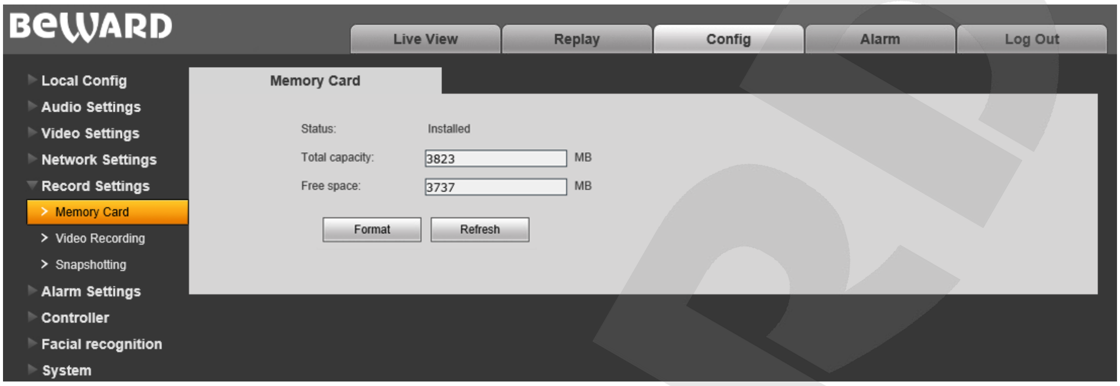
A HTTP request without additional parameters is made as follows:

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

Chapter 9. Config: Record Settings

9.1. Memory Card

The **"Memory Card"** settings menu is shown below:



Status: Installed

Total capacity: 3823 MB

Free space: 3737 MB

Pic. 9.1

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

[Format]: Start formatting the memory card.

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

ATTENTION!

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

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

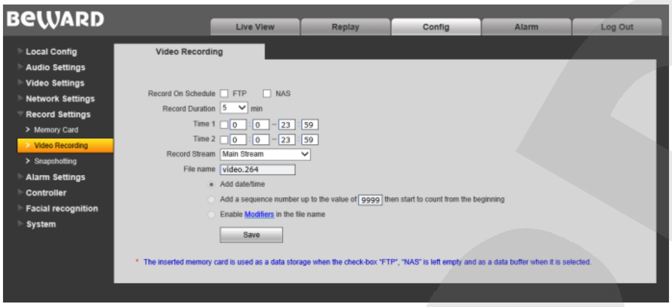
The device does not support memory cards with several partitions after formatting.

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

9.2. Video Recording

The **“Video Recording”** settings menu is shown below:



Video Recording

Record On Schedule □ FTP □ NAS

Record Duration 5 min

Time 1 □ 0 : 0 -- 23 : 59

Time 2 □ 0 : 0 -- 23 : 59

Record Stream Main Stream

File name video.264

● Add date/time

○ Add a sequence number up to the value of 9999 then start to count from the beginning

○ Enable Modifiers in the file name

* The inserted memory card is used as a data storage when the check-box “FTP”, “NAS” is left empty and as a data buffer when it is selected.

Pic. 9.2

Record on Schedule: Enable scheduled video recording to the FTP and/or NAS server. FTP server parameters can be set in the **«FTP»** menu (see paragraph 8.8). NAS storage parameters can be set in the **«NAS»** menu (see paragraph 8.9). When transferring files to FTP/NAS server, an event suffix is added the filenames.

Suffix	Description	Example
MD	Motion detector	image_MD.jpeg
P	Periodic event	video_P.jpeg
I	Alarm input	video_I.jpeg

NOTE:

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

Record Duration: set the duration for video files. Available values: 1~60 min.

ATTENTION!

The memory card installed by default also used for caching files when recording them to the FTP server. The duration of video clips does not depend on the size of the inner buffer of the door station.

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

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

Stream type: choose between the main or sub streams used for recording.

NOTE:

«Stream Type» also applies to video recording on alarm.

File name: enter the name for the recorded files.

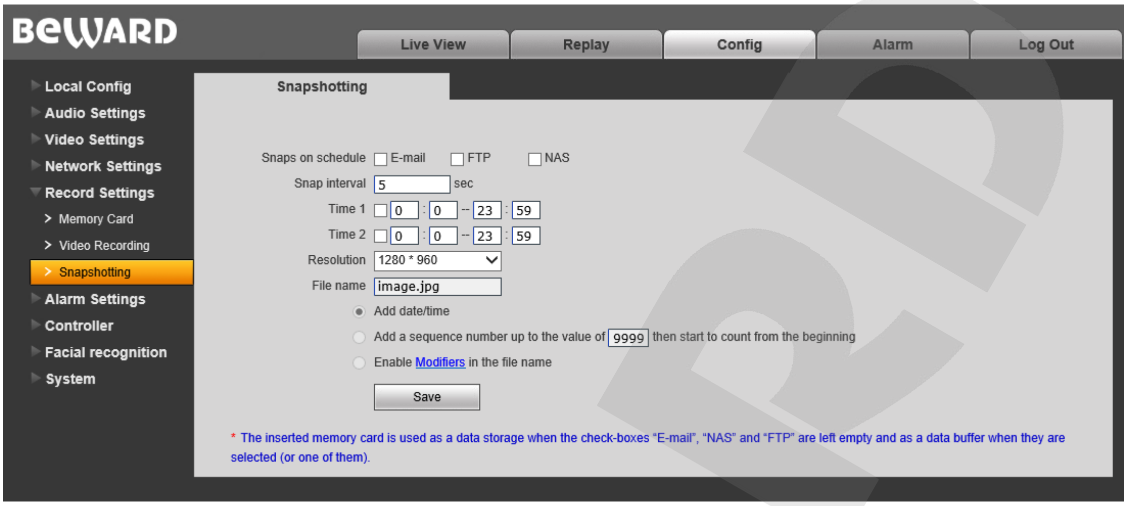
Also, you may use one of the following options

- **Add time/date** – adds a date/time stamp to the filename, regardless of the event type (continuous recording or alarm recording)
- **Add sequence numbers up to the value of **** then start the count from the beginning** – enter the highest number of files that can be recorded before overwriting., This option works regardless of the event type (continuous recording or alarm recording)
- **Enable modificators in the filename** – adds various modifiers to the filename. Too see the full list of available modifiers, please click the "modificators" hyperlink. The modifiers can be applied to all types of videos, regardless of the event type (continuous recording or alarm recording).

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

9.3. Snapshotting

The **“Snapshotting”** settings menu is shown below:



Snaps on schedule □ E-mail □ FTP □ NAS

Snap interval 5 sec

Time 1 □ 0 : 0 -- 23 : 59

Time 2 □ 0 : 0 -- 23 : 59

Resolution 1280 * 960

File name image.jpg

● Add date/time

○ Add a sequence number up to the value of 9999 then start to count from the beginning

○ Enable Modifiers in the file name

* The inserted memory card is used as a data storage when the check-boxes “E-mail”, “NAS” and “FTP” are left empty and as a data buffer when they are selected (or one of them).

Pic. 9.3

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

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 8.7**),** FTP-client parameters can be set in the **«FTP»** menu (see paragraph 8.8), NAS parameters can be set in the **«NAS»** menu (see paragraph 8.9). When transferring files to FTP/NAS server, an event suffix is added the filenames.

Suffix	Description	Example
MD	Motion detector	image_MD.jpeg
P	Periodic event	video_P.jpeg
I	Alarm input	video_I.jpeg

NOTE:

If **«FTP»** and/or **«NAS», «E-mail»** options are disabled the snapshots will be stored in the memory card,

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

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

ATTENTION!

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

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

Resolution: select resolution for snapshots

> **NOTE:**
> «Resolution» also applies to snapshotting on alarm.

File name: enter the name for the recorded files.

Also, you may use one of the following options

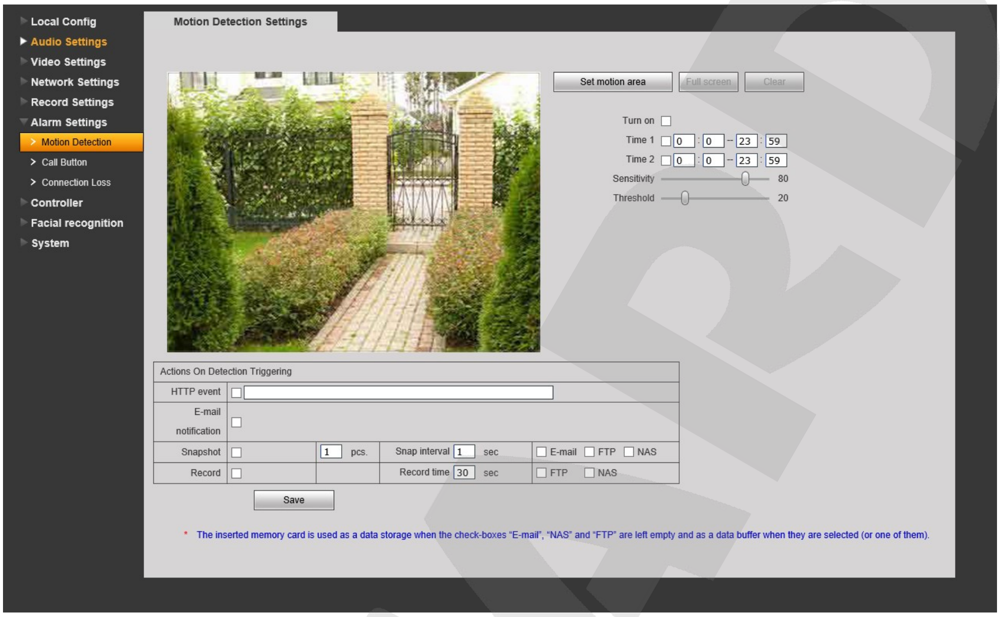
- **Add time/date** – adds a date/time stamp to the filename, regardless of the event type (continuous recording or alarm recording)
- **Add sequence numbers up to the value of **** then start the count from the beginning** – enter the highest number of files that can be recorded before overwriting., This option works regardless of the event type (continuous recording or alarm recording)
- **Enable modificators in the filename** – adds various modifiers to the filename. Too see the full list of available modifiers, please click the "modificators" hyperlink. The modifiers can be applied to all types of snapshots, regardless of the event type (continuous recording or alarm recording).

