TVIP40000

User Manual

Version 10/2010

Original English user manual. Keep for future use.

Introduction

Dear Customer,

Thank you for purchasing this product.

This product meets the requirements of the applicable European and national guidelines. The corresponding declarations and documents can be obtained from the manufacturer (www.abus-sc.com).

To maintain this condition and to ensure risk-free operation, you as the user must observe these operation instructions!

Before initial start-up, read through the complete operating instructions observing operating and safety instructions.

All company and product names mentioned in this document are registered trademarks.
All rights reserved.

If you have any questions, please contact your installer or your local dealer!

⚠

Disclaimer

This user manual was prepared with greatest care. If you should notice omissions or inaccuracies, please inform us about these on the back of this manual given address.
The ABUS Security-Center GmbH assumes no liability for technical and typographical faults and reserves the right to make at any time modifications to the product or user manual without a previous announcement.
The company is not liable or responsible for direct and indirect subsequent damages which are caused in connection with the equipment, the performance and the use of this product.
No guarantee for the content of this document is taken.

Icon explanation

⚡ **A flash in the triangle is used if there is danger for the health, e.g. by an electric shock.**

⚠ **An exclamation mark in the triangle points to an important note in this user manual which must be minded.**

ℹ **This symbol can be found when you are to be given tips and information on operation.**

Important safety advice

⚡ **The warranty will expire for damage due to non-compliance with these operating instructions. ABUS will not be liable for any consequential loss!**

⚠ **ABUS will not accept liability for damage to property or personal injury caused by incorrect handling or non-compliance with the safety-instructions.**
In such cases the warranty will expire.

Dear customer,
The following safety instructions are intended not only for the protection of your health, but also for the protection of the device. Please read through the following points carefully:

- There are no parts on the inside of the product which need to be serviced. Apart from this, the license (CE) and the guarantee/warranty will lapse if you open/take the product apart.
- The product will be damaged even it falls from a low height.
- This device can be used in internal area.
- At the installation of the product please take care that direct sunlight cannot fall onto the image sensor of the device. Please follow the installation instructions in the corresponding chapter of this user manual.

Avoid using the device under the following unfavorable ambient conditions:

- wetness or excessive air humidity
- extreme cold or heat
- direct sunlight
- dust or combustible gases, vapors or solvents
- strong vibration
- strong magnetic fields, such as those found in the vicinity of machinery or loudspeakers
- the video server may not be installed on unstable surfaces

General safety instructions:

- Do not leave packaging material lying around carelessly. Plastic/ foil/bags and polystyrene parts etc. could become dangerous toys for children.
- For safety reasons don’t give the video server into child hands due to them being able to swallow small parts.
- Please do not insert objects through the openings into the device.
- Use only accessories which are specified by the manufacturer.
  Please do not connect incompatible parts to the device.
- Please pay attention to the safety instructions and user manuals of the other connected devices.
- Check the device for damages before installation. If this should be the case please do not use it.
- Please adhere to the operational voltage limitations listed in the technical data. High voltage could destroy the device and pose a health hazard (electric shock).

Safety advice

1. Mains supply: Power supply 110 - 250VAC, 50/60Hz / 12VDC, 1,5A (included in package content)
   Operate this product only from the type of power supply indicated on the marking label. If you are not sure of the type of power supplied to your home, consult your local power company. Disconnect the product from the mains before you start any maintenance or installation procedures.

2. Overloading
   Do not overload a wall outlet, extension cord or adapter as this may result in electric fire or shock.

3. Cleaning
   Disconnect the product from the wall outlet before cleaning. Use a light damp cloth (no solvents) to dust the product.

Warnings

Follow all safety and operating advises before starting-up the device!

1. Follow these directions in order to avoid damage of the power cord or plug:
   - Do not modify or process the power cord or plug arbitrarily.
   - Do not bend or twist the power cord.
   - Make sure to disconnect the power cord holding the plug.
   - Keep heating appliances as far as possible from the power cord in order to prevent the cover vinyl from melting.

2. Follow these directions. Failure to follow any of them may cause electrical shock:
   - Do not open the main body, except for installing the HDD.
     Disconnect the product from the mains before you start.
   - Do not insert metal or inflammable objects inside the product.
   - In order to avoid any damage during lighting use a surge protection.

3. Do not use the product when it is out of order. If you continue to use the product when defective, serious damage can be caused to it. Make sure to contact your local product distributor if the product is out of order.

During the installation into an existing video surveillance system make sure that all devices are disconnected from the low and supply voltage circuit.

If in doubt allow a professional electrician to mount, install and wire-up your device. Improper electrical connection to the mains does not only represent at threat to you but also to other persons.
Wire-up the entire system making sure that the mains and low voltage circuit remain separated and cannot come into contact with each other in normal use or due to any malfunctioning.

Unpacking

While you are unpacking the device please handle it with utmost care.

If you notice any damage of the original packaging, please check at first the device.
If the device shows damages, please contact your local dealer.

Inhaltsverzeichnis

Intended use

For a detailed description of functions, refer to Chapter 4, “Initial start-up".

⚠ Any other use than that described above can lead to damage to the product and in addition involve other risks. This does not include operation for other applications and would in case of doing so the guarantee and any related liability will lapse. This is also the case if any unauthorized changes or additions have been made to the product.

⚠ Please read through the entire manual carefully before putting this product into operation. This operating manual contains guidelines that are important for correct mounting and operating.

1. Scope of delivery

ABUS D1 Video server
TVIP40000

Power supply

Mounting bracket

Quickguide

Software CD
including user manual

2. Installation

Make sure that all previous listed accessories were included in scope of delivery. In order to operate the video server an Ethernet network cable is necessary. The cable has to comply with specifications of UTP categories 5 (CAT 5) and must not exceed 100 meters of length.

2.1 Power supply

Before you start the installation make sure that the mains voltage and the nominal voltage of the video server correspond.

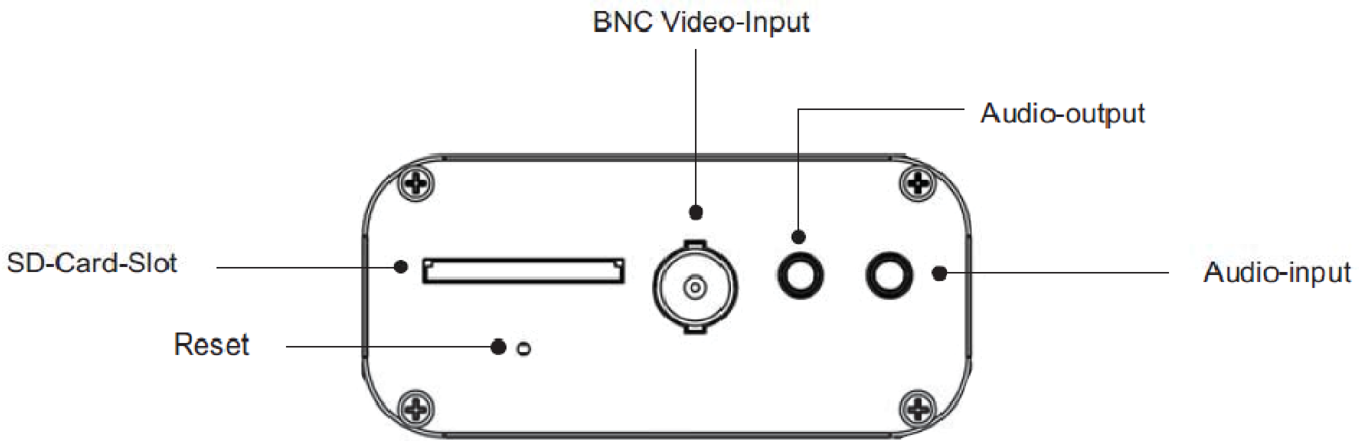
2.2 Installing the video server

To install the video server on the wall, you will need the mounting brackets and screws included in the scope of delivery.

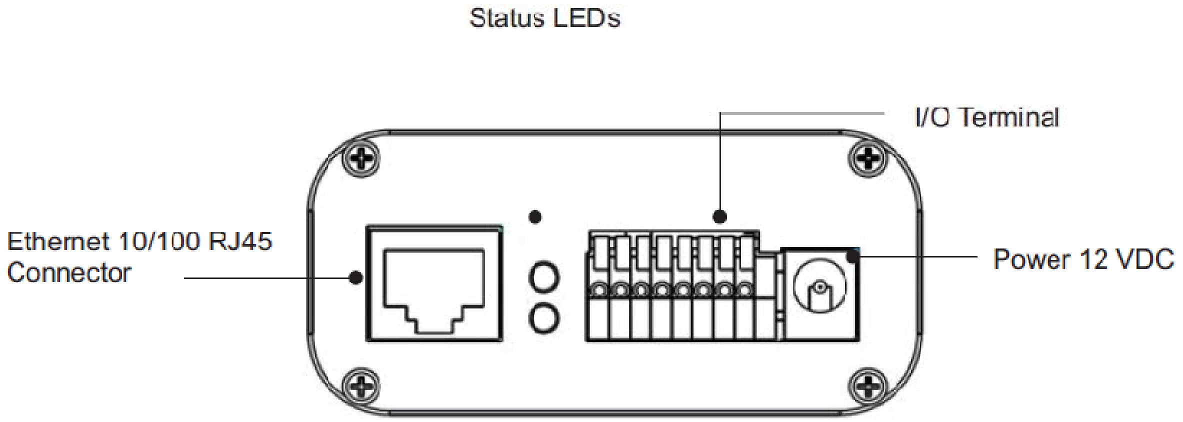
⚠ **ATTENTION!**
Make sure to disconnect the video server from the power supply during installation.

3. Video server description

3.1 Front view

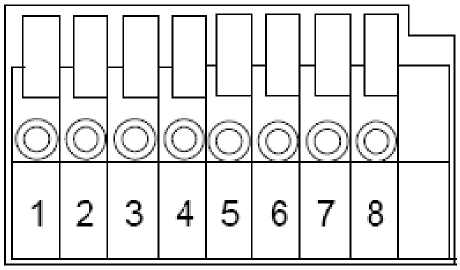


3.2 Rear view

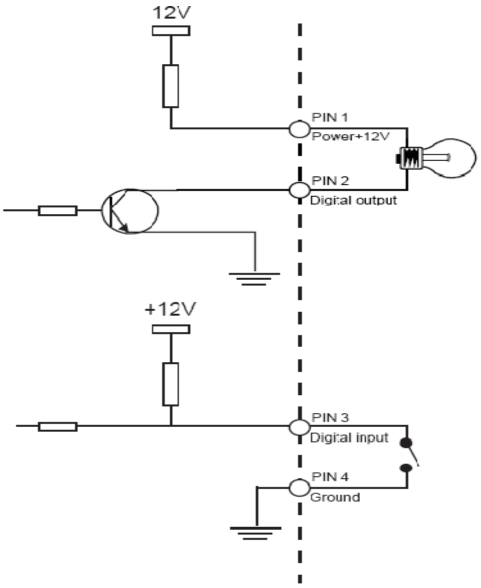


3.3 Alarm inputs and digital outputs

PIN	Descritption
1	+12V Output
2	Digital output
3	Digital input
4	Ground
5	24V AC input
6	24V AC input
7	RS-485 +
8	RS-485 -



3.4 Gate input / output ans status display



Status LED description:

Status / LED colour	Green	Red
System start	Off	On
Video server turned off	Off	Off
Network works (heartbeat)	1/s	On
Network problem	Off	On
Firmware update	1/s	0.1/s
Restoring factory settings	0.1/s	0.1/s

In order to **reboot** the video server or restore the factory settings press the reset button. Use an appropriate small tool.

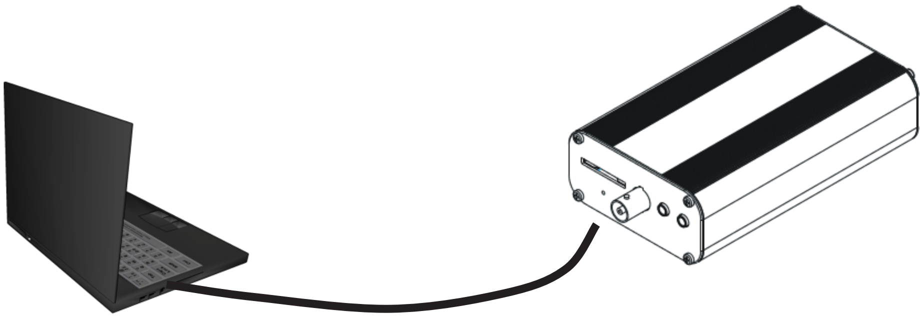
Video server reboot: Press the reset button once and wait until the video server to restart.

Restore factory settings: Press and hold the reset button for approx. 30 seconds until the status LEDs start flashing. All settings will be reset to factory default.