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

Chapter 10. Config: Alarm Settings

10.1. Motion Detection Settings

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



Turn on □

Time 1 □ 0 : 0 -- 23 : 59

Time 2 □ 0 : 0 -- 23 : 59

Sensitivity 80

Threshold 20

Actions On Detection Triggering				
HTTP event	□			
E-mail notification	□			
Snapshot	□	1 pcs.	Snap interval 1 sec	□ E-mail □ FTP □ NAS
Record	□		Record time 30 sec	□ FTP □ NAS

* The inserted memory card is used as a data storage when the check-boxes “E-mail”, “NAS” and “FTP” are left empty and as a data buffer when they are selected (or one of them).

Pic. 10.1

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

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

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

[Clear]: clear all motion detection areas.

Enable: enable/ disable the motion detection function.

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

Sensitivity: Set the relative level of sensitivity of the motion detector. The sensitivity based on the speed and contrast of the moving object in relation to the background. If the value is high, the motion detection alarm will be triggered even by slow-moving, low-contrast objects.

Threshold: Set the size threshold for the moving object. If the value is high, the motion detection alarm will be triggered only by bigger objects.

> **NOTE:**
> If the Sensitivity is set too high and the Threshold is set too low, false alarms may occur. The parameters must be calibrated individually according to the user’s needs.

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 (See paragraph 8.13 for further details).

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 / NAS: Set E-mail and/or FTP/NAS server as destinations for snapshots. If none are 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.

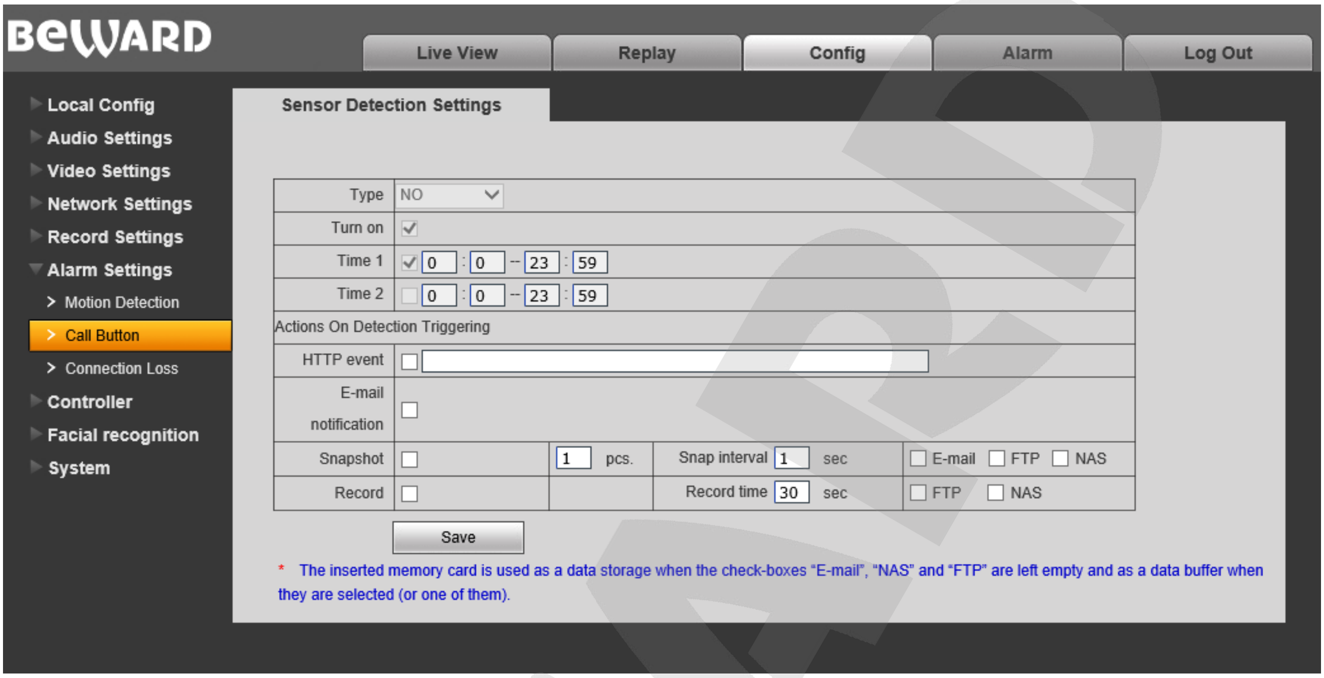
FTP: Set the FTP server as a destination for recorded video files. If disabled, the memory card will be used instead.

> **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

10.2. Call Button

The “**Call Button**” settings menu is shown below:



Type	NO			
Turn on	☑			
Time 1	☑ 0 : 0 -- 23 : 59			
Time 2	□ 0 : 0 -- 23 : 59			
Actions On Detection Triggering				
HTTP event	□			
E-mail notification	□			
Snapshot	□	1 pcs.	Snap interval 1 sec	□ E-mail □ FTP □ NAS
Record	□		Record time 30 sec	□ FTP □ NAS

Save

* The inserted memory card is used as a data storage when the check-boxes “E-mail”, “NAS” and “FTP” are left empty and as a data buffer when they are selected (or one of them).

Pic. 10.2

This option is always enabled by default, so the **“Enable”** and **“Time 1/2”** checkboxes are not available.

HTTP event: If enabled, pressing the call button of the door station will trigger the sending of parameters to the HTTP/HTTPS server (see paragraph 8.16 for further details).

E-mail notification: Send an e-mail notification when the call button is pressed.

Snapshot: Make snapshots when the call button is pressed. You can set the number of snapshots in the field to the right

Snap interval: Set the time interval between snapshots.

E-mail / FTP / NAS: Set E-mail and/or FTP, NAS 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 NAS, FTP server or E-Mail, so you can find the files on the memory card

Record: enable/ disable video recording when the call button is pressed.

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!

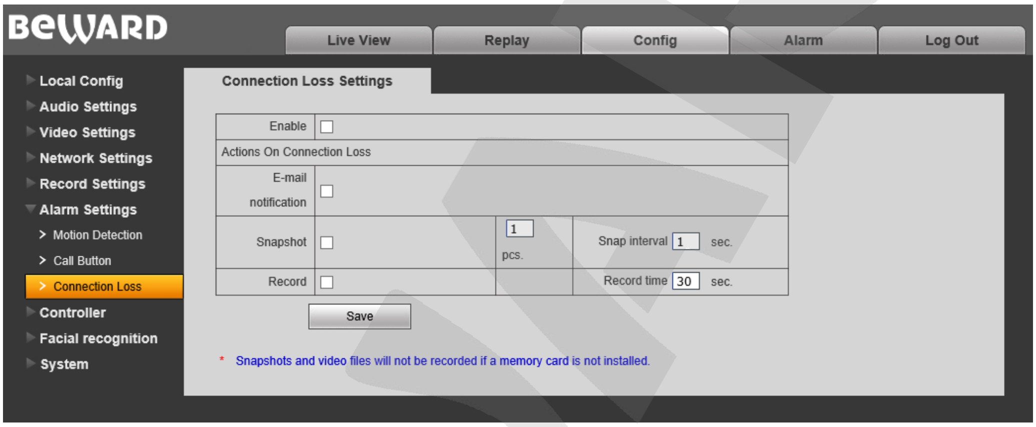
The default memory card is also used for caching files when sending them to FTP server. The duration of video files is not limited by the size of the inner buffer of the door station

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

10.3. Connection Loss

The “**Connection Loss**” settings menu is shown below:



Connection Loss Settings

Enable	☐		
Actions On Connection Loss			
E-mail notification	☐		
Snapshot	☐	1 pcs.	Snap interval 1 sec.
Record	☐		Record time 30 sec.

Save

* Snapshots and video files will not be recorded if a memory card is not installed.

Pic. 10.3

Here you can set different actions which can be performed in case of connection loss.

Enable: Enable/ disable recording of snapshots and videos in case of connection loss.

E-mail notification: Enable E-mail notifications on connection loss. Notifications are sent right after the connection issues are solved.

Snapshot: Make snapshots in case of connection loss. Set the number of snapshots in the field to the right

Snapshot interval: Set the time interval between snapshots.

Record: Activate video recording in case of connection loss.

Record time: Set the duration for recorded video files.

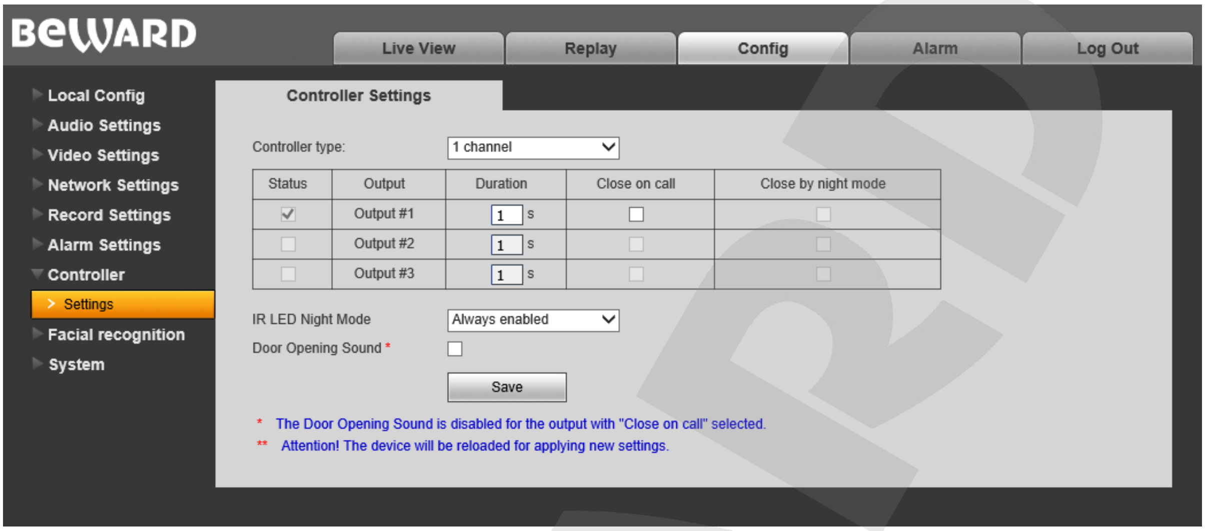
NOTE:

In case of connection loss snapshots and video files can only be recorded if the memory card is installed!

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

Chapter 11. Config: Controller

The “**Controller**” settings menu is shown below:



Controller Settings

Controller type: 1 channel

Status	Output	Duration	Close on call	Close by night mode
☑	Output #1	1 s	☐	☐
☐	Output #2	1 s	☐	☐
☐	Output #3	1 s	☐	☐

IR LED Night Mode: Always enabled

Door Opening Sound * ☐

Save

* The Door Opening Sound is disabled for the output with "Close on call" selected.

** Attention! The device will be reloaded for applying new settings.

Pic. 11.1

The package contents may include a 1-channel (NC103 / NC103P) or a 3-channel controller (NC311P), depending on the purchased model of the door station.

Various types of devices can be connected to the door station. These may include: doors/door locks, garage openers, light switches, alarm systems etc. 1-channel controllers support one device, while 3-channel devices support up to 3 devices.

3-channel controllers allow operating 3 different door locks via a single door station. For example, you can open the gates, the garage door and the front door.

Controller type: Choose between «1 channel» and «NC311P». selecting «NC311P» will enable the additional «Controller connection» option. (See below).

Duration: Set the duration for the closed/open status of controller outputs (depending on the type of the lock and its controller).

For the NC311P controller type, if the duration value is “0”, the controller outputs stay open until receiving a closing command from the user. If the duration value is in the range from 0.1 to 3600 seconds, the controller outputs will open and close in specified time.

Close on call: Set closing relay output contacts when the call button is pressed if necessary (for example, when connection a door bell).

Facial recognition: This option appears when the “Facial recognition” function is enabled (see chapter 12). The door opens if a face is successfully recognized.

Night Mode IR LED: IR LED has 2 operating modes – «Always enabled» and «On request». The «On request» mode is active by default.

In the «On request» mode IR LED activates when the call button is pressed or when receiving the video stream via program client (PC applications or web browser)

In the «Always enabled» mode the door station automatically switches between Day/Night modes on sensor without additional external actions.

The «On request» mode is preferable: it increases LED operating time and hides the door station from prying eyes during nighttime.

Door Opening Sound: The door station speaker plays sound signals when opening the door via BEWARD Intercom and Beward IP Visor software.

> **NOTE:**
> The “Door Opening Sound” function does not work together with the “Close on call” option for the selected relay output.
> The “Door Opening Sound” function does not work when opening the door via the SIP connection (sound cannot be played when the SIP channel is open)

> **ATTENTION!**
> Using the “On Request” mode and the motion detection function simultaneously at nighttime leads to malfunctions and must be avoided.

Controller connection: (NC311P controller type only) press the **[Connect]** button to set interactions between the controller and the door station.

> **ATTENTION!**
> When connecting the NC311P controller (included in DS06AP-3L package contents) for the first time (or when replacing it with another NC311P controller), it is obligatory to set interaction between the controller and the door station. Otherwise, you will not be able to operate the controller.

Press the **“LINK”** button on the controller (refer to the Installation Manual for details) and press the **[Connect]** button. The interaction process will take about 1 minute. Do not turn off or restart the door station during the interaction process.

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

Chapter 12. Config: Facial Recognition

Facial recognition is a function of automatic access control which allows, without using any additional equipment, a specified group of visitors to enter a building. The function can operate independently, without connecting the door station to the Internet.

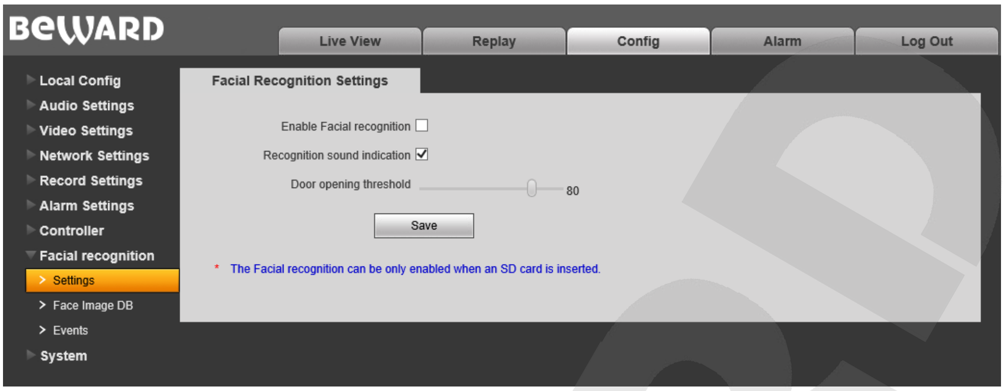
NOTE:
Facial recognition is only available for DS06A, DS06A and DS06AP (firmware version - **3.1.0.0.6.18**)

By default, the facial recognition is initiated when a visitor pushes and holds (during 1 second) the call button of the door station. In the process of analyzing visitor’s face the door station emits a sound during the one a visitor should stand still and look into the lens of the door station camera. In case of recognition the door station emits a short sound signal and opens the door. In case a visitor is not added to the face image database or the door station is not recognized him, it emits two short signals.

ATTENTION!
The facial recognition algorithm works when a face is 0.5 meter away from the door station or closer.

NOTE:
As an infrared filter is used to improve facial recognition results at any time of the day or night, a video image from the door station becomes black and white in short periods
The number of simultaneous connections (users) to the door station affects the face recognition time. Having more than 4 simultaneous connections is not recommended.

12.1 Settings



Facial Recognition Settings

Enable Facial recognition □

Recognition sound indication ☑

Door opening threshold 80

* The Facial recognition can be only enabled when an SD card is inserted.

Pic. 12.1

Enable Facial recognition: Enable the facial recognition function.

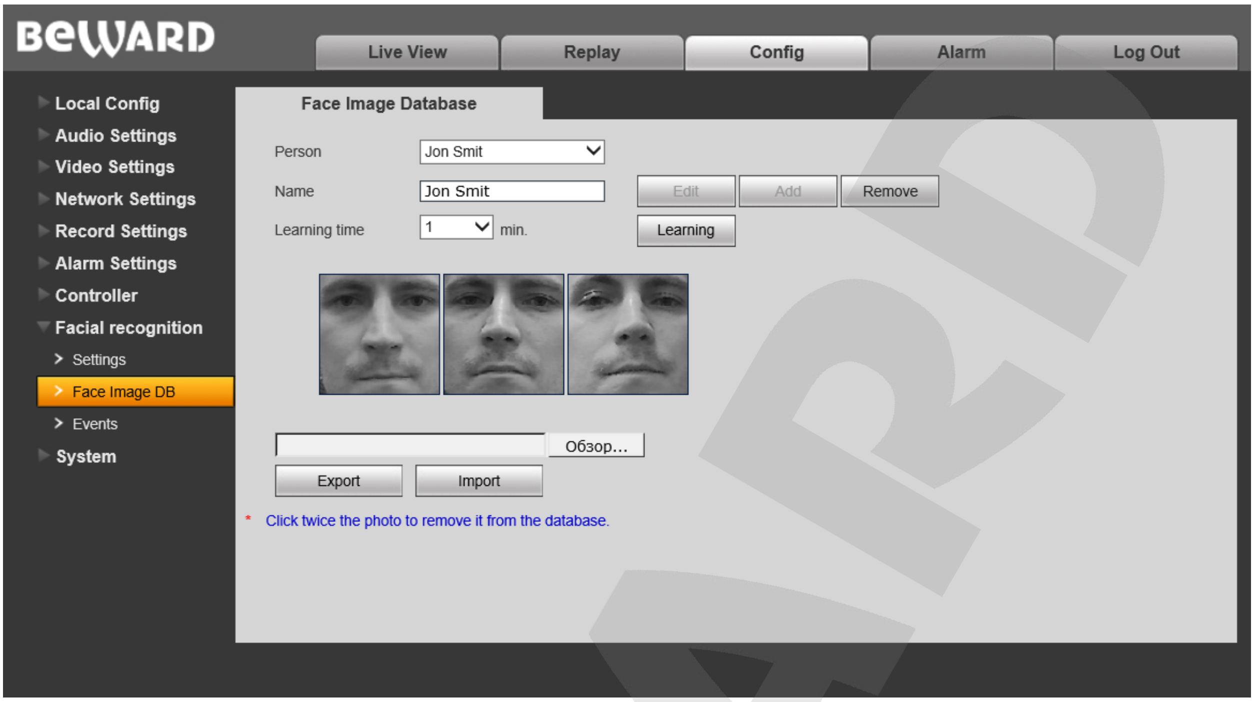
> **NOTE:**
> *The function is only available on the DS06A door stations with an SD card inserted.*

Recognition sound indication: Enable emitting sound signals (recognized/unrecognized, face analysis) by the door station.