4. Initial start-up

Direct connection between video server and PC / laptop

1. Make sure to use a crossover network cable
2. Connect the cable with the Ethernet port of the PC / Laptop and the video server
3. Connect the power supply to the video server
4. Configure the IP address of the PC / Laptop to 169.254.0.1
5. Continue with point 5.1 in order to finish the initial installing and build-up a connection to the video server

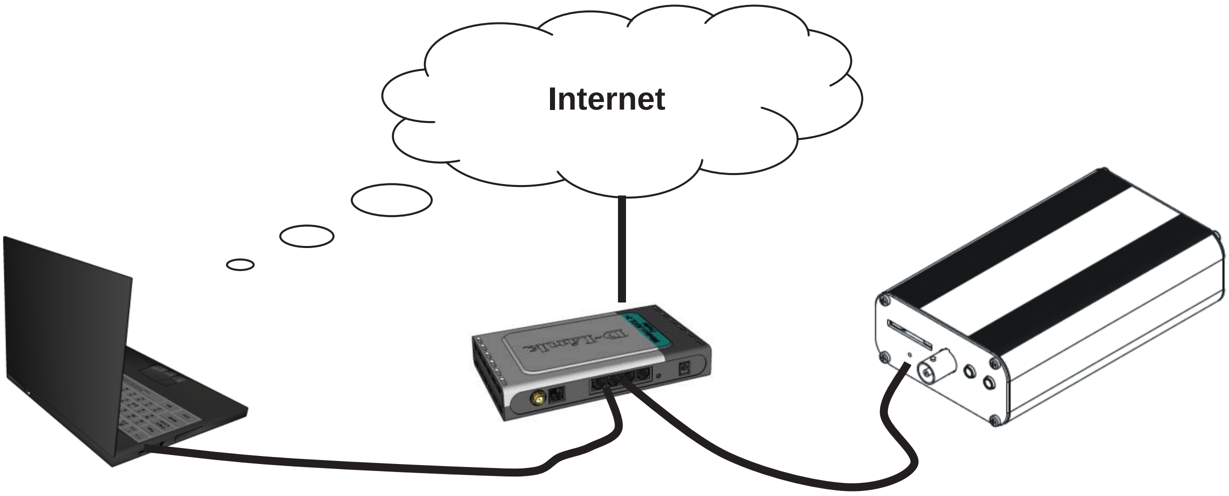


➀ Crossed Ethernet cable

Connecting the video server by using a router / switch

1. Make sure to use a pair of patch cables
2. Connect the cable with Ethernet port of the PC / laptop with the router / switch.

3. Connect the cable with the network cable and with the router / switch.
4. Connect the power supply to the video server
5. If there is a name server (DHCP) available in your network then set the IP address of your PC / laptop to “automatically receive IP address”
   If there is no name server (DHCP) available set the IP address of your PC / laptop to 169.254.0.1
6. Continue with point 5.1 in order to finish the initial installing and build-up a connection to the video server



Patch cable

4.1 First video server access

The first video server access takes place by using the program „Installation Wizard 2“.
After starting the wizard it will automatically search the network for all connected EyeseoIP network video servers and video servers.

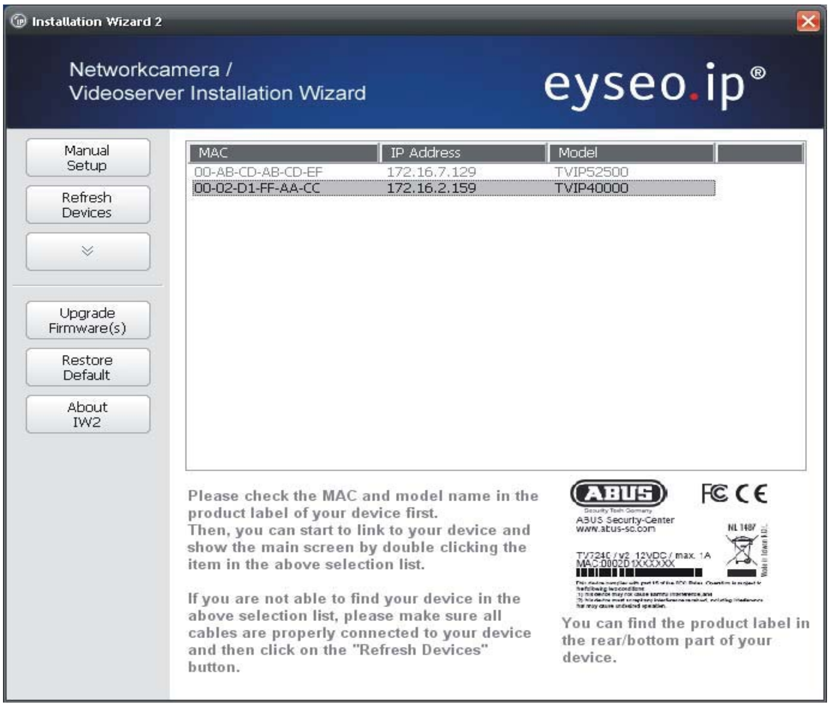
You can find the program on the on the CD at **CD-ROM\Tools\EyseoIP Tools**

Install the program on your PC and start it. The wizard will automatically search your network for EyseoIP video server.

The IP address at factory default is **169.254.0.99**. Without using the installation wizard you can only connect to the video server if the IP address of the PC is between 169.254.0.1 and 169.254.0.98.

If a DHCP server is active in your network the IP address for your PC and video server will be set automatically.

Start now the installation wizard. If no DHCP server is active the installation wizard adds a virtual IP address in the range of 169.1254.0.xx. As long as the installation wizard is active you can access the network video server by using the virtual IP address. We recommend adjusting immediately the video servers network settings to the IP settings of the PC’s network.



MAC	IP Address	Model
00-AB-CD-AB-CD-EF	172.16.7.129	TVIP52500
00-02-D1-FF-AA-CC	172.16.2.159	TVIP40000

Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

You can find the product label in the rear/bottom part of your device.

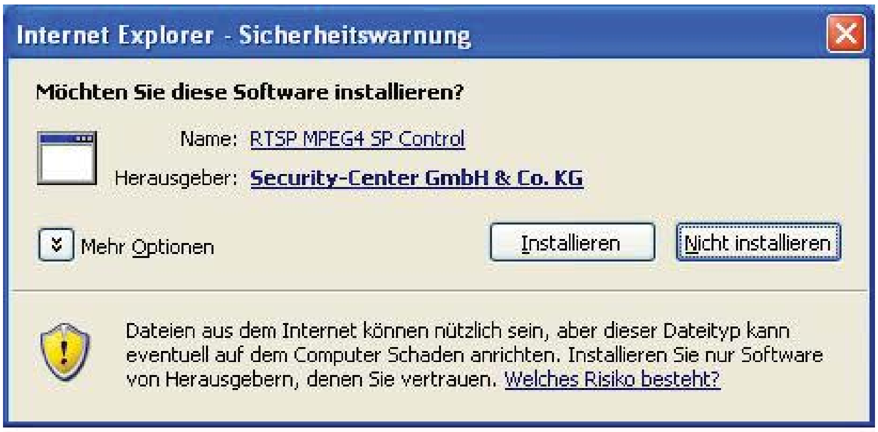
After closing Installation wizard 2 the additional virtual IP adress will be removed. If IP-Video server’s IP address is still in a different IP area then the one from your PC the video server access is no longer possible.

4.2 Connecting to the video server by using a web browser

If connecting to the video server by using Mozilla Firefox or Netscape a QuickTime stream will be displayed. This requires that QuickTime from Apple is installed

In order to show the video stream when using Microsoft Inter Explorer a video plug-in is required. This will be installed when connecting to the video server. A window will appear asking you to install the plug-in. Press the install button to continue an install the plug-in. Depending on the security setup of the Internet Explorer the installation might be blocked. In this case you need to adjust the security settings.

4.3 Installing the Active-X plug-in



Internet Explorer - Sicherheitswarnung

Möchten Sie diese Software installieren?

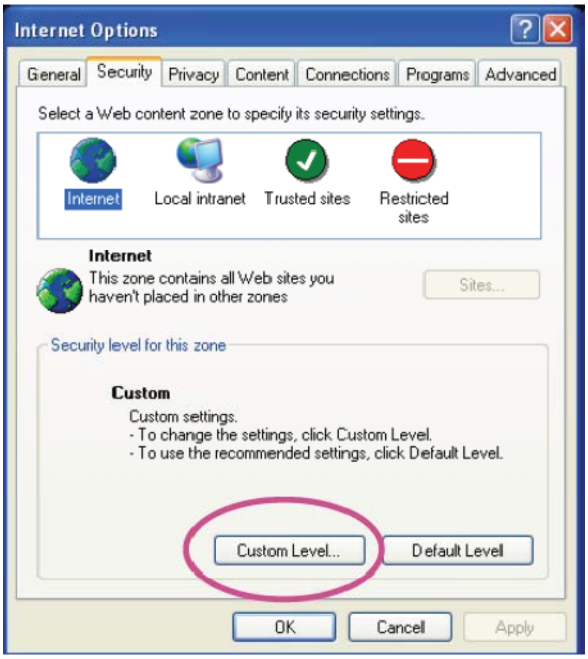
Name: RTSP MPEG4 SP Control

Herausgeber: Security-Center GmbH & Co. KG

Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Installieren Sie nur Software von Herausgebern, denen Sie vertrauen. Welches Risiko besteht?

For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you don't have Quick Time on your computer, please download it first, then launch the web browser.

4.4 Adjusting the security settings



Internet Options

Select a Web content zone to specify its security settings.

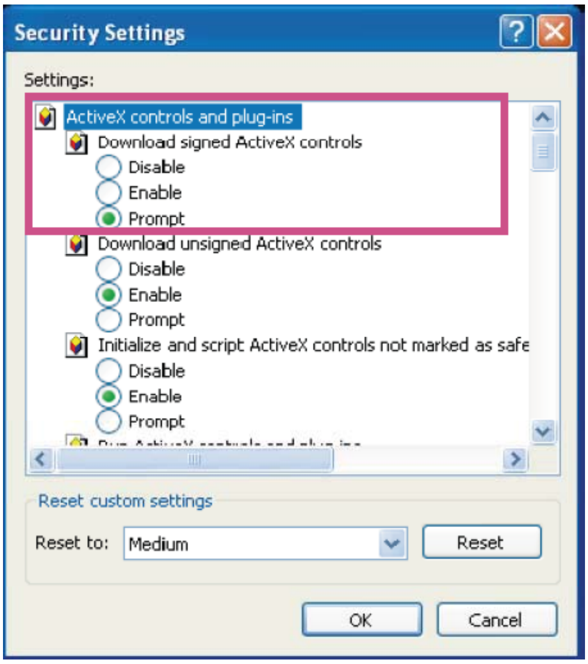
Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.



Security Settings

Settings:

ActiveX controls and plug-ins

Download signed ActiveX controls
○ Disable
○ Enable
● Prompt

Download unsigned ActiveX controls
○ Disable
● Enable
○ Prompt

Initialize and script ActiveX controls not marked as safe
○ Disable
● Enable
○ Prompt

Reset custom settings

Reset to: Medium

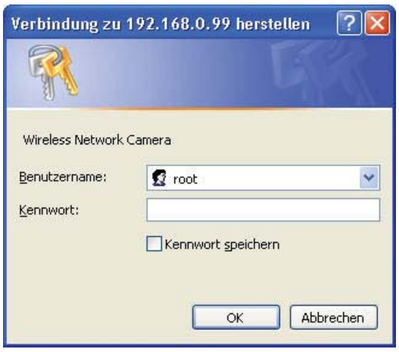
NOTICE!
The security settings of the Internet Explorer can prevent displaying the video stream. Change at „Extras/Internet Options/Security“ to a lower level. Make sure to activate the ActiveX control elements at “Custom Level”.

4.5 Password authentication

At factory default there is no admin password set for accessing the video server. For security reasons the administrator should immediately set a password after the initial setup. After setting an admin password the video server will request for every access a username and password.

The permanent default username for the admin will be **„„root”** and cannot be changed. The only way to reset the password if it is forgotten is to reset the video server to factory default settings.

In order to access the video server enter username “root” and the before defined password.



Verbindung zu 192.168.0.99 herstellen

Wireless Network Camera

Benutzername: root

Kennwort:

☐ Kennwort speichern

-> After successful authentication you will connect to the video server and a video stream will be displayed.

4.6 Connecting to the video server by using a RTSP player

You can display the MPEG-4 video streams by connecting to the video server with a RTSP capable media player. Following free media players support RTSP:

- VLC Media Player
- Real Player
- QuickTime Media Player

The RTSP address has to be entered as following:

rtsp://<IP-address of the network video server>:<rtsp Port>/<Name of the video stream >

How to change the name of the video stream will be explained further on.