Door opening threshold: This option allows you to set a specific recognition threshold; when it is reached the door station opens the door. The bigger a threshold value, the higher a security level, but then there are also higher requirements to the match of visitor’s face real-time image and the one from the database. Reducing the threshold value leads to better recognition results but may cause recognition errors and opening the door to unknown persons.

> **ATTENTION!**
> Opening the door by facial recognition can’t be used for buildings with an increased security level! Recognition errors (their frequency depends on the threshold value) and opening the door to unknown persons is possible
> The following conditions may influence the correctness of facial recognition operation):
> - A back light of the sun or other light sources
> - Clothes and accessories (such as glasses, kerchiefs, masks etc.) that can conceal the face partially or completely.
> - Light-reflecting and light-absorbing paints (make-up) on visitor’s face.

12.2 Face Image Database



Person: Jon Smit

Name: Jon Smit

Learning time: 1 min.

* Click twice the photo to remove it from the database.

Pic. 12.2

Face image database contains a list of visitors which are allowed to enter the building, passing the facial recognition procedure.

> **NOTE:**
> *Face image database can contain up to 30 images. Up to 5 images per one visitor are available.*

Person: Adrop-down list of visitors added to the door station database.

After choosing a particular person you can edit his name and face images which are used for the facial recognition.

Name: Visitor's name and surname.

Edit: This button allows you to change visitor's name.

Add: Click this button to add a new person to the database.

Remove: Click this button to remove visitor's data (including the face images) from the database.

Learning: Activate Learning mode which is used for adding face images for the current person. When the mode is activated, the door station starts periodically emitting short sound signals. To allow the camera to capture a face, a visitor should stand before the door station and push the call button. When a face is captured successfully the door station emits one short sound signal; in case a face is captured not successfully the door station emits two short sound signals. Duration of the Learning mode is specified in the **Learning time** field.

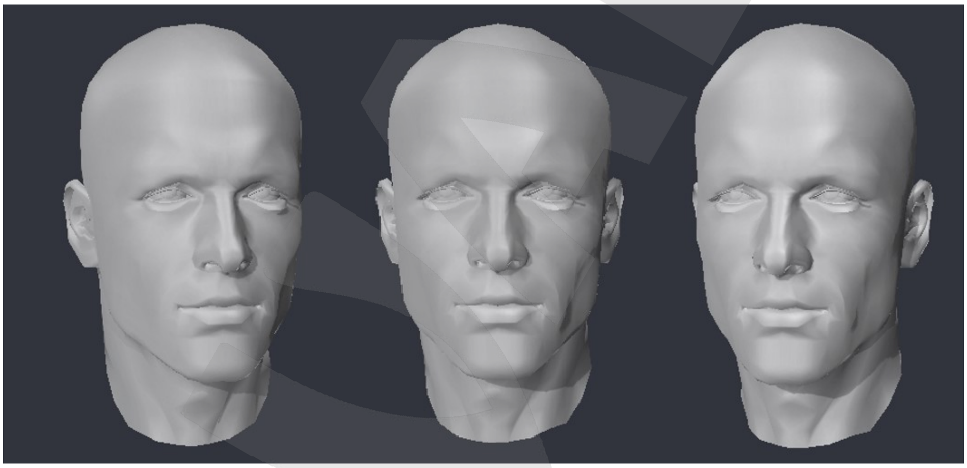
Face images area: Face images of the chosen person are situated in this area.

You can click the image twice to remove it from the database.

Export and **Import** buttons are used to transfer the database from one door station to another.

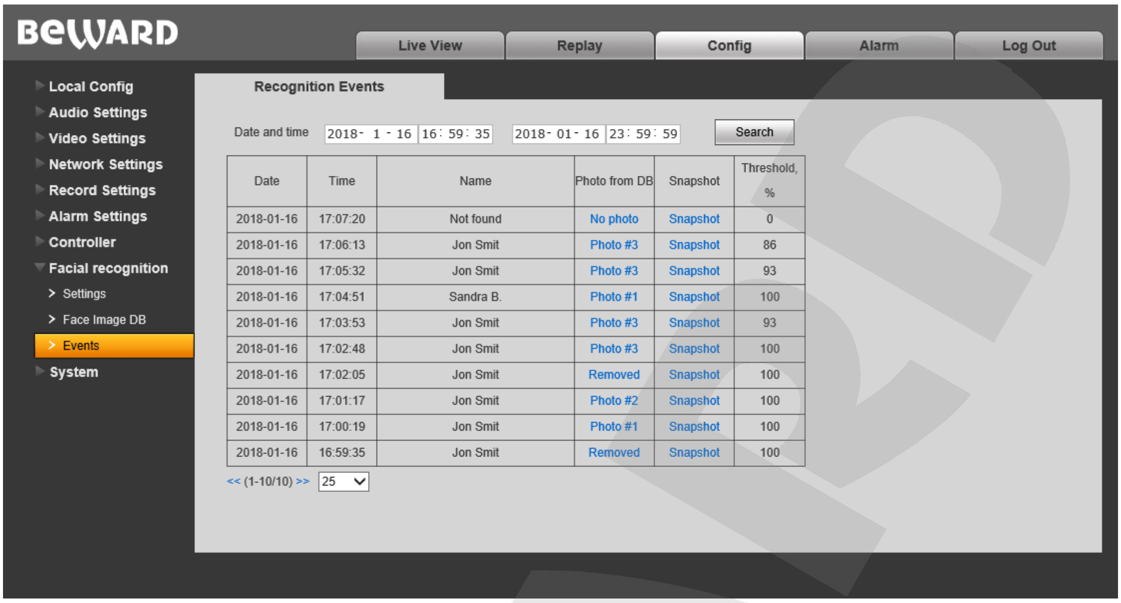
Recommendations on filling up the Face image database:

- *Create and set the database on the door station installed on the wall. Do not change the position of the door station after the facial recognition function is set!*
- *Stand before the door station in a way you can easily push the call button.*
- *Stand still and look directly into the lens of the door station camera while it captures your face until you will hear the sound signal.*
- *Make 2-3 images with different positions of the face (see the picture below).*



Pic. 12.3

12.3 Events



Date and time 2018- 1 - 16 16: 59: 35 2018- 01 - 16 23: 59: 59

Date	Time	Name	Photo from DB	Snapshot	Threshold, %
2018-01-16	17:07:20	Not found	No photo	Snapshot	0
2018-01-16	17:06:13	Jon Smit	Photo #3	Snapshot	86
2018-01-16	17:05:32	Jon Smit	Photo #3	Snapshot	93
2018-01-16	17:04:51	Sandra B.	Photo #1	Snapshot	100
2018-01-16	17:03:53	Jon Smit	Photo #3	Snapshot	93
2018-01-16	17:02:48	Jon Smit	Photo #3	Snapshot	100
2018-01-16	17:02:05	Jon Smit	Removed	Snapshot	100
2018-01-16	17:01:17	Jon Smit	Photo #2	Snapshot	100
2018-01-16	17:00:19	Jon Smit	Photo #1	Snapshot	100
2018-01-16	16:59:35	Jon Smit	Removed	Snapshot	100

<< (1-10/10) >> 25

Pic. 12.4

Events: This tab contains a log of facial recognition events when the function is enabled. The events are situated in the table which is divided to several columns:

Date and **Time**: Date and time of an event.

Name: Visitor’s name in the database.

Photo from DB: Visitor’s face image from the database used for the matching procedure.

Snapshot: Visitor’s face real-time image.

Threshold, %: Shows how much the face from the captured image matches the face from the database.