Example:
rtsp://192.168.0.99:554/live.sdp

4.7 Connecting to the network video server by using a mobile phone

Make sure that your mobile phone is able to establish a internet connection. Furthermore the mobile phone has to have an RTSP capable media player like:

- Real Player
- Core Player

More information you can find in chapter “RTSP-Transmission”.

Please notice that limited access can occur, due to low mobile network bandwidth. We recommend following settings to optimize the video stream:

Video compression	MPEG-4
Resolution	176x144
I Frame	1 Second
Video quality (constant bit rate)	40 Kbit / Second
Audio Compression (GSM-AMR)	12.2 Kbit / Second

If the media player does not support the RTSP authentication, then deactivate this option in the RTSP settings of the video server.

The RTSP address has to be entered as following:

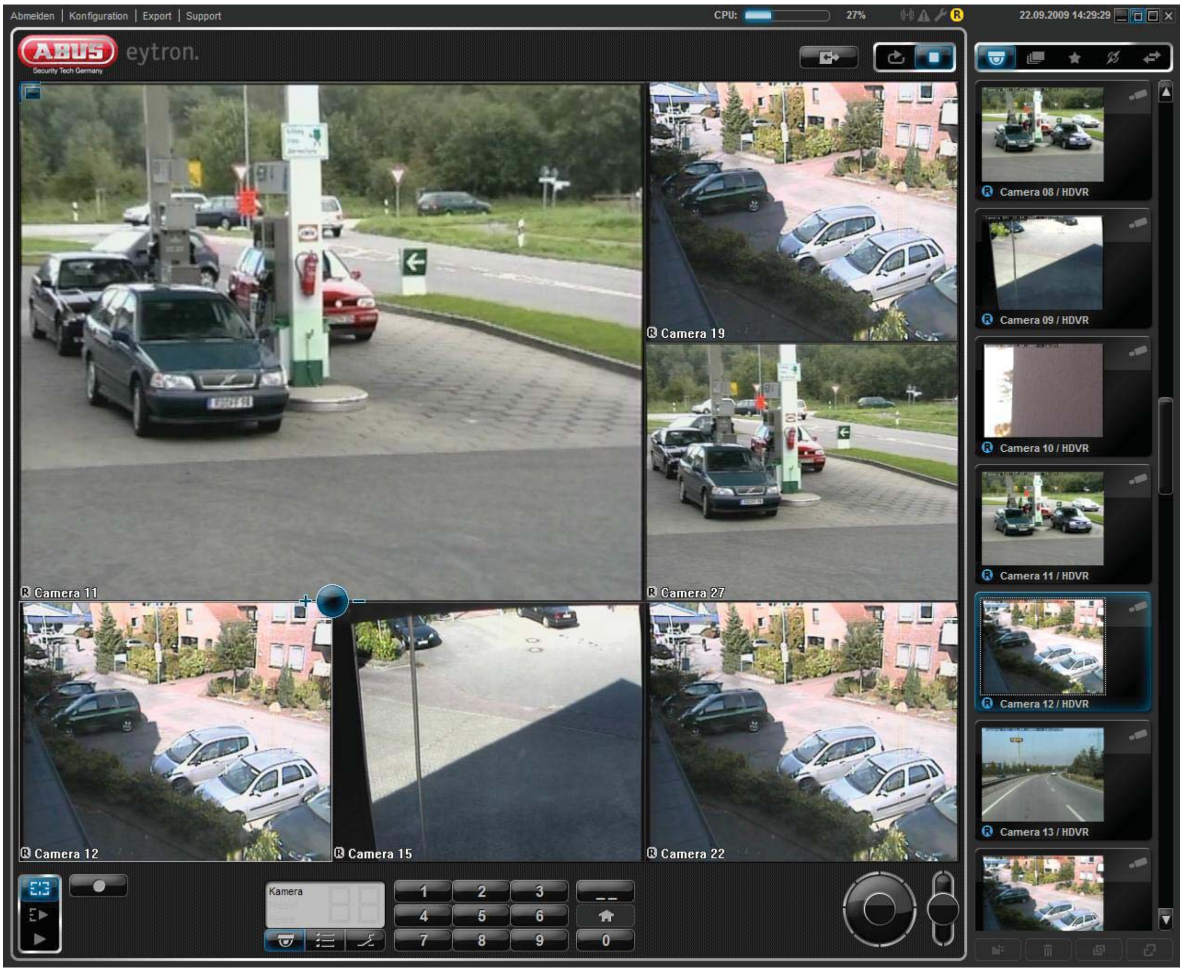
rtsp://<IP-address of the video server >:<rtsp Port>/<Name of the video stream >

How to change the name of the video stream will be explained further on.

Example:
rtsp://192.168.0.99:554/live.sdp

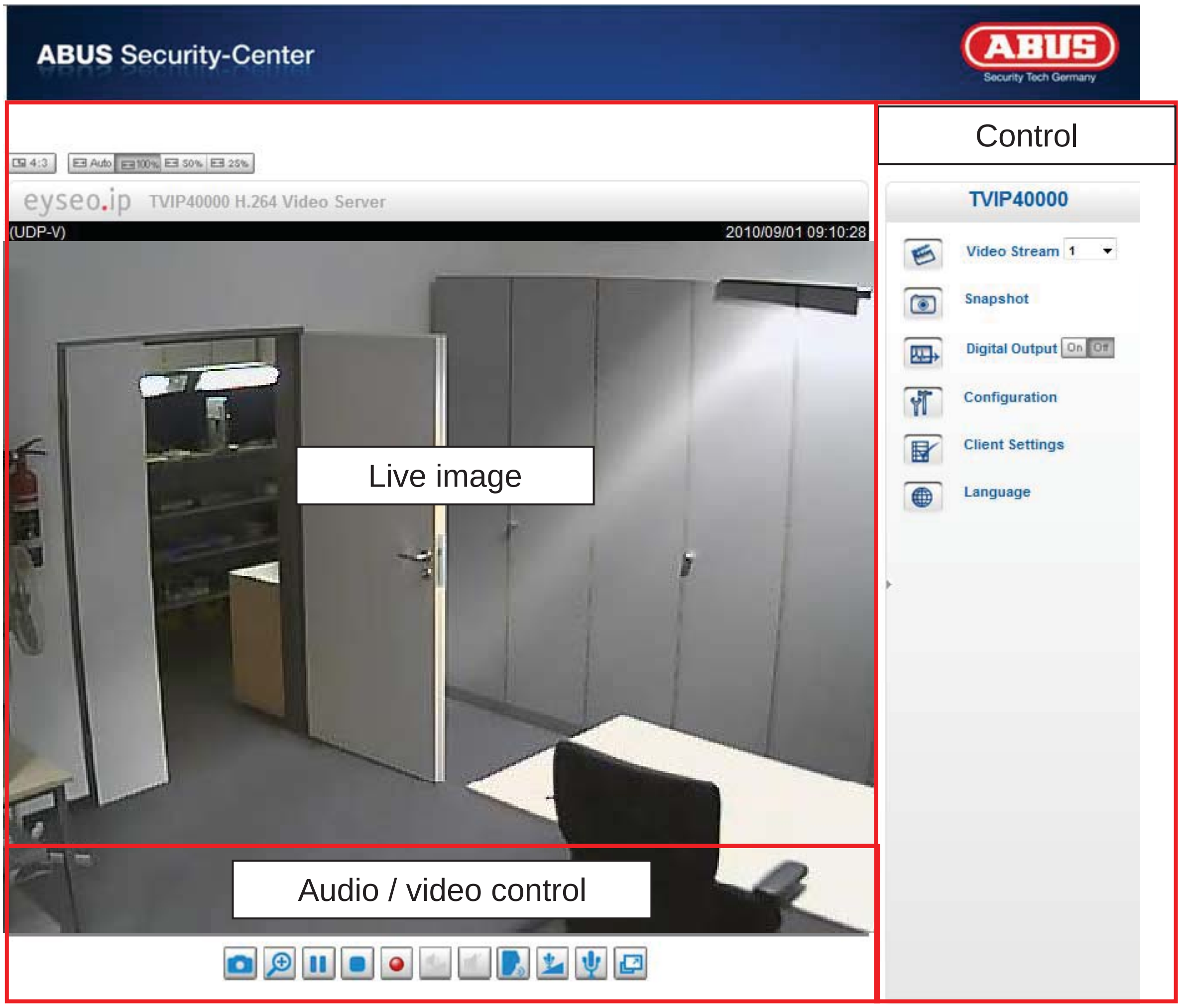
4.8 Connecting to the video server by using eytron VMS Express

The included CD contains the free recording software eytron VMS Express. This software enables you to connect and display to several IP video servers and record these. Further information can be found in the manual of the software located on the CD.



5. User functions

Open the main menu on the video server. The interface is divided into the following main areas:



Live image

- Change the zoom level by pressing the mouse scroll button.
- Click in the live picture to take over control of an analogue pan/tilt camera directly.

Video server control

Video Stream
Select from video streams 1 – 4 to view the live image.

Snapshot
Create a snapshot (without ActiveX plug-in).

Digital Output
Switch the digital output on and off manually.

Configuration
Configure the video server (administrator settings).

Client Settings
Configure the client settings; you can find detailed information on the following pages.

Language

Set the interface language.

Pan/tilt/zoom control

Use the control buttons to control the digital and mechanical pan/tilt/zoom function.

Auto 100% 50% 25% Variable view sizes

Using these buttons, you can choose from three different zoom levels for the live picture (100%, 50% and 25%). You can also adjust the live picture to automatically fit the current browser size. Do do this, select the “AUTO” option.

4:3 Screen ratio

Press the “4:3” button to set the page ratio of the live picture to 4:3.

Show/hide menu

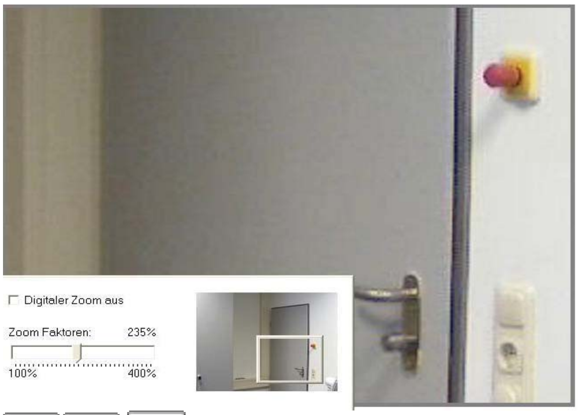
5.1 Audio / video control

Variable view sizes

The web browser displays a new window containing the snapshot. To save the image file to your PC, right-click the image and select “Save As”.

Digital zoom and snapshot

Click on the magnifying glass icon underneath the video server view. The control panel for the digital zoom appears. Disable the “Disable Digital Zoom” box and change the zoom factor with the slider.



☐ Digitaler Zoom aus

Zoom Faktoren: 235%

Start / stop live image view

The live stream can be stopped (paused) or exited. In both cases, the live stream can be continued by pressing the play symbol.

Local recording

A recording on the local hard disk can be started or stopped here. You can configure the recording path under “Client Settings”.

Adjust the volume

Press to manually set the audio output level.

Audio On / Off

Talk

As long as this button is pressed, the audio signals from the PC are transmitted to the audio output of the video server.

Microphone volume

Press to manually adjust the level for the audio input of the video server.

Mute

Press to switch the audio input of the video server on and off.

Full-screen

Activates the full-screen view. The live image on the video server is shown on the entire screen.

5.2 Client settings

The user settings are saved on the local computer. The following settings are available:

Media Options Allow the user to disable the audio or video function.

Protocol Options Allows a connection protocol to be selected between the client and the server.
The following protocol options are available for optimising the application: UDP, TCP, HTTP.

The UDP protocol gives you a larger number of audio and video streams in real time. However, some data packets can be lost due to the large data volume in the network. Pictures may be unclear in this case.
The UDP protocol is recommended if you have no special requirements.

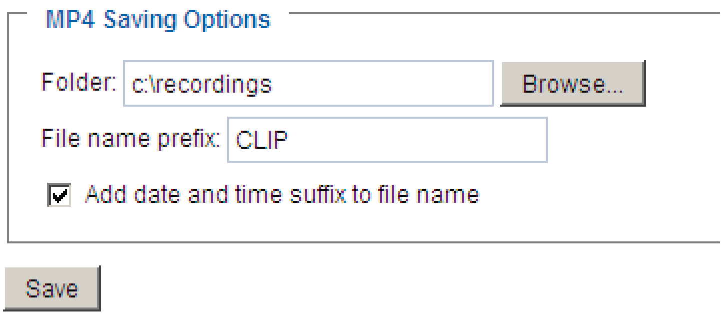
With the TCP protocol, fewer data packets are lost and the video display is more accurate. The disadvantage of this protocol is that the realtime stream is worse than with the UDP protocol.

Select the HTTP protocol if the network is protected by a firewall and only the HTTP port (80) is to be opened.