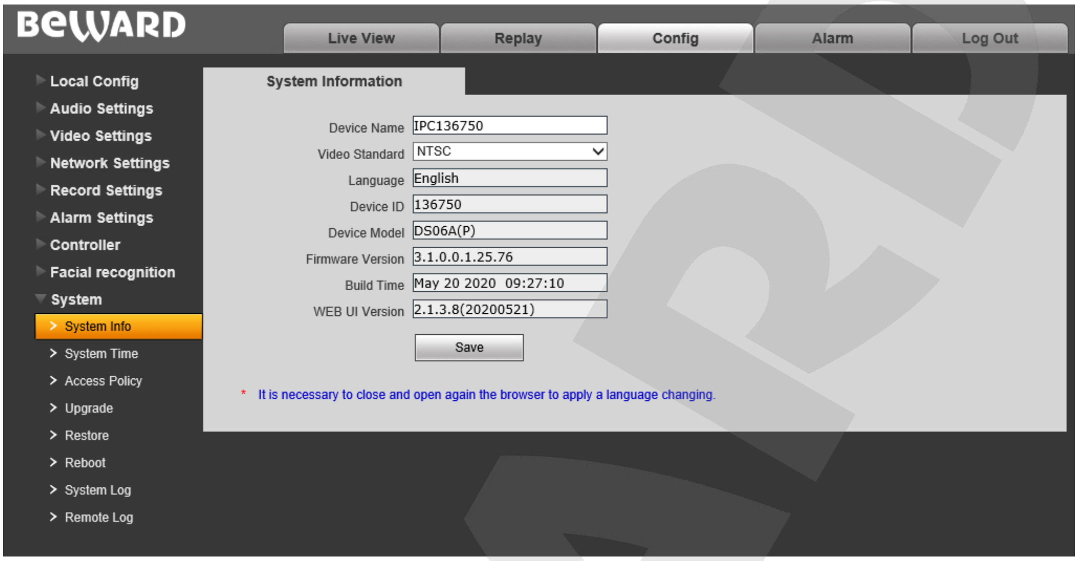
NOTE:

If some face image is removed from the database, then it is marked as “Removed” in the event list. If no images are found in the database to be matched with the currently captured face image, then the visitor is marked as ”Not found”.

Chapter 13. Config: System

13.1. System Info

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



Device Name IPC136750

Video Standard NTSC

Language English

Device ID 136750

Device Model DS06A(P)

Firmware Version 3.1.0.0.1.25.76

Build Time May 20 2020 09:27:10

WEB UI Version 2.1.3.8(20200521)

* 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.

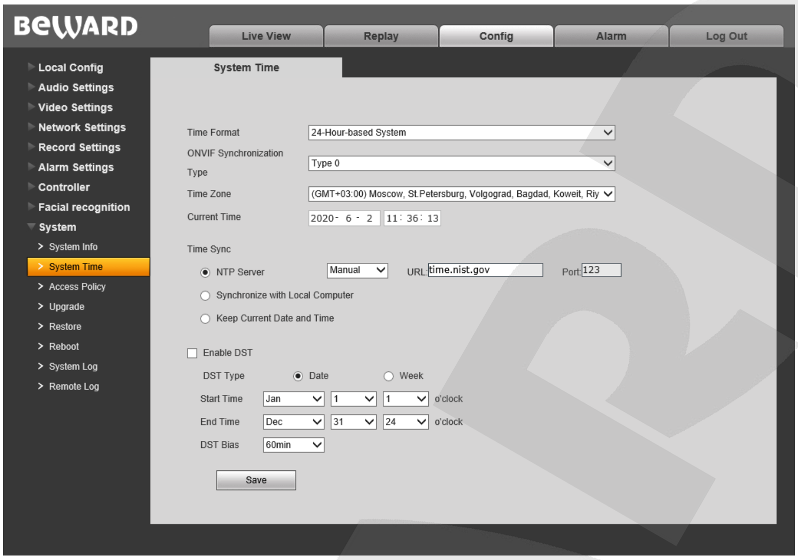
Build Date: The date when the firmware was built.

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:



System Time

Time Format: 24-Hour-based System

ONVIF Synchronization Type: Type 0

Time Zone: (GMT+03:00) Moscow, St.Petersburg, Volgograd, Bagdad, Koweit, Riy

Current Time: 2020- 6 - 2 11: 36: 13

Time Sync

● NTP Server Manual URL: time.nist.gov Port: 123

○ Synchronize with Local Computer

○ Keep Current Date and Time

□ Enable DST

DST Type ● Date ○ Week

Start Time Jan 1 1 o'clock

End Time Dec 31 24 o'clock

DST Bias 60min

Pic. 13.2

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

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

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

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

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

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

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

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

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

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

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

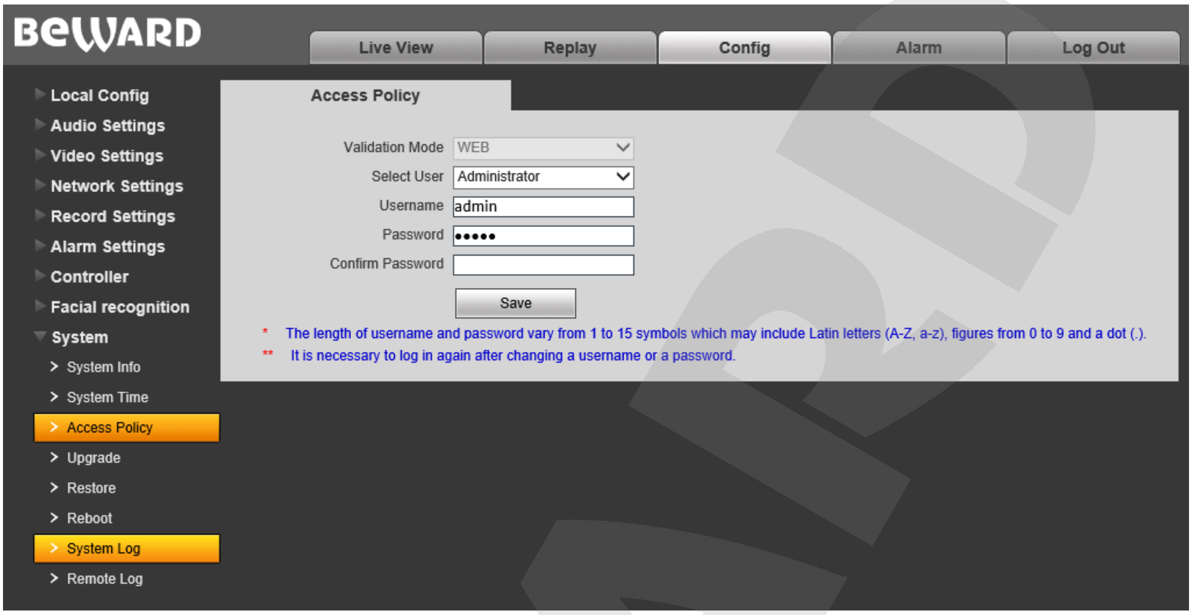
Start / End Time: Set the time of advancing and backward adjusting.

DST Bias: Set a size of the time shift.

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

13.3. Access Policy

The **«Access Policy»** settings menu is shown below:



Validation Mode: WEB
Select User: Administrator
Username: admin
Password: •••••
Confirm Password:

* 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 (.).

** It is necessary to log in again after changing a username or a password.

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”**.

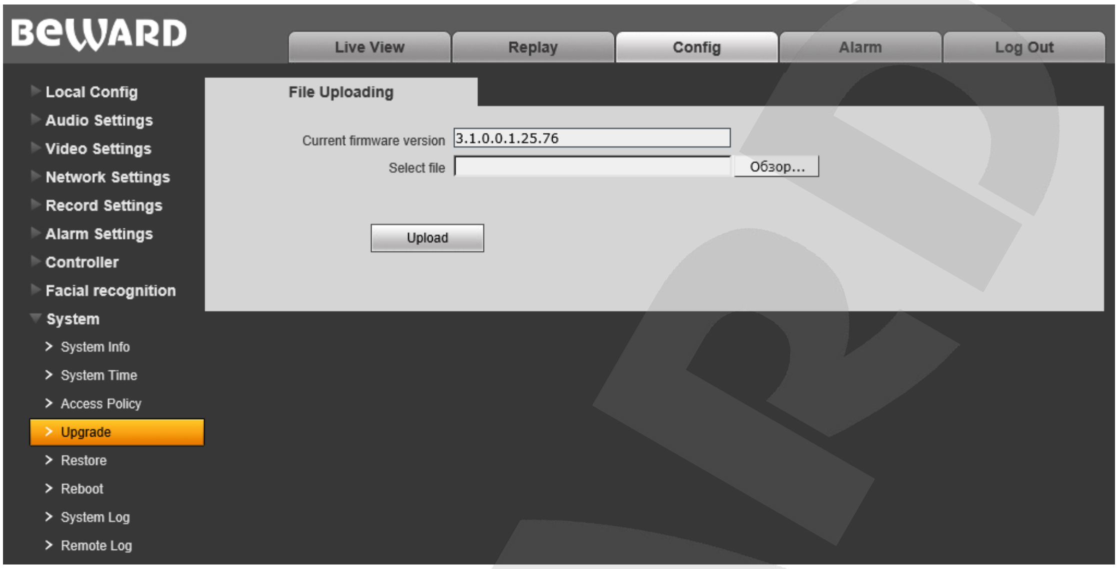
Press the **[Save]** button to apply new settings.