The selection of the protocol is recommended in the following order: UDP – TCP – HTTP.

MP4 Saving Options: Here, you can modify the data path to save the data immediately. Activating the "Add date and time suffix to filename" option generates files under the following name:

CLIP_20091115-164403.MP4
FileExtensionName_YearMonthDay-HourMinuteSecond.MP4



MP4 Saving Options

Folder: c:\recordings

File name prefix: CLIP

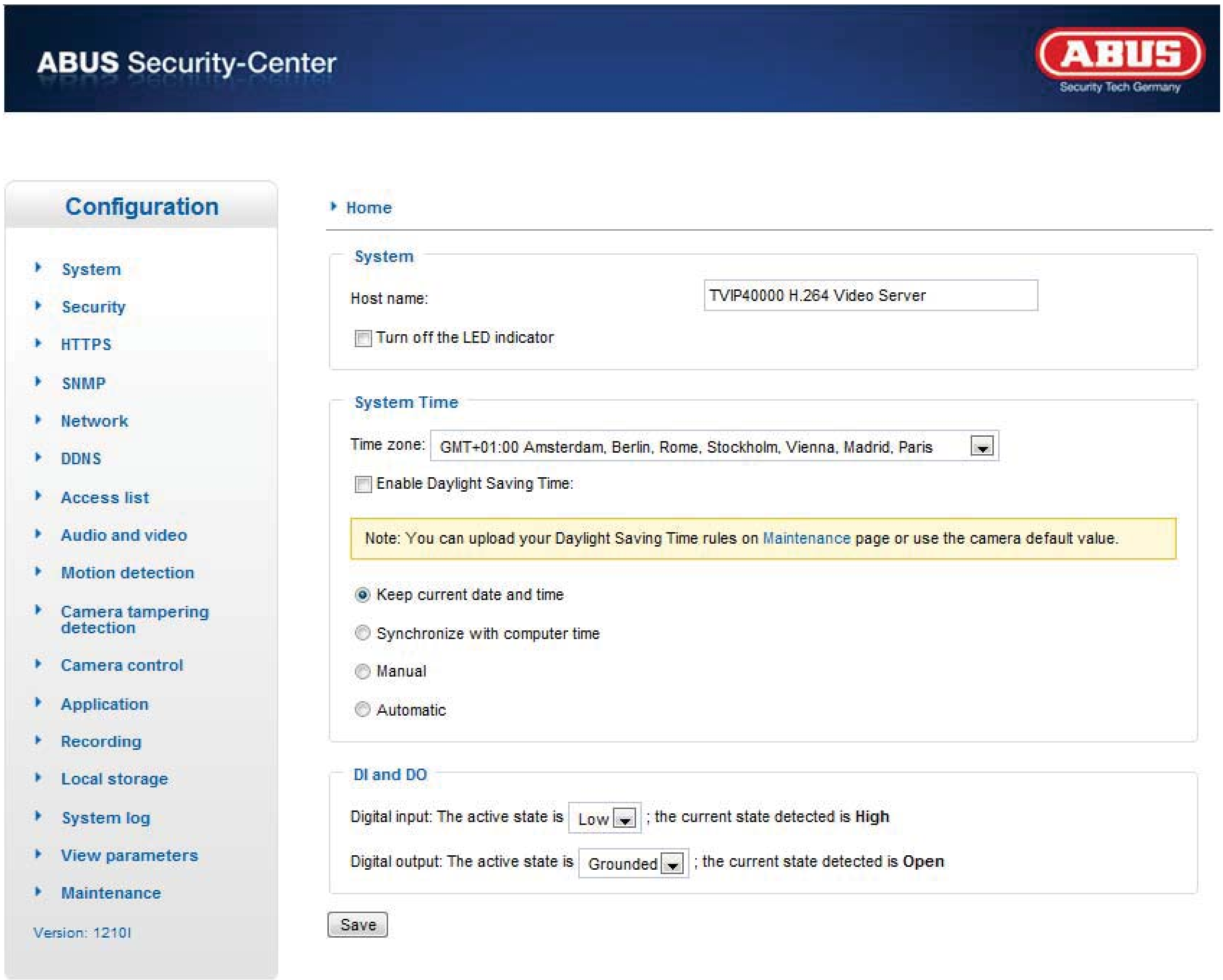
☑ Add date and time suffix to file name

The recorded data can be played back using an MP4-compatible video player (e.g. VLC Media Player).

6. Administrator Settings

6.1 System

Only the administrator has access to the system configuration. The following sections explain each of the elements in the left-hand column. Specific tasks on the Options page are printed in bold. The administrator can enter the URL under the picture to go directly to the pictures page of the configuration.



System

Host name: TVIP40000 H.264 Video Server

□ Turn off the LED indicator

System Time

Time zone: GMT+01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris

□ Enable Daylight Saving Time:

Note: You can upload your Daylight Saving Time rules on Maintenance page or use the camera default value.

● Keep current date and time

○ Synchronize with computer time

○ Manual

○ Automatic

DI and DO

Digital input: The active state is Low ; the current state detected is **High**

Digital output: The active state is Grounded ; the current state detected is **Open**

"Host name" This is the text that is shown as the title on the main page.

"Turn off the LED indicator" Select this option to switch off the LED display on the video server. This prevents other persons knowing that the video server is in operation.

"Time Zone" Adjusts the time according to the selected time zone.

"Enable Daylight Saving Time" Activates daylight saving time settings in the video server. The daylight saving time settings for every time zone are already saved in the video server.

"Keep current date and time" Choose this option if you wish to keep the current date and time of the video server. An internal realtime clock stores the date and time even after the system has been switched off due to a power cut.

“Synchronise with computer time” Synchronises the date and the time of the video server with the local computer. The read-only date and time of the PC are displayed following the update.

“Manual” Sets the date and the time according to the administrator’s input. Note the date/time format when entering in the respective fields.

“Automatic” Synchronises the date and time with the NTP server via the Internet every time the video server is switched on. This is not possible if the respective time server cannot be reached.

“NTP server” Assigns the IP address or the domain name of the time server. If you leave this text box empty, the video server is connected to the default time servers.

“DI and DO” Sets the pre-defined state for the alarm input and relay output.

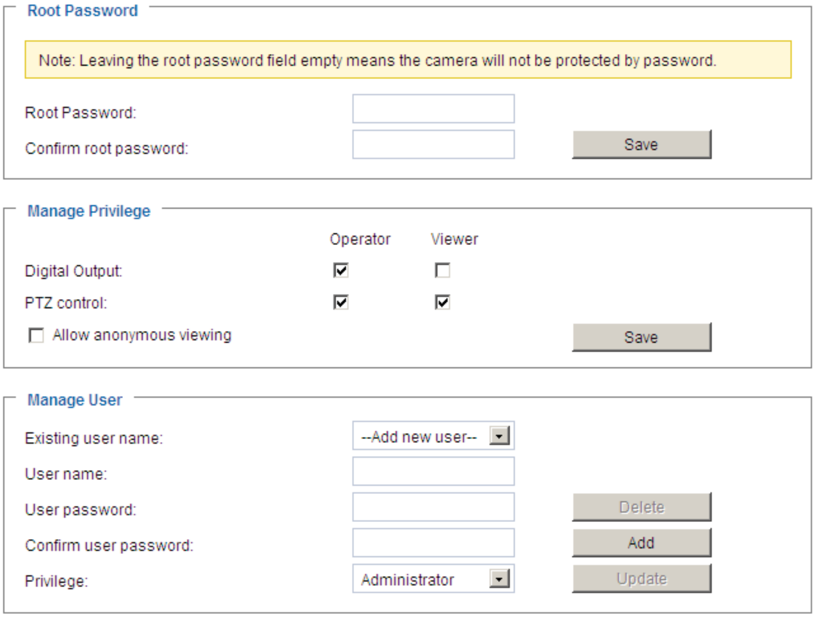
Do not forget to press **“Save”** in order for your changes to take effect.

6.2 Security

“Root Password” Allows users to change the administrator password by entering a new password. For security reasons, the passwords entered are shown as asterisks. After **“Save”** is clicked, the web browser prompts the administrator to enter the new password for accessing the video server.

“Add new user” Enter the new user name and password and click **“Add”**. The new user is displayed on the list of user names. Up to twenty user accounts can be configured.

“Edit users” Open the list of user names, select the user that you wish to edit, and change the required values. To apply the changes, click **“Update”**.



Root Password

Note: Leaving the root password field empty means the camera will not be protected by password.

Root Password:

Confirm root password:

Manage Privilege

	Operator	Viewer
Digital Output:	☑	□
PTZ control:	☑	☑

□ Allow anonymous viewing

Manage User

Existing user name: --Add new user--

User name:

User password:

Confirm user password:

Privilege: Administrator

“Delete user” Open the list of user names, select a user and click **“Delete”**, to delete this user from the list.

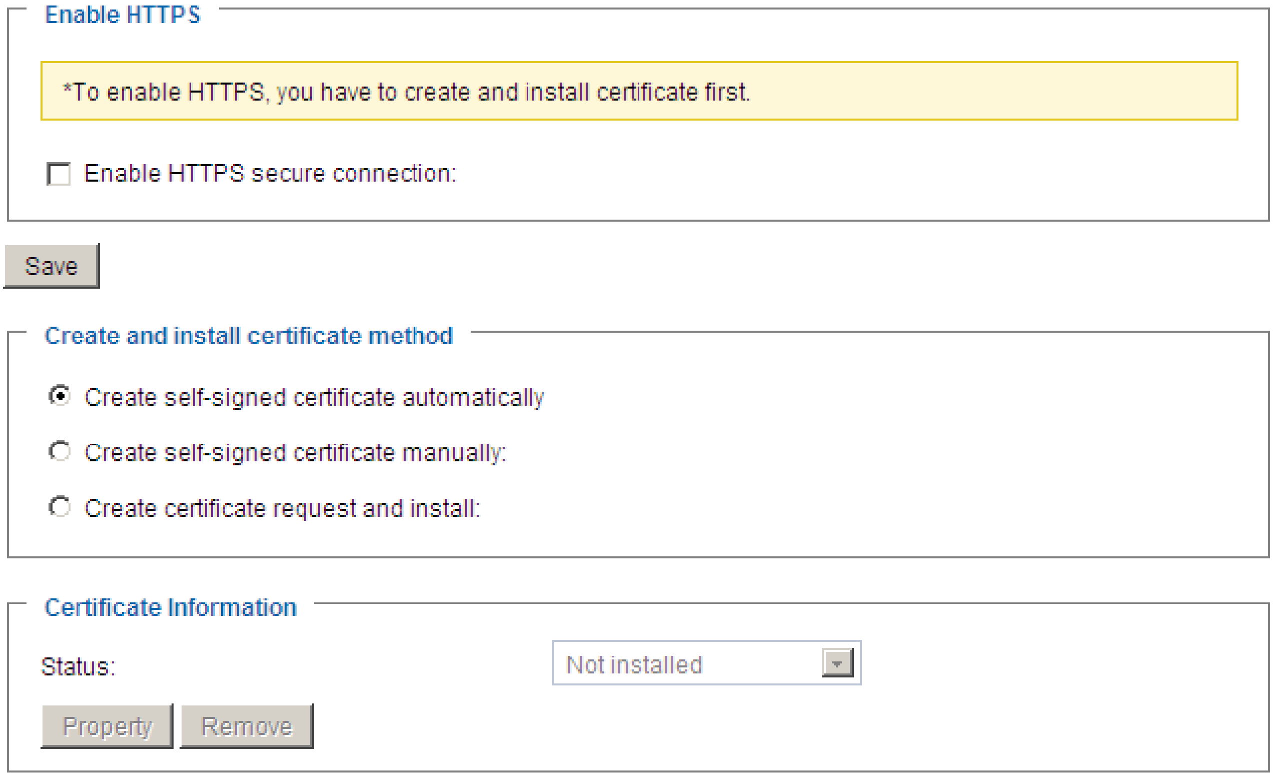
User administration

Administrator: Complete unrestricted access to the video server.
Operator: No access to the configuration page. Can also execute URL commands (e.g. PTZ).
User: Access is restricted to the main page (live view).

Digital Output: The user group can control the alarm input and output.
PTZ control: The user group has access to the PTZ control.
Allow anonymous viewing: There is no prompt for a user name and password when the main page is displayed.

6.3 HTTPS

The HTTPS
protocol is used for encryption and for authenticating communication between the web server (video server) and browser (client PC) on the Internet. All data transmitted between the video server and client PC is encrypted using SSL. Apart from SSL encryption (compatible with all standard browsers), a source authorisation certificate is required in order to use HTTPS.



Enable HTTPS

*To enable HTTPS, you have to create and install certificate first.