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 **“File Uploading”** menu is shown below:



File Uploading

Current firmware version 3.1.0.0.1.25.76

Select file

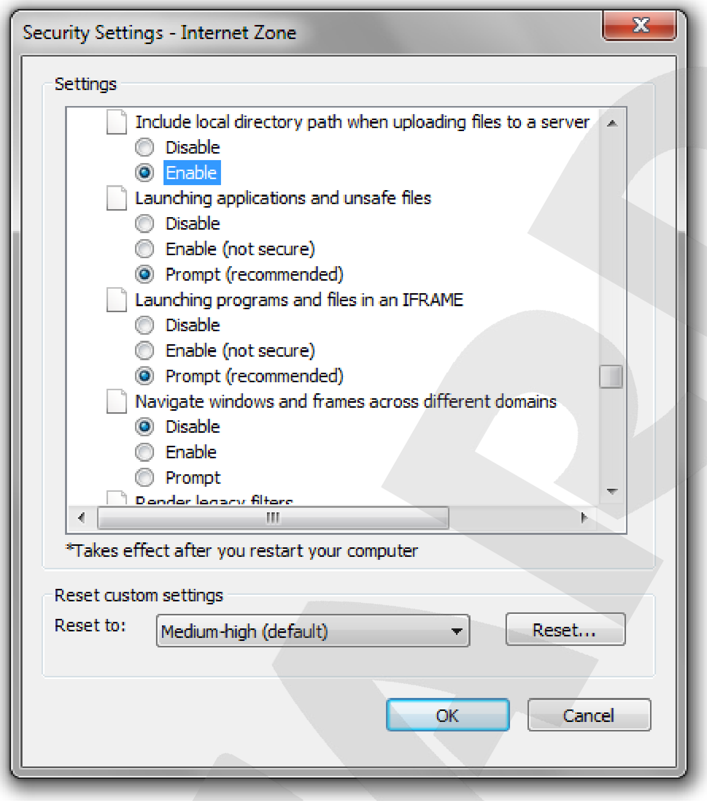
Pic. 13.4

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

1. Press the **[Browse]** button. Choose the appropriate file in the opened File Explorer window and press the **[Open]** button.
2. Press the **[Upload]** button to start upgrading. The 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*).



Security Settings - Internet Zone

Settings

Include local directory path when uploading files to a server
- ○ Disable
- ● Enable

Launching applications and unsafe files
- ○ Disable
- ○ Enable (not secure)
- ● Prompt (recommended)

Launching programs and files in an IFRAME
- ○ Disable
- ○ Enable (not secure)
- ● Prompt (recommended)

Navigate windows and frames across different domains
- ● Disable
- ○ Enable
- ○ Prompt

Render legacy filters

*Takes effect after you restart your computer

Reset custom settings

Reset to: Medium-high (default)

Pic. 13.5

3. Set door station parameters by default (see paragraph 13.5).

ATTENTION!

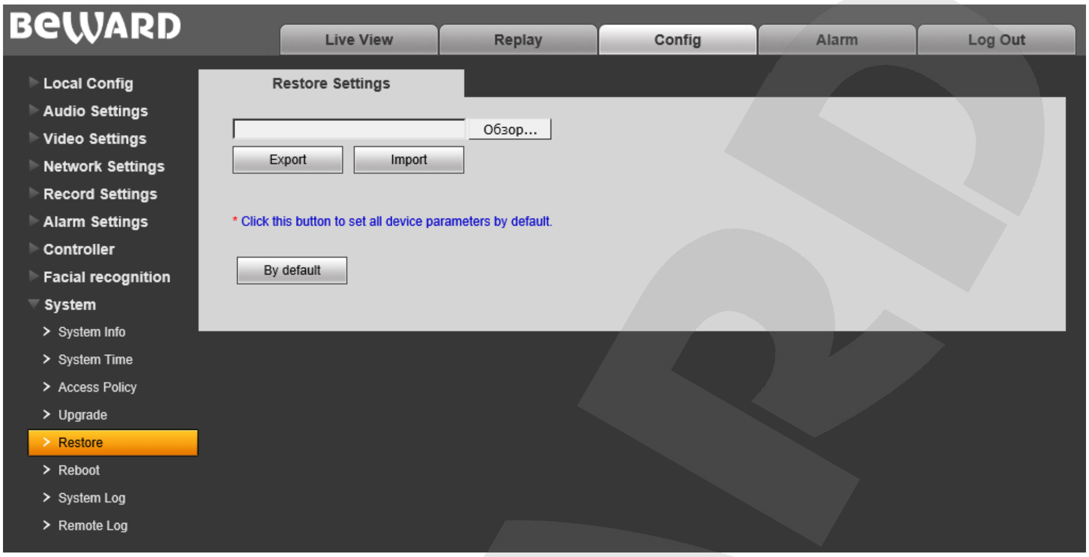
Use only appropriate firmware files which are compatible with the device model! The device may operate incorrectly and be damaged in case of using an unsuitable firmware file.

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

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

13.5. Restore

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



* Click this button to set all device parameters by default.

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).

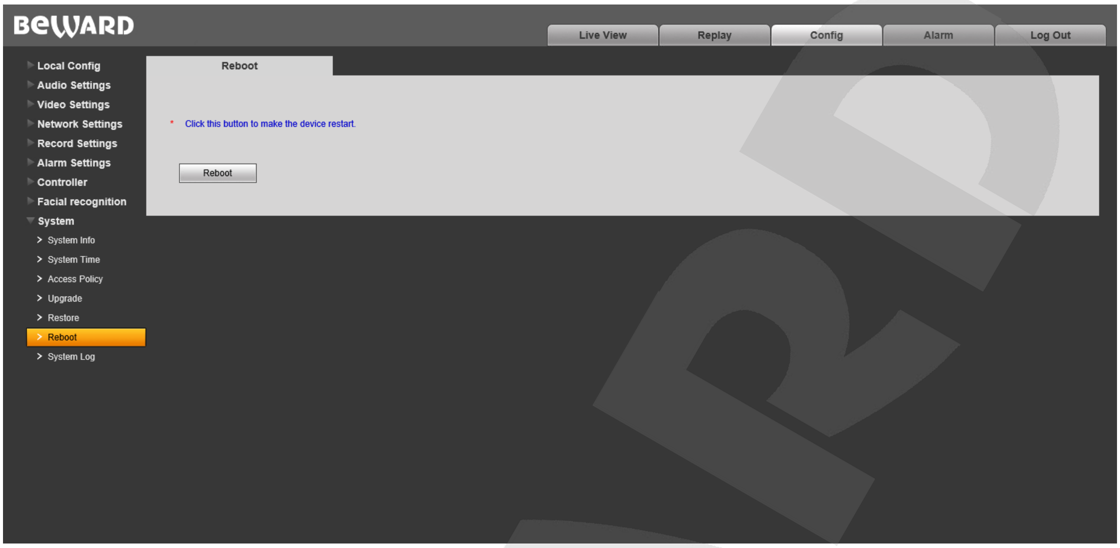
[Import]: Click to reset the settings from the **".bak"** file. Click **[Browse]**, choose the file and click **[Import]**. After restoring the settings, the device will be rebooted.

[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.

13.6. Reboot

The **“Reboot”** menu is shown below:



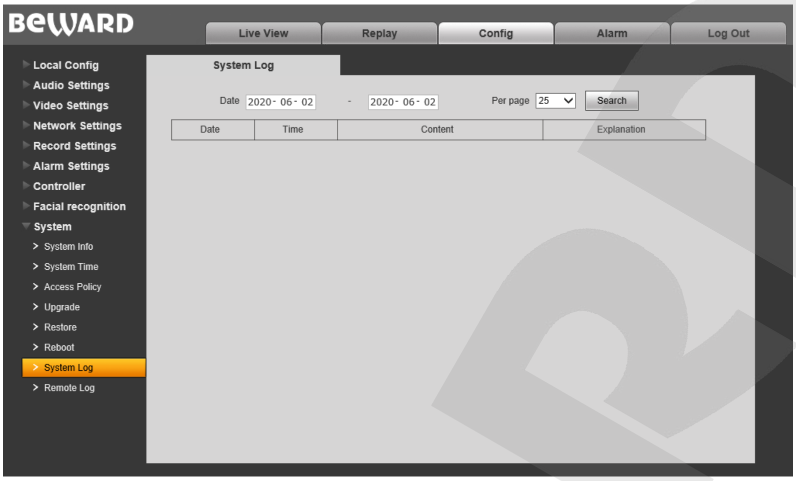
* Click this button to make the device restart.

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:



Date 2020- 06- 02 - 2020- 06- 02 Per page 25

Date	Time	Content	Explanation

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.

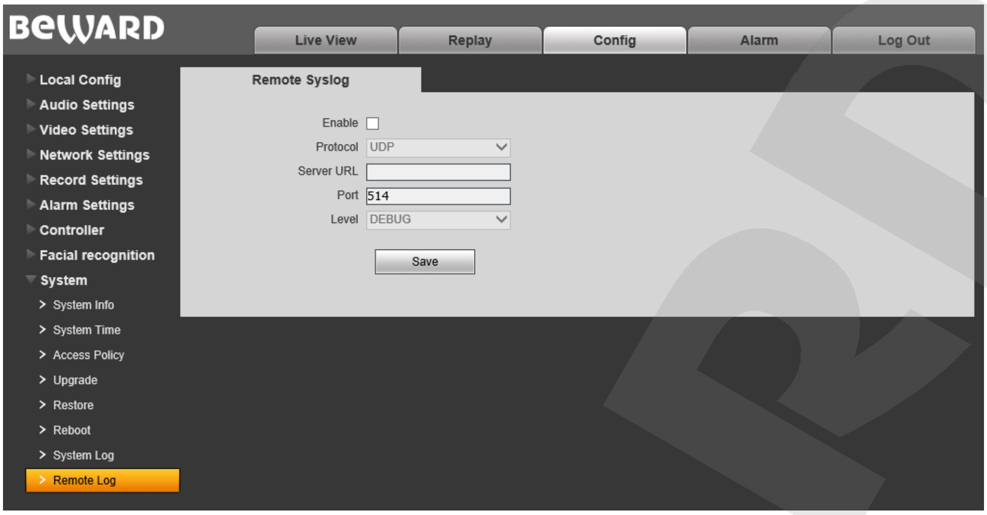
Date: Specify the necessary search period.

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

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

13.8 Remote log

The **Remote log menu** is shown below**:**



Enable □

Protocol UDP

Server URL

Port 514

Level DEBUG

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.