□ Enable HTTPS secure connection:

Create and install certificate method

● Create self-signed certificate automatically

○ Create self-signed certificate manually:

○ Create certificate request and install:

Certificate Information

Status: Not installed

"Enable HTTPS secure connection" You can choose between unencrypted (HTTP) + encrypted (HTTPS) access or encrypted (HTTPS) access only.

If a secure HTTPS connection is enabled, the video server can be accessed using the following lines:
https:\\"IP-Adresse"
If you wish to stream using the HTTPS connection, use the following link:
https:\\"IP-Adresse":"HTTPS-Port\Live.sdp

Creating and installing a certificate

"Create self-signed certificate automatically" The pre-defined certificate in the video server is used. With this option, no settings can be made by users.

"Create self-signed certificate manually" A new certificate is generated. Specific data must be entered.

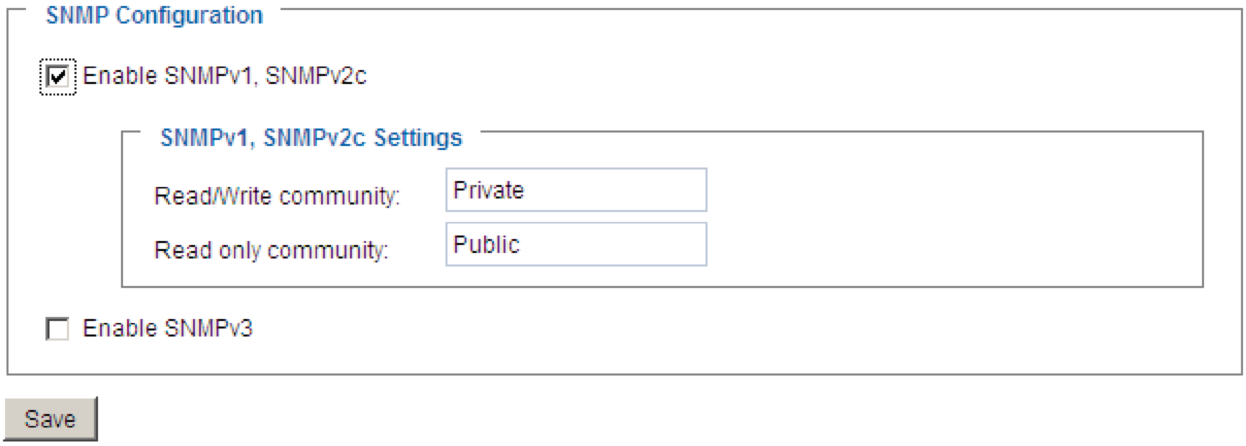
"Create certificate request and install" Select this option if you wish to generate a certificate request which is then submitted to a certificate authority. A certificate issued by a recognised certification authority (e.g. VeriSign) can also be installed on the video server.

Note: When using a "self-signed certificate", you may receive a warning message from your browser. Self-signed certificates are always classed as insecure by the browser as the source certificate and authorisation of the certification authority are both absent.

6.4 SNMP

The Simple Network Management Protocol is a network protocol that can be used to monitor and control network devices (e.g. routers, servers, switches, printers, computers etc.) from a central station. Here, the Protocol controls the communication between the monitored devices and the monitoring station. Enable this function if you are using an SNMP management server in your network. You can also access software solutions that can be installed on your PC system.

"Enable SNMPv1, SNMPv2c" Depending on your SNMP server settings, you can define the name fields of the read/write community here.



SNMP Configuration

☑ Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings

Read/Write community: Private

Read only community: Public

□ Enable SNMPv3

"Enable SNMPv3" If your SNMP server supports the SNMP protocol in version 3, you can execute the status query with encryption. To do this, an encryption algorithm and password for the read/write community status query must be saved in the video server and SNMP server.

6.5 Network

6.5.1 Network settings

All changes made on this page cause the system to restart in order for the changes to take effect. Make sure that the fields are correctly filled before you click "Save".

"LAN" The default is LAN. Use this setting if the video server is connected to a LAN. You also have to make other settings such as the IP address or the subnet mask.

"Obtain an IP address automatically" Every time the video server is restarted, it is assigned an IP address via a DHCP server.

"Use fixed IP address" The network data is fixed here, e.g. the IP address.

"IP address" This is required for network identification.

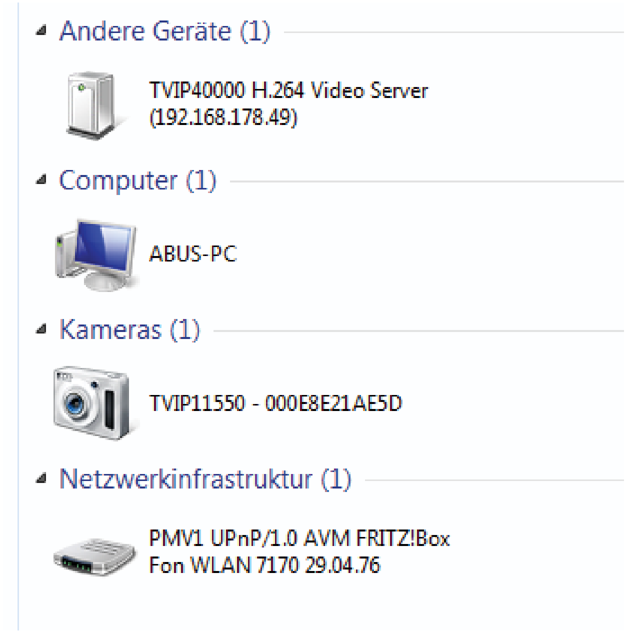
"Subnet mask" This defines whether the destination is in the same subnet. The default value is **"**255.255.255.0".

"Standard-Router" Gateway for transmitting pictures to another subnet. An invalid router setting prevents transmission to these destinations in different subnets. If a cross-link cable connection is available, you must enter an IP which is in the same subnet range as the video server (e.g. 192.168.0.1).

"Primary DNS" Server of the primary domain name with which the hostnames are converted into IP addresses.

"Secondary DNS" Server of the secondary domain name for generating a reserve copy of the primary DNS.

"Use UPnP" This enables Universal Plug and Play. If your operating system supports UPnP, the video server can be accessed directly via UPnP management (Windows: network environment)



Andere Geräte (1)

TVIP40000 H.264 Video Server
(192.168.178.49)

Computer (1)

ABUS-PC

Kameras (1)

TVIP11550 - 000E8E21AE5D

Netzwerkinfrastruktur (1)

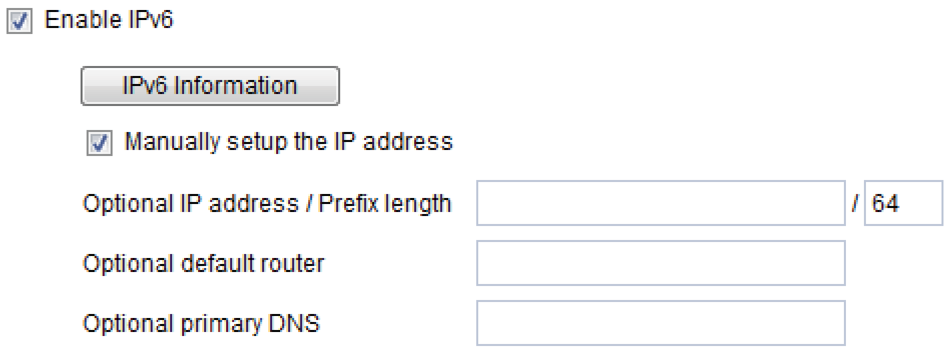
PMV1 UPnP/1.0 AVM FRITZ!Box
Fon WLAN 7170 29.04.76

⚠ Make sure that the option "Use UPnP" is always enabled. UPnP is also used by eytron VMS to search the video server.

"UPnP port forwarding ON" Enables Universal Plug and Play port forwarding for network services. If your router supports UPnP, then port forwarding for video streams is activated automatically on the router for the video server using this option.

"PPPoE" Use this setting if the video server is connected directly to a DSL modem. You will receive a user name and password from your ISP (Internet Service Provider).

"IPv6" Use this function to work with IP addresses of generation v6.



☑ Enable IPv6

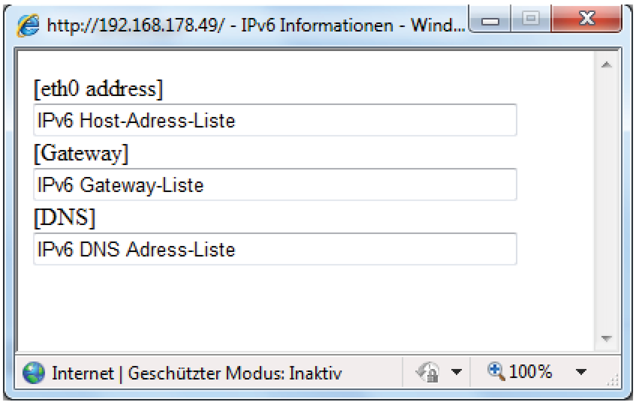
☑ Manually setup the IP address

Optional IP address / Prefix length	/ 64
Optional default router	
Optional primary DNS	

⚠ Please note that your network and hardware must support IPv6.

If IPv6 is enabled, the video server always waits until it is assigned an IPv6 address via DHCP.
If no DHCP server is available, set up the IP address manually.
To do this, enable "Manually setup the IP address" and enter the IP address, default router and DNS address.

"IPv6 Information" All the IPv6 information is displayed in a separate window.



http://192.168.178.49/ - IPv6 Informationen - Wind...

[eth0 address]

IPv6 Host-Adress-Liste

[Gateway]

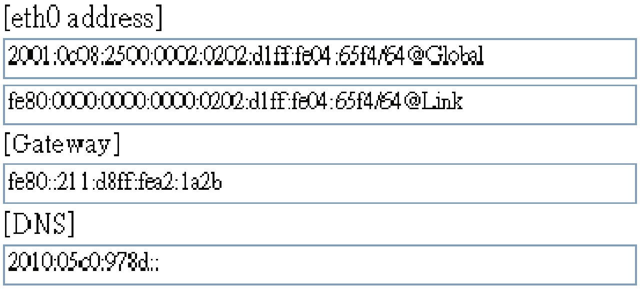
IPv6 Gateway-Liste

[DNS]

IPv6 DNS Adress-Liste

Internet | Geschützter Modus: Inaktiv
100%

If the IPv6 settings are correct, you can read all the settings in the lower window.



[eth0 address]

2001:0c08:2500:0002:0202:d1ff:fe04:65f4/64@Global

fe80:0000:0000:0000:0202:d1ff:fe04:65f4/64@Link

[Gateway]

fe80::211:d8ff:fea2:1a2b

[DNS]

2010:05c0:978d::

6.5.2 IEEE 802.1x

Activate this function if your network environment uses the standard IEEE 802.1x, a port-based access control in the network.
IEEE 802.1x improves the security of local networks.
A connection is only permitted if all certificates between the server and "client" have been verified. They are authenticated by a switch/access point, which sends queries to the RADIUS authentication server.
Otherwise no connection is made and access to the port is denied.

⚠ Please note that your network components and the RADIUS server must support the standard IEEE 802.1x.

6.5.3 HTTP

"HTTP port" This port can be different from the standard port 80 (80, or 1025 – 65535). If this port is changed, users must be informed to ensure a successful connection. Example: If the administrator changes the HTTP port of the video server with the IP address 192.168.0.99 from 80 to 8080, users have to enter "http://192.168.0.99:8080" in the web browser instead of "http://192.168.0.99".