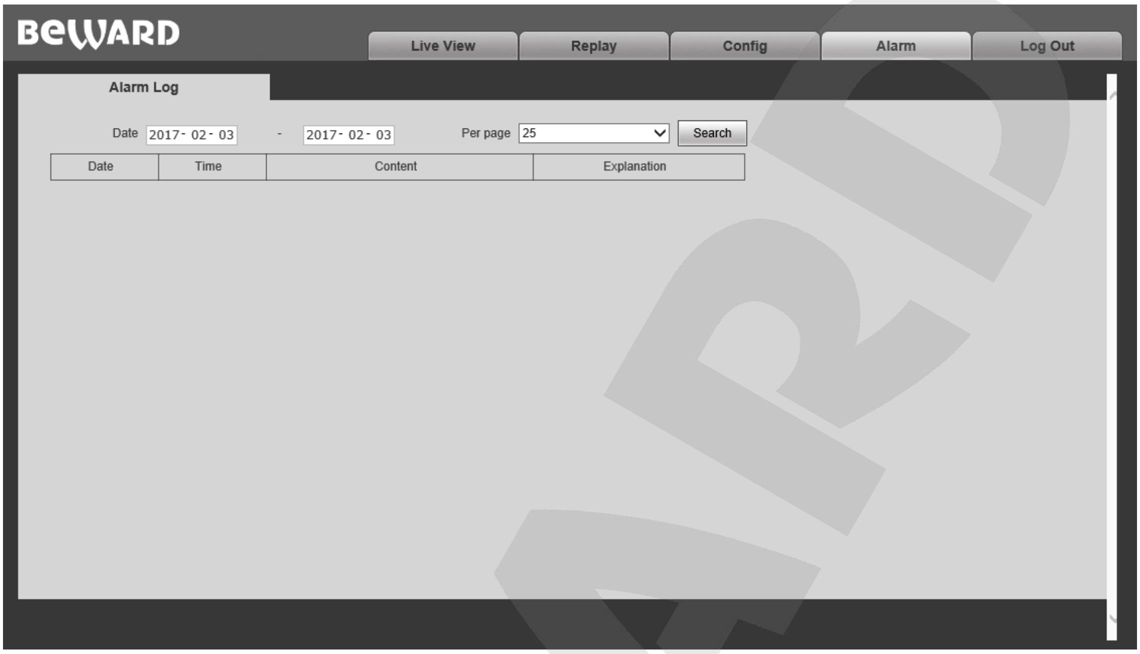
Level: Specify the urgency level of event messages.

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

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

Chapter 14. Alarm

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



Date 2017- 02- 03 - 2017- 02- 03 Per page 25

Date	Time	Content	Explanation

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 DS06A(P)

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. Acoustic 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

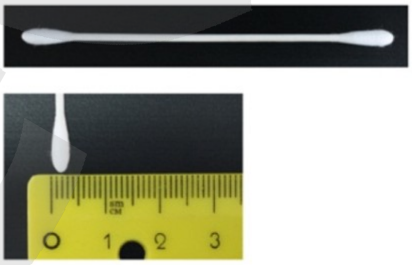
Appendix A. Factory Defaults

You can see some of the factory default parameters below.

Parameter	Value
IP address	**192.168.0.99**
Subnet mask	**255.255.255.0**
Gateway	**192.168.0.1**
Username (administrator)	**admin**
Password (administrator)	**admin**
HTTP port	**80**
Data port	**5000**
RTSP port	**554**
ONVIF port	**2000**
NTP-server	**time.nist.gov** **time.windows.com** **time-nw.nist.gov** **time-a.nist.gov** **time-b.nist.gov**

Appendix B. Maintenance

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



Pic. B1

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

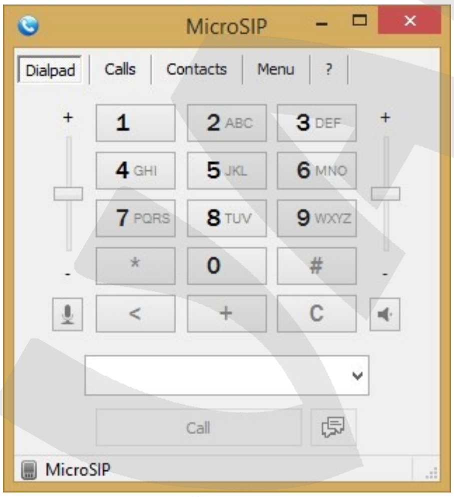
Appendix C. SIP settings example

C1. 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. C1

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

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

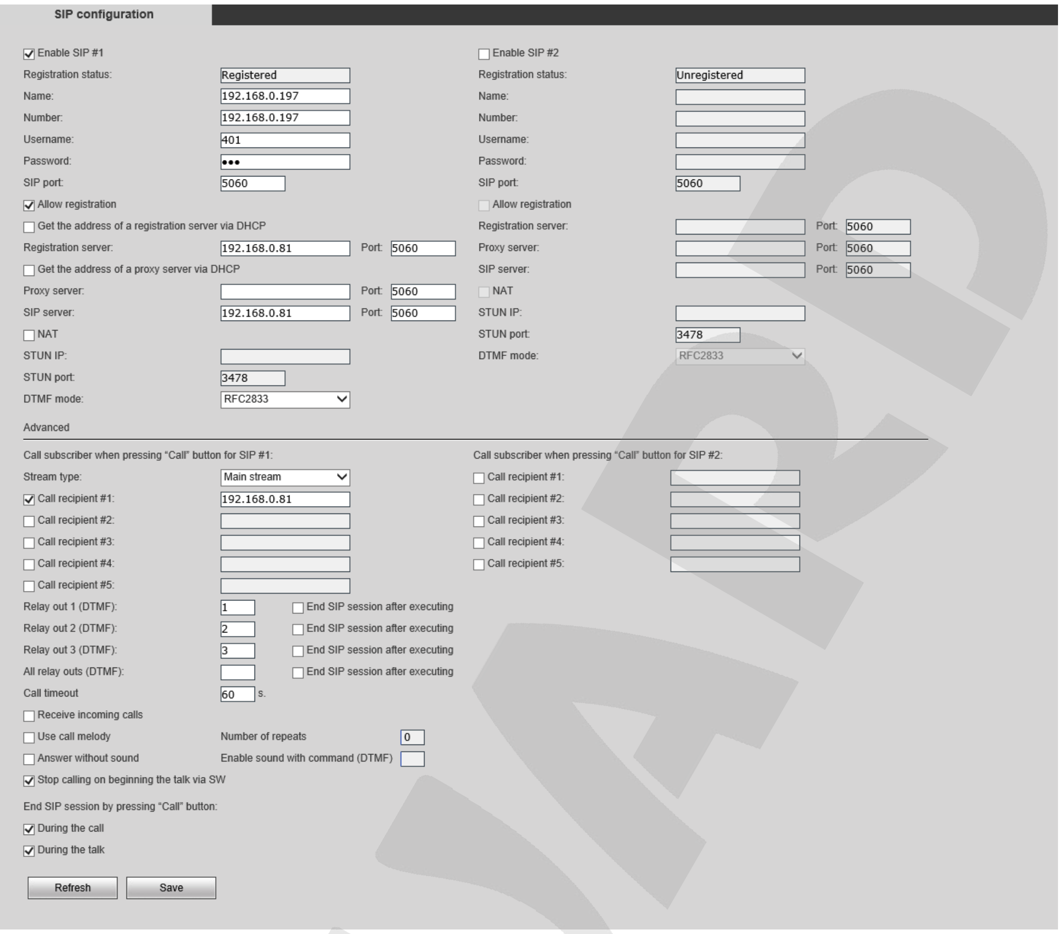
Enable SIP #1: enable the SIP option.

Name: enter a device name for its easy identification.

Number: enter the door station IP address.

Call recipient #1: enter the IP address of the device which will receive the call (for example, PC).

To apply new settings, click **[Save]** (*Pic. C2*).



SIP configuration

☑ Enable SIP #1

Registration status: Registered

Name: 192.168.0.197

Number: 192.168.0.197

Username: 401

Password: •••

SIP port: 5060

☑ Allow registration

□ Get the address of a registration server via DHCP

Registration server: 192.168.0.81 Port: 5060

□ Get the address of a proxy server via DHCP

Proxy server: Port: 5060

SIP server: 192.168.0.81 Port: 5060

□ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

□ Enable SIP #2

Registration status: Unregistered

Name:

Number:

Username:

Password:

SIP port: 5060

□ Allow registration

Registration server: Port: 5060

Proxy server: Port: 5060

SIP server: Port: 5060

□ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

Advanced

Call subscriber when pressing “Call” button for SIP #1:

Stream type: Main stream

☑ Call recipient #1: 192.168.0.81

□ Call recipient #2:

□ Call recipient #3:

□ Call recipient #4:

□ Call recipient #5:

Relay out 1 (DTMF): 1 □ End SIP session after executing

Relay out 2 (DTMF): 2 □ End SIP session after executing

Relay out 3 (DTMF): 3 □ End SIP session after executing

All relay outs (DTMF): □ End SIP session after executing

Call timeout 60 s.