"Secondary HTTP port" Additional HTTP port for the video server access

For the direct access to individual video streams over the web, the following access names can be configured. Access is gained via compressed JPEG images and allows web browsers (Firefox, Netscape) which cannot process ActiveX plug-ins to access the video stream directly:

"Access name for stream 1" Access name for the MJPEG stream 1
"Access name for stream 2" Access name for the MJPEG stream 2
"Access name for stream 3" Access name for the MJPEG stream 3
"Access name for stream 4" Access name for the MJPEG stream 4

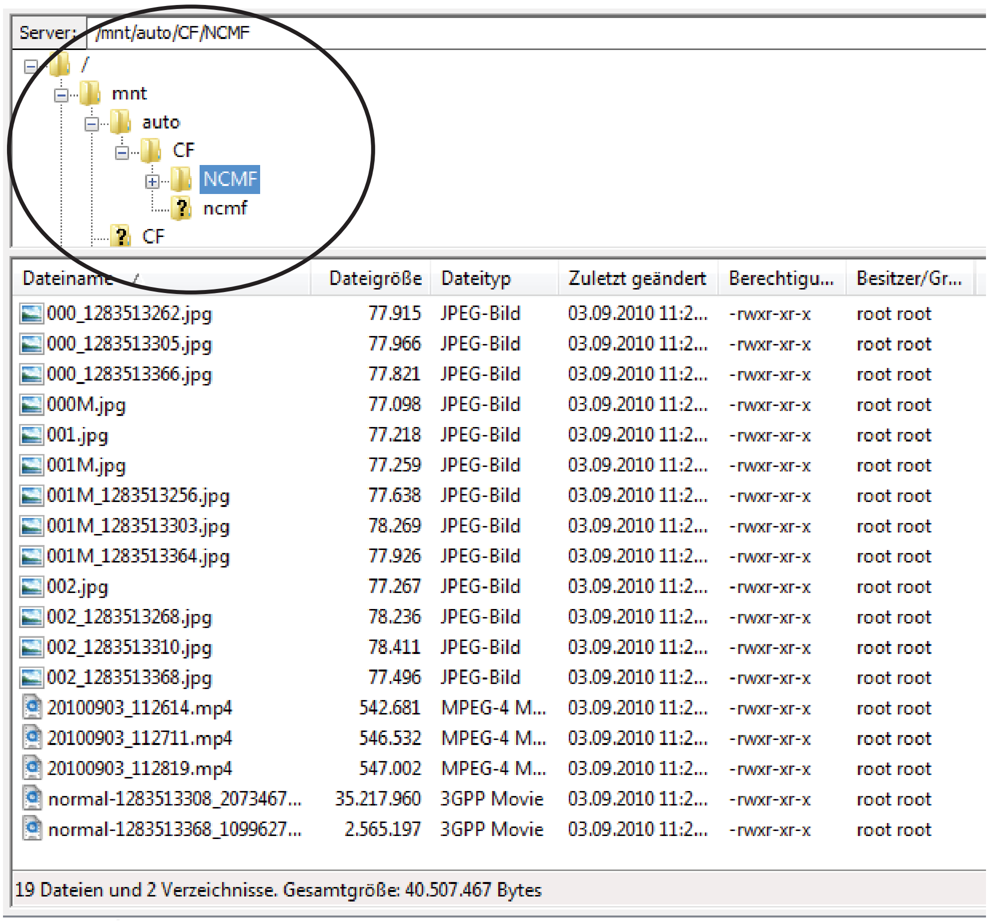
⚠ Note: Internet Explorer does not support the display of MJPEG images without Active

6.5.4 FTP

“**FTP port**” This is the internal FTP server port. It can be a different port to the standard port 21 (21, or 1025 – 65535). The video data saved on the video server can be called up directly via FTP. Use a separate FTP program for this purpose.

The address format for entering the connection data is as follows:
Server: IP address of the video server
User name: Administrator user
Password: Password of administrator
Port: FTP port of the video server

Example (with FTP program)
Server: 192.168.0.99
User name: root
Password: admin
Port: 1026



Server: /mnt/auto/CF/NCMF

```
/
  mnt
    auto
      CF
        NCMF
        ncmf
    CF
```

Dateiname	Dateigröße	Dateityp	Zuletzt geändert	Berechtigu...	Besitzer/Gr...
000_1283513262.jpg	77.915	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513305.jpg	77.966	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000_1283513366.jpg	77.821	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
000M.jpg	77.098	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001.jpg	77.218	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M.jpg	77.259	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513256.jpg	77.638	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513303.jpg	78.269	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
001M_1283513364.jpg	77.926	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002.jpg	77.267	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513268.jpg	78.236	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513310.jpg	78.411	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
002_1283513368.jpg	77.496	JPEG-Bild	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112614.mp4	542.681	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112711.mp4	546.532	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
20100903_112819.mp4	547.002	MPEG-4 M...	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513308_2073467...	35.217.960	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root
normal-1283513368_1099627...	2.565.197	3GPP Movie	03.09.2010 11:2...	-rwxr-xr-x	root root

19 Dateien und 2 Verzeichnisse. Gesamtgröße: 40.507.467 Bytes

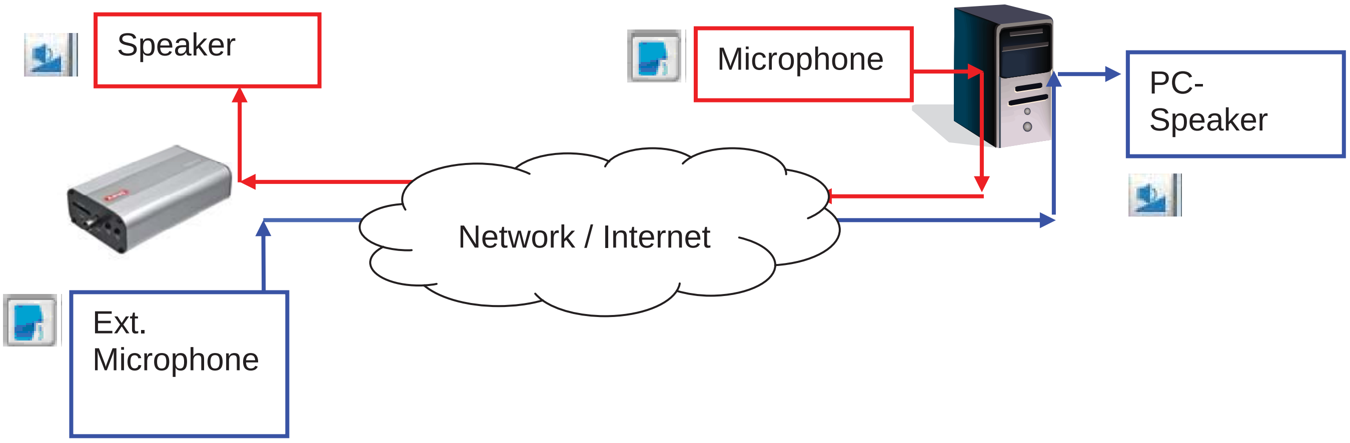
6.5.5 HTTPS

“HTTPS port” This is the port setting for the internal HTTPS port. It can be a different port to the standard port 443 (443, or 1025 – 65535). You can find further configuration options for HTTPS in section 5.5.3.

6.5.6 Two-way audio

“Two-way audio” This is the port for the two-way audio function. This port can be different from the standard port 5060 (5060 or 1025 – 65535).

To be able to use the two-way audio function, you must enable **“Video and audio”** for the selected video stream MPEG-4/H.264. MJPEG only supports the transmission of video data and is therefore not suitable for this function.



Live stream functions:

Start the audio data transmission.

Control the sensitivity of the video server audio input.

Switch off the microphone/audio input.

Click the button again to stop the audio transmission.

6.5.7 RTSP transmission

“RTSP authentication” The authentication options are: disable (standard), basic (simple) or an expanded mode (digest).

⚠ I If the RTSP authentication is enabled, the user name and password of a valid user (e.g. administrator) must be entered during the RTSP connection setup.
IMPORTANT: The RTSP authentication must be supported by the video player (e.g. Realplayer 10.5).

“Access name for stream 1” This is the access name 1 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 1>, to establish a connection.

“Access name for stream 2” This is the access name 2 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 2>, to establish a connection.

“Access name for stream 3” This is the access name 3 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 3>, to establish a connection.

“Access name for stream 4” This is the access name 4 for establishing a connection from a client. The codec type must be MPEG4. Use
rtsp://<IP address>:RTSP port /<access name 4>, to establish a connection.

RTSP access with VLC:
rtsp://192.168.0.99:10052/live.sdp

“RTSP port” This port can be different from the standard port 554 (554; or 1025 to 65535). If you change it, note that the input format is analogue to the HTTP port.

“RTP port for video” This port can be different from the default port 5558. The port number must always be even.

“RTCP port for video” This port must be the “RTP port for video” plus 1.

“RTP port for audio” This port can be different from the default port 5556. The port number must always be even.

“RTCP port for audio” This port must be the “RTP port for audio” plus 1.

6.5.8 Multicast transmission

Multicast is the message transmission from a single point to a group (also known as a multiple-point connection). The advantage of multicast is that messages can be transmitted simultaneously to several recipients or a closed user group without the bandwidth of the sender increasing according to the number of recipients. When using multicast, the sender only requires the same bandwidth as a single recipient. The packets are multiplied on each network distributor (switch, router).

Multicast allows data to be sent efficiently to many recipients at the same time in IP networks. This is made with a special multicast address. In IPv4, the address range 224.0.0.0 to 239.255.255.255 is reserved for this purpose.

The following multicast settings can be configured for streams 1 - 4 in the video server.

Enable **“Always multicast”** to use multicast.

“Multicast group address” Specifies a group of IP hosts which belong to this group

“Multicast video port” This port can be different from the default port 5560. The port number must always be even.

“Multicast RTCP video port” This port must be the “Multicast video port” plus 1.

“Multicast audio port” This port can be different from the default port 5562. The port number must always be even.

“Multicast RTCP audio port” This port must be the “Multicast audio port” plus 1.

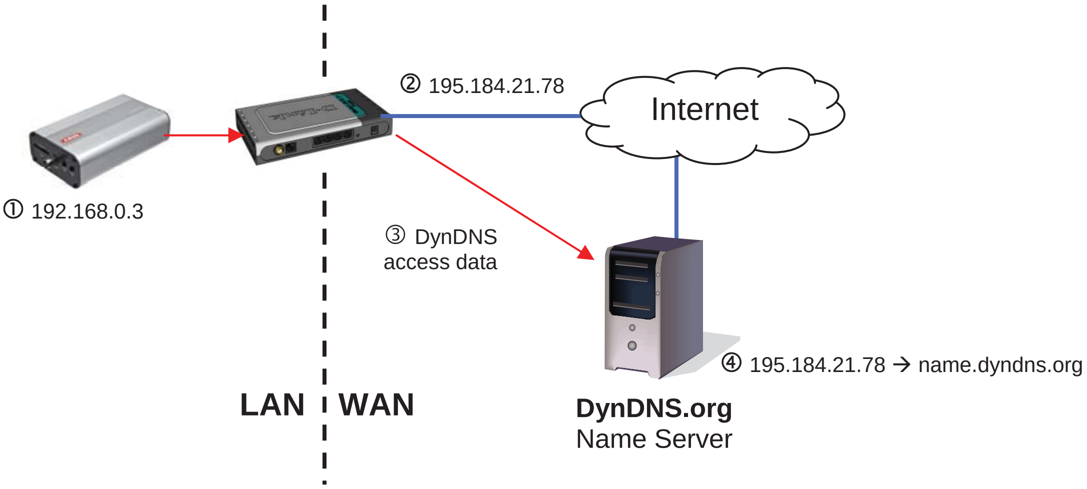
“Multicast TTL” Time to Live

⚠ If you are setting up port forwarding in a router, all ports should always be forwarded this way (RTSP + HTTP). This is imperative for successful communication.

7. DDNS

DynDNS or DDNS (Dynamic Domain Name System) is a system used for updating domain name entries in real time. The video server is equipped with an integrated DynDNS client, which updates the IP address independently via a DynDNS provider. If the video server is positioned behind a router, we recommend using the DynDNS function on the router.

The following diagram offers an overview of accessing and updating the IP address using DynDNS.



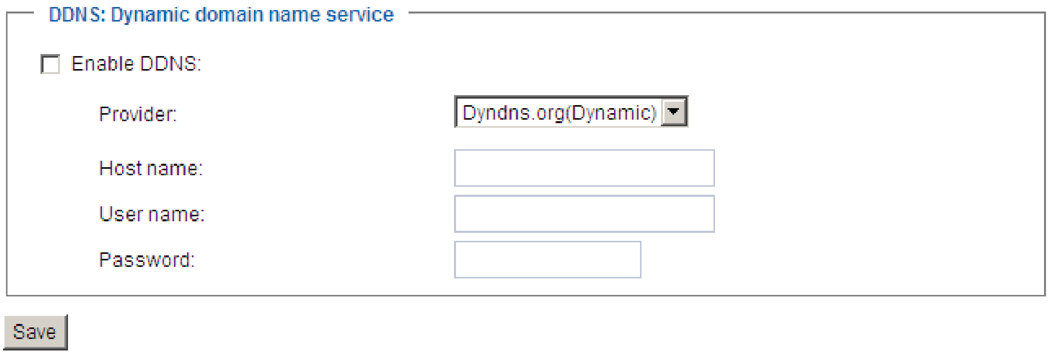
“Enable DDNS” Enables the DDNS function.

“Service providers” The provider list contains the hosts that provide DDNS services. Connect to the service provider’s website to make sure that the service is available.

“Host name” This field must be completed if you want to use the DDNS service. Enter the host name registered with the DDNS server.

“User name/email” The user name and the email address must be entered in this field to set up a connection to the DDNS server or to inform users about the new IP address. Note: If you enter a “User name” in this field, you must enter a “Password” in the next field.

“Password” To be able to use the DDNS service, enter your password in this field.

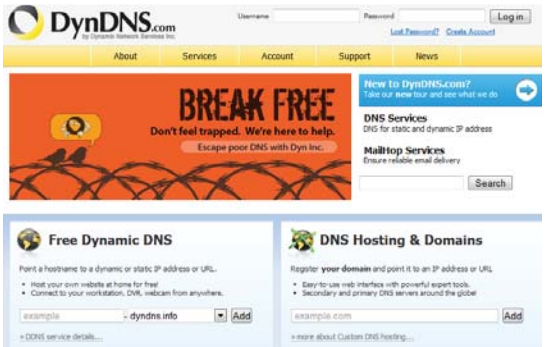

DDNS: Dynamic domain name service

□ Enable DDNS:

Provider:	Dyndns.org(Dynamic) ▾
Host name:	
User name:	
Password:	

7.1 Setting up a DDNS account

Set up a new account at DynDNS.org



DynDNS.com by Dynamic Network Services Inc.

Username Password Log in

Lost Password? Create Account

About Services Account Support News

BREAK FREE

Don't feel trapped. We're here to help.

Escape poor DNS with Dyn Inc.

New to DynDNS.com? Take our **new** tour and see what we do

DNS Services
DNS for static and dynamic IP address

MailHop Services
Ensure reliable email delivery

Search

Free Dynamic DNS

Point a hostname to a dynamic or static IP address or URL.

- Host your own website at home for free!
- Connect to your workstation, DVR, webcam from anywhere.

example - dyndns.info Add

» DDNS service details...

DNS Hosting & Domains

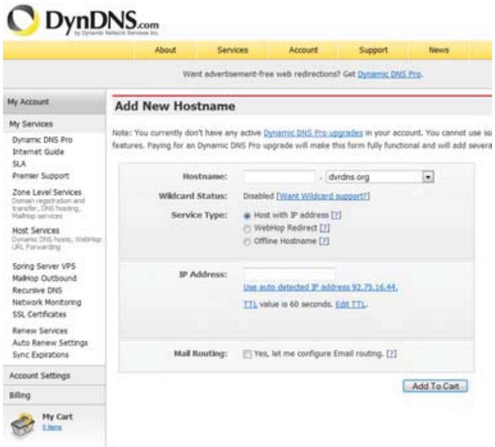
Register **your domain** and point it to an IP address or URL

- Easy-to-use web interface with powerful expert tools.
- Secondary and primary DNS servers around the globe!

example.com Add

» more about Custom DNS hosting...

Save the account information



DynDNS.com by Dynamic Network Services Inc.

About Services Account Support News

Want advertisement-free web redirections? Get Dynamic DNS Pro.

My Account

My Services
Dynamic DNS Pro
Internet Guide
SLA
Premier Support
Zone Level Services
Domain registration and transfer, DNS hosting, MailHop services
Host Services
Dynamic DNS hosts, WebHop URL Forwarding
Spring Server VPS
MailHop Outbound
Recursive DNS
Network Monitoring
SSL Certificates
Renew Services
Auto Renew Settings
Sync Expirations

Account Settings

Billing

My Cart
1 Item

Add New Hostname

Note: You currently don't have any active Dynamic DNS Pro upgrades in your account. You cannot use so features. Paying for an Dynamic DNS Pro upgrade will make this form fully functional and will add severa

Hostname:	. dyndns.org
Wildcard Status:	Disabled [Want Wildcard support?]
Service Type:	● Host with IP address [?] ○ WebHop Redirect [?] ○ Offline Hostname [?]
IP Address:	Use auto detected IP address 92.75.16.44. TTL value is 60 seconds. Edit TTL.
Mail Routing:	□ Yes, let me configure Email routing. [?]

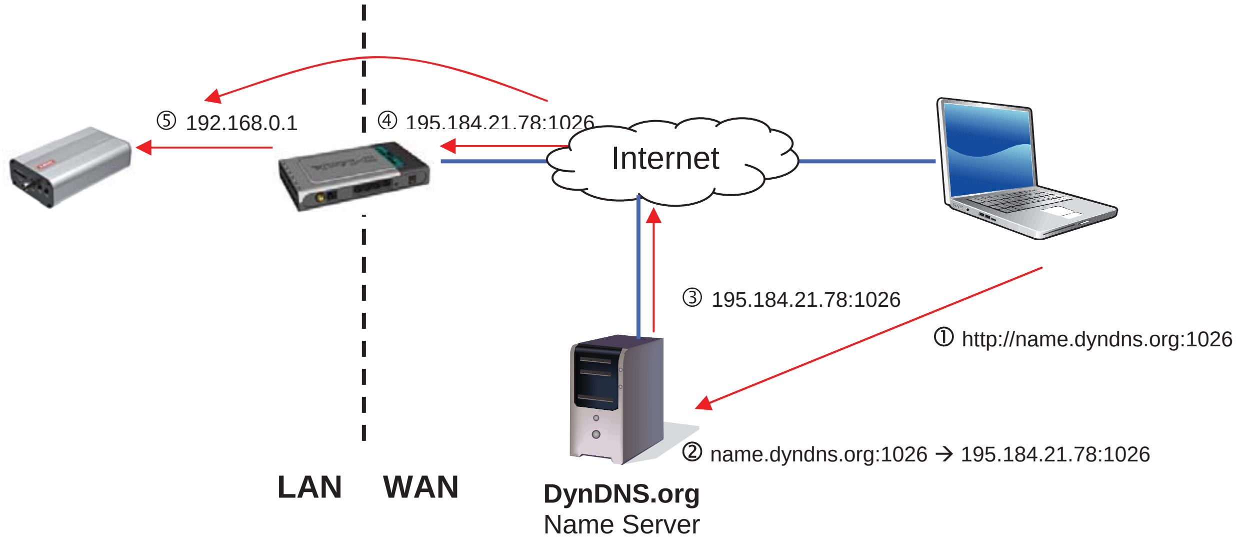
Add To Cart

Note down your user data and enter this into the configuration of the video server.

7.2 DDNS access via a router

If your network video server is positioned behind a router, then access via DynDNS must be configured in the router. A description of the DynDNS router configuration for common router models can be found on the ABUS Security-Center website: www.abus-sc.com.

The following diagram offers an overview of accessing a video server behind a router via DynDNS.org.



Port forwarding of all relevant ports (at least RTSP + HTTP) must be set up in the router in order to use DynDNS access via the router.

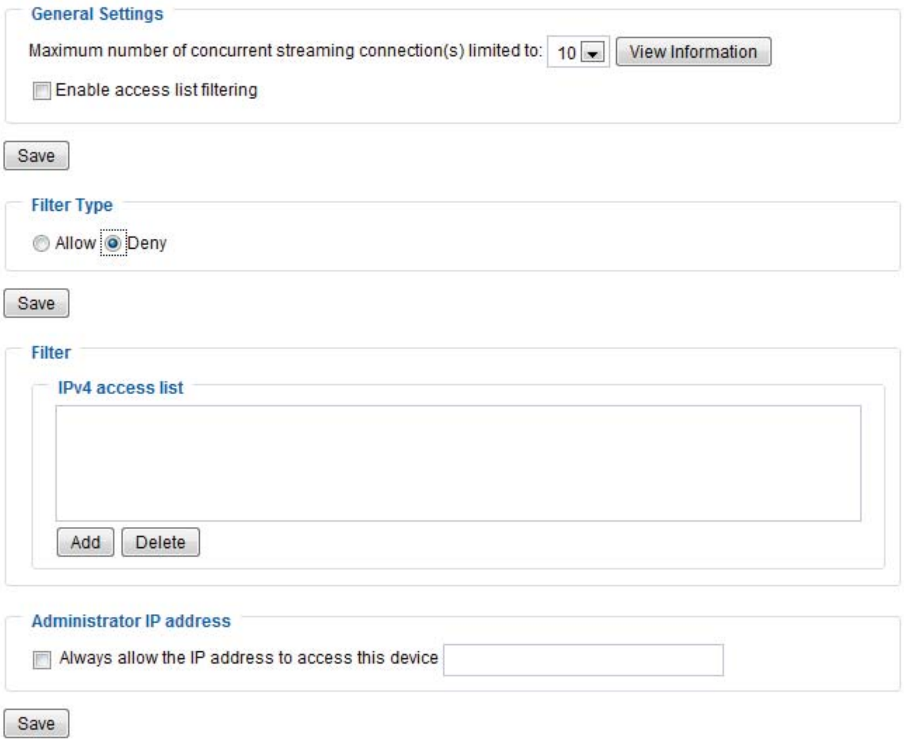
8. Access list

This is where you control access to the video server using IP address lists.

“Maximum number of concurrent streaming connection(s) limited to” Number of possible simultaneous connections to the video server. Depending on the bandwidth available for the video server, it may make sense to limit the access.
“Enable access list filtering” Enables the IP address filters listed defined under “Filters”
You have two options for defining IP address filtering:

- “Allow” filter type: only IP addresses in the defined address space have access, or
- “Deny” filter type: IP addresses in the defined address space have no access.

Click **“Add”** to configure the address ranges. The following configuration options are given:



Maximum number of concurrent streaming connection(s) limited to: 10

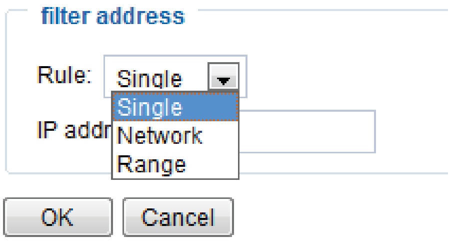
□ Enable access list filtering

○ Allow ● Deny

□ Always allow the IP address to access this device

Rule: Single, Range, Network:

- Single: a specific IP address is added
- Range: IP address ranges from - to can be defined
- Network: IP addresses with a specific subnet mask can be defined



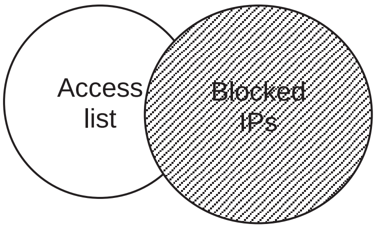
Rule: Single

IP addr

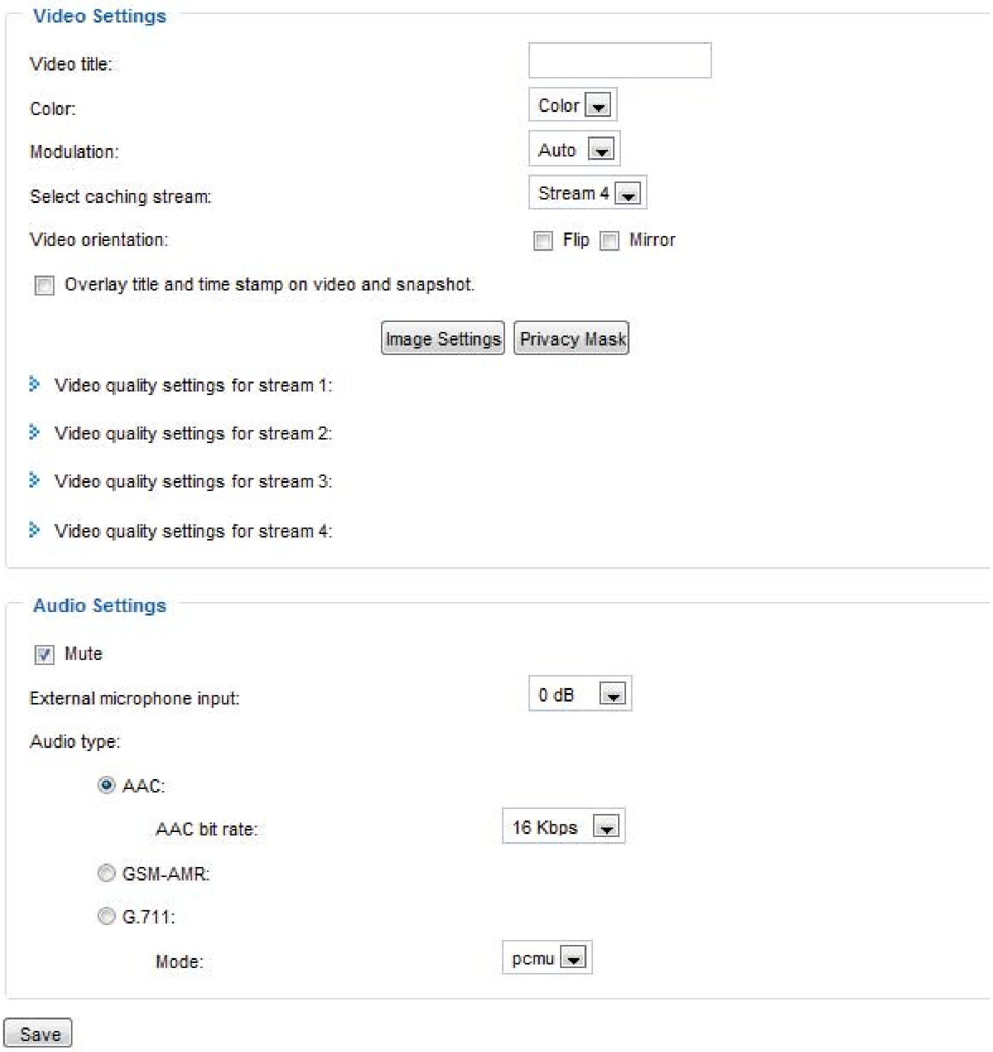
Example:
The IP address range from 192.168.0.1 to 192.255.255.255 should be permitted.
The following IP addresses should be blocked 192.168.1.0 to 192.168.255.255.

Result:
Access is only granted for IPs from the following range: 192.168.0.1 – 192.168.0.255.

An intersection is formed between IPs which are allowed access and denied access.



9. Audio and Video



Video Settings

Video title:

Color: Color

Modulation: Auto

Select caching stream: Stream 4

Video orientation: □ Flip □ Mirror

□ Overlay title and time stamp on video and snapshot.

Video quality settings for stream 1:

Video quality settings for stream 2:

Video quality settings for stream 3:

Video quality settings for stream 4:

Audio Settings

☑ Mute

External microphone input: 0 dB

Audio type:

● AAC:

AAC bit rate: 16 Kbps

○ GSM-AMR:

○ G.711:

Mode: pcmu

“Video title” The text appears in the black bar above the video window with a timestamp. This timestamp (date and time) is provided by the integrated realtime clock of the video server.

“Colour” Choose between colour and black and white display.

“Modulation” Select between the video standard NTSC and PAL or automatic video signal recognition via the video server.

“Select caching stream” The selected video stream is used for recording the pre- and post-alarm video data (see “Application” section).

“Flip” Rotates the video horizontally. Select this option if the camera has been installed upside down.

“Mirror” Rotates the video vertically.

⚠ Select the flip and mirror options if the camera is installed on the ceiling.

“Overlay title and time stamp on video and snapshot” You can use this option to display the title and time stamp directly in the video image and snapshots. The input for “Video title” is used here.

9.1 Image Settings

“Brightness, contrast, saturation, sharpness” Adjust the values according to your lighting conditions.

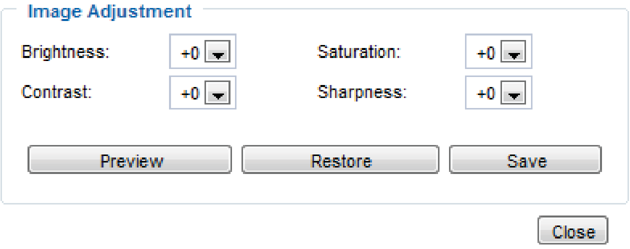


Image Adjustment

Brightness: +0

Saturation: +0

Contrast: +0

Sharpness: +0

⚠ If the lighting conditions for the camera change, image settings for bad lighting conditions may compromise the image quality of videos with good lighting conditions.

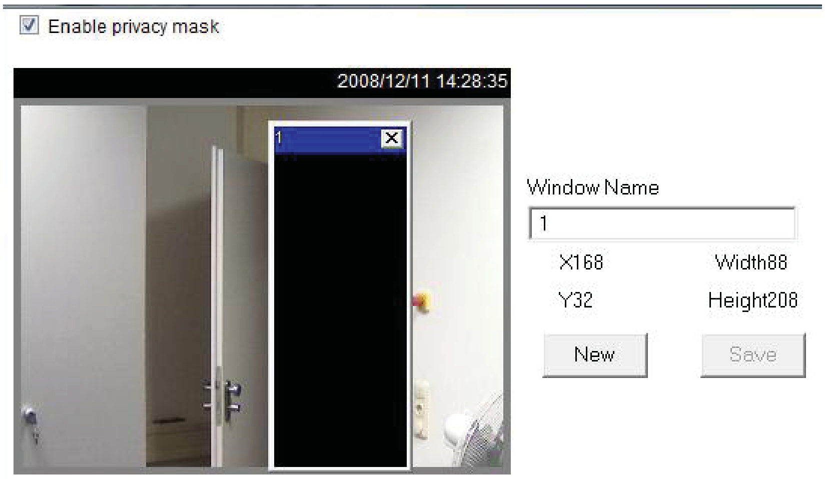
To view the changed settings for the image, click “Preview”. To save the picture parameters, click “Save”. To discard your changes, click “Restore”.

9.2 Privacy masking zones

This function allows you to hide areas in the video image. You can select 5 areas of any size.

Enable this function by selecting the **“Enable privacy mask”** option.

Click **“New”** to create a new window; you can then adjust the size. Click **“Save”**, to apply the changes.



☑ Enable privacy mask

2008/12/11 14:28:35

Window Name: 1

X168 Width88

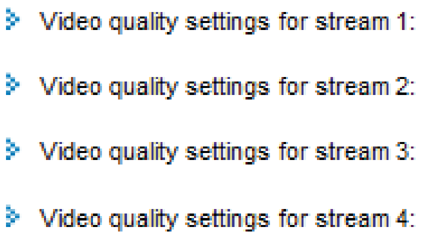
Y32 Height208

⚠ This function should not be enabled if the PTZ/ePTZ function of the camera is being used. This function can only be configured if MS Internet Explorer is used as a browser (ActiveX mode).

9.3 Basic setting:

Video options

The video server has four video streams with different quality settings available for flexible application.



- Video quality settings for stream 1:
- Video quality settings for stream 2:
- Video quality settings for stream 3:
- Video quality settings for stream 4:

Settings for streams 1, 2, 3 and 4
You can configure streams 1 – 4 in the respective menus.

⚠ The quality settings for stream 4 is determined on QCIF. Use stream 4 for streaming on mobile devices.

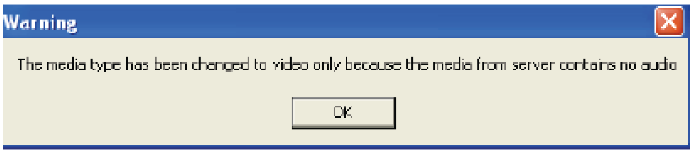
"Image compression" Select from H.264/MPEG-4/MJPEG.
"Image size" Select your desired resolution here.
"Max. image rate" Select your maximum refresh rate here.
"Key frame interval" Determines how often an Intra Frame is generated. The shorter the interval, the better the image quality, and the higher the network usage costs.
"Video quality fixed image rate" Sets the image rate at a constant value. The image quality is reduced the more complex an image is (e.g. motion).
"Fixed image quality" Sets the image quality at a constant value. The bit rate increases with the image complexity (e.g. motion).

Compression → Recording duration ↓	**H.264**	**MPEG-4**	**MJPEG**
1 minute video sequence in D1 resolution with "good" quality	Approx. **12** MB	Approx. **14** MB	Approx. **60** MB
Storage capacity **32 GB** SD card	Approx. **43** hours	Approx. **36** hours	Approx. **9** hours

⚠ At the end of the manual you can find a detailed table with every quality setting combined with every resolution.

9.4 Audio settings

“Mute” All audio functions in the video server are deactivated. A note appears when you access the video server.



Warning

The media type has been changed to video only because the media from server contains no audio

“External microphone/audio amplification” Adjust the value from +21 db to -33 db.

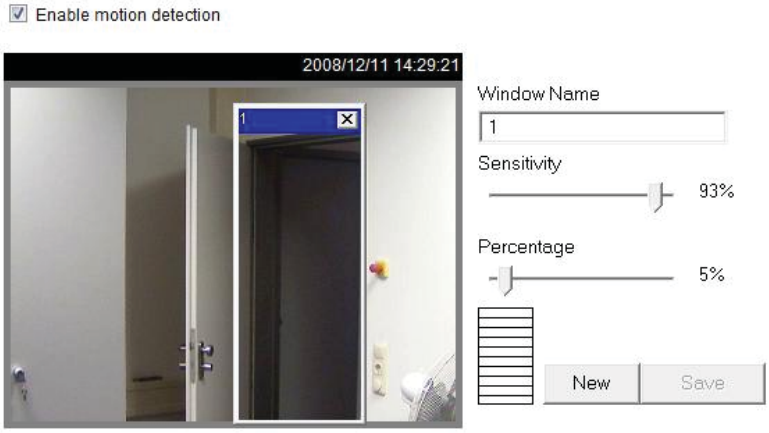
“Audio type” Select the audio type and desired bit rate. A higher value requires more bandwidth:

- **“AAC”** (Advanced Audio Coding) Special codec for audio data compression under MPEG-4/H.264.
- “**GSM-AMR”** (Global System for Mobile Communications – Adaptive Multi Rate) Voice codec in GSM mobile telephone network.
- **“G.711”** pmca/pmcu (Pulse Code Modulation).

10. Motion detection

You can activate up to three motion zones in the video server. Select “**Enable motion detection**”, to configure the function.

The motion detection function is only active once you have defined an action under the “Application” menu item.



☑ Enable motion detection

Window Name: 1

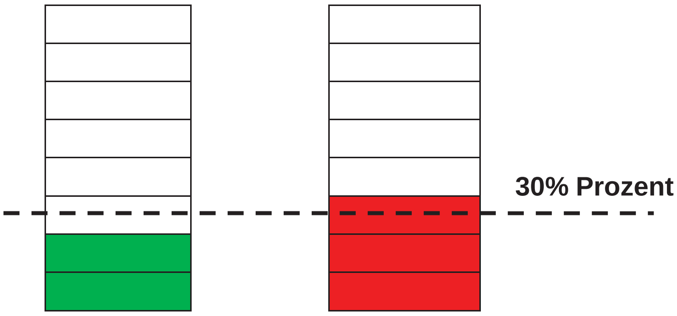
Sensitivity: 93%

Percentage: 5%

“**Window Name**” The text appears at the top of the window.
“**Sensitivity**” Sensitivity in changes of picture sequence (e.g.: sensitivity high: triggering by slight picture change).
“**Percentage**” Specifies the percentage of the image that has to change for the motion sensor to be triggered.

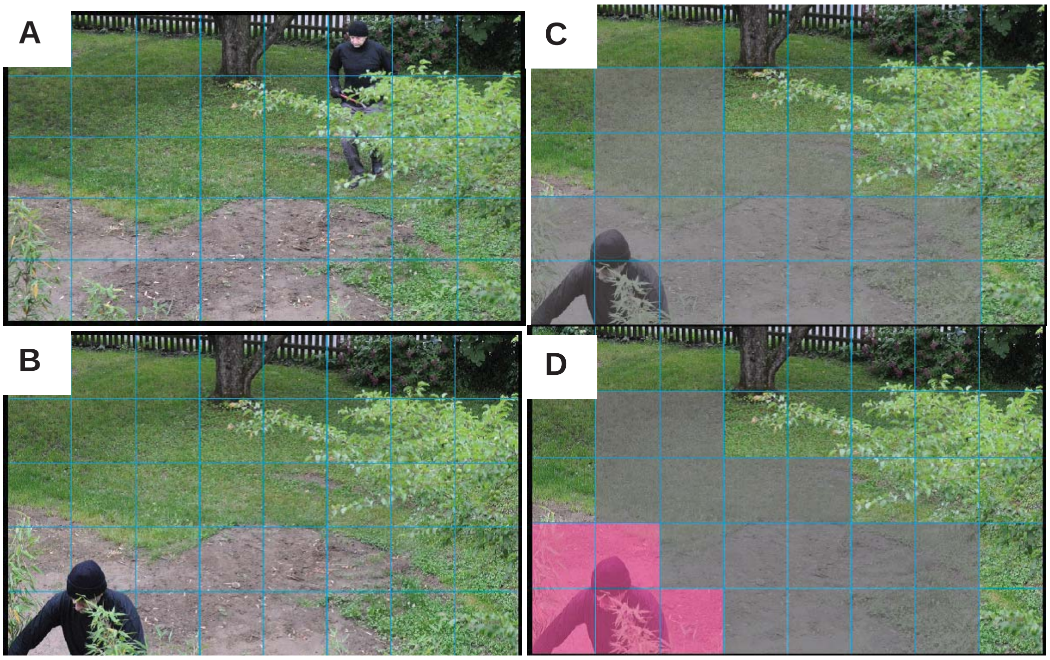
Click “New” to add a new window. To resize the window or move the title bar, click the window frame, keep the mouse button pressed and drag the window to the required size. Close the window by clicking the “x” in the top right corner.
Click “Save” to save the window settings. A bar graph rises or falls according to the picture variation.

A green bar means that the picture variation is below the surveillance level, whilst a red bar means that the picture variation is above the surveillance level. If the bar is red, the detected window appears with a red frame. When you return to the homepage, the monitored window is hidden. As soon as motion is detected, the red frame is displayed.



Green area: Motion recognised, however alarm is not triggered.
Red area: Picture variation (motion) exceeds the limit value of 30% and triggers an alarm.

Functionality of motion detection:



Two parameters are available for configuring motion detection: **Sensitivity** and **percentage**. The figure shows