□ Receive incoming calls

□ Use call melody Number of repeats 0

□ Answer without sound Enable sound with command (DTMF)

☑ Stop calling on beginning the talk via SW

End SIP session by pressing “Call” button:

☑ During the call

☑ During the talk

Call subscriber when pressing “Call” button for SIP #2:

□ Call recipient #1:

□ Call recipient #2:

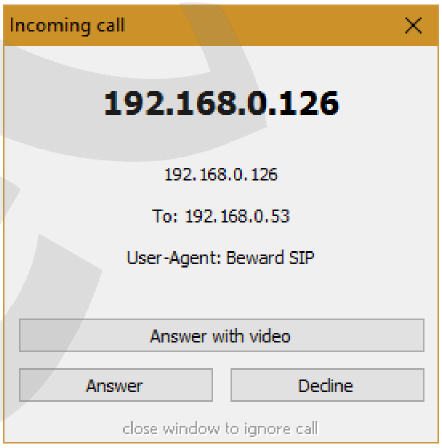
□ Call recipient #3:

□ Call recipient #4:

□ Call recipient #5:

Pic. C2

If the settings are correct then you will see the following window after pressing the call button of a door station:



Incoming call

192.168.0.126

192.168.0.126

To: 192.168.0.53

User-Agent: Beward SIP

Pic. C3

You can answer or cancel the call.

Setting the SIP direct connection is finished.

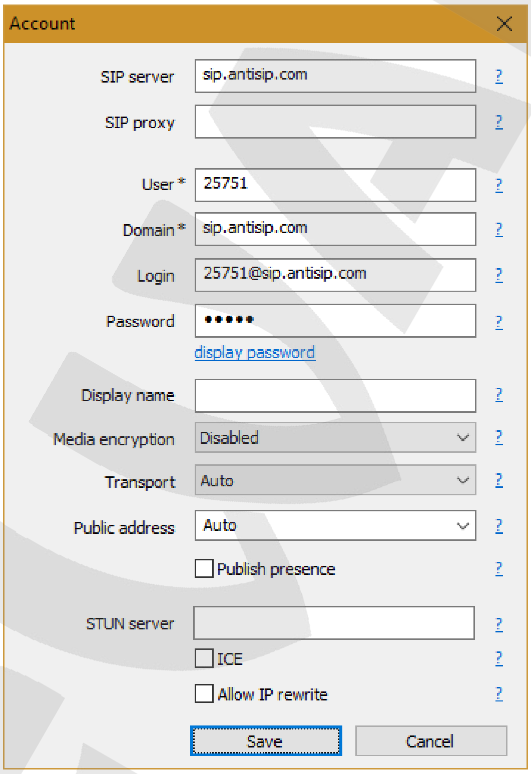
C2. SIP server

Setting connection via a SIP server 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) in case of using a SIP server. 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 given on the *Picture B1*. Click ***Menu – Add account***:



Account

SIP server	sip.antisip.com
SIP proxy	
User *	25751
Domain *	sip.antisip.com
Login	25751@sip.antisip.com
Password	•••••
	display password
Display name	
Media encryption	Disabled
Transport	Auto
Public address	Auto
	☐ Publish presence
STUN server	
	☐ ICE
	☐ Allow IP rewrite

Pic. C4

Enter the following main data:

SIP server: your SIP server address.

User: your account username.

Domain: your account domain.

Login: username for authentication.

Password: your account password.

STUN server: enter the STUN server address to access via NAT.

If necessary, you can also enter additional parameters. To apply new settings, click **[Save]**.

> **NOTE:**
> Contact your system administrator for local SIP server settings. If you have no a local SIP server then you can use any Internet SIP server you prefer.

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

You commonly need specify the following parameters:

Enable SIP #1: Enable a SIP option.

Name: Enter the name to identify a door station.

Number: Enter the SIP number for your account.

Username: Enter the username for authentication.

Password: Enter the password for authentication.

SIP port: Enter the SIP port (by default – 5060).

Allow registration: Use a SIP server.

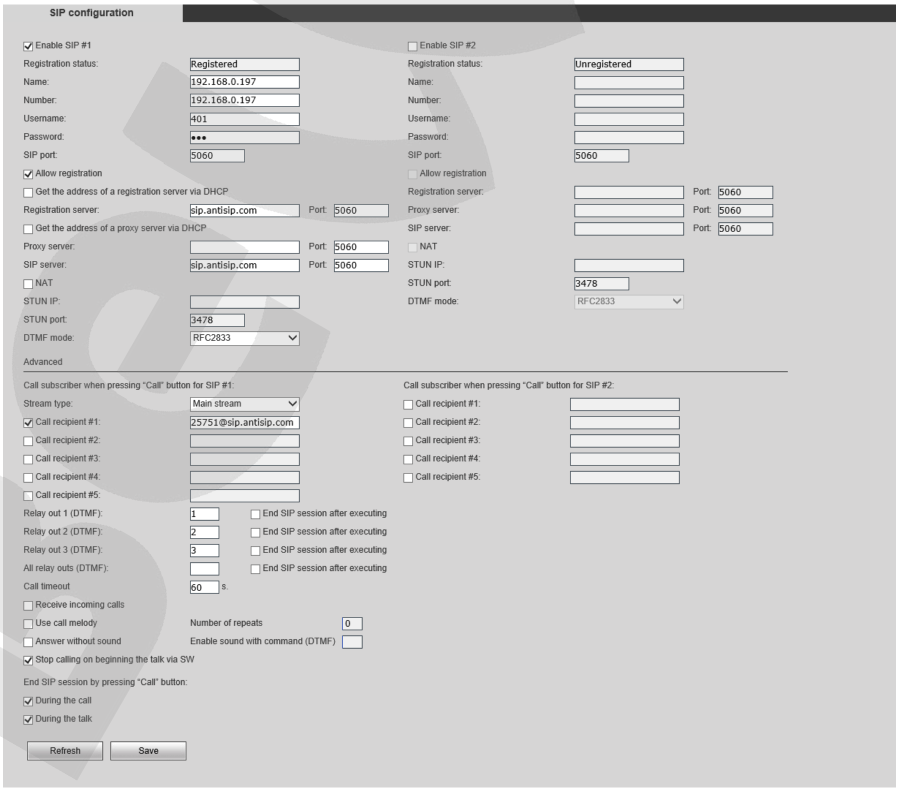
Registration server: Enter the domain address for your SIP account.

SIP server: Enter the address of your SIP server.

Call recipient #1: Enter the SIP number of the device which will receive the call (for example, SIP number of a PC).

STUN IP: Enter the STUN server address to access via NAT.

To apply new settings, click **[Save]** (*Pic. C5*).



SIP configuration

☑ Enable SIP #1

Registration status: Registered

Name: 192.168.0.197

Number: 192.168.0.197

Username: 401

Password: •••

SIP port: 5060

☑ Allow registration

☐ Get the address of a registration server via DHCP

Registration server: sip.antisip.com Port: 5060

☐ Get the address of a proxy server via DHCP

Proxy server: Port: 5060

SIP server: sip.antisip.com Port: 5060

☐ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

☐ Enable SIP #2

Registration status: Unregistered

Name:

Number:

Username:

Password:

SIP port: 5060

☐ Allow registration

Registration server: Port: 5060

Proxy server: Port: 5060

SIP server: Port: 5060

☐ NAT

STUN IP:

STUN port: 3478

DTMF mode: RFC2833

Advanced

Call subscriber when pressing “Call” button for SIP #1:

Stream type: Main stream

☑ Call recipient #1: 25751@sip.antisip.com

☐ Call recipient #2:

☐ Call recipient #3:

☐ Call recipient #4:

☐ Call recipient #5:

Relay out 1 (DTMF): 1 ☐ End SIP session after executing

Relay out 2 (DTMF): 2 ☐ End SIP session after executing

Relay out 3 (DTMF): 3 ☐ End SIP session after executing

All relay outs (DTMF): ☐ End SIP session after executing

Call timeout 60 s.

☐ Receive incoming calls

☐ Use call melody Number of repeats 0

☐ Answer without sound Enable sound with command (DTMF)

☑ Stop calling on beginning the talk via SW

End SIP session by pressing “Call” button:

☑ During the call

☑ During the talk

Call subscriber when pressing “Call” button for SIP #2:

☐ Call recipient #1:

☐ Call recipient #2:

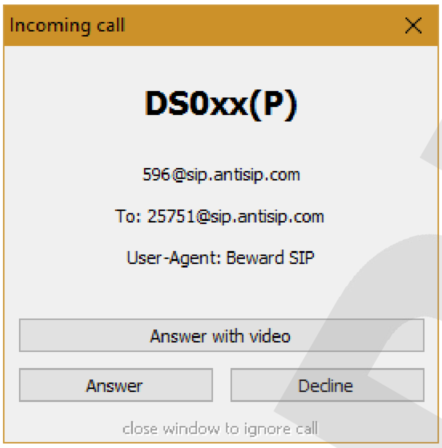
☐ Call recipient #3:

☐ Call recipient #4:

☐ Call recipient #5:

Pic. C5

If the settings are correct then you will see the following window after pressing the call button of a door station:



DS0xx(P)

596@sip.antisip.com

To: 25751@sip.antisip.com

User-Agent: Beward SIP

Pic. C6

You can answer or cancel the call.

The setting 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 E. 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 to11 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.

NAS (Network Attached Storage) is a file-level computer data storage connected to a computer network (usually local). Often manufactured as a purpose-built specialized computer. Several such computers can be combined into a single NAS system.

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.

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that uses a special tunnel in a standard unprotected network to establish a protected connection with the server. Available as a standard protocol in nearly every operating system and devices with VPN support, which allows it to be used without any third-party software.

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.

SIP (Session Initiation Protocol) is an IP telephony-based signaling protocol used to transfer voice data. SIP protocol is based on the “Client-Server-Client” principle, i.e. an exchange of queries from Clients and responses from the Servers.

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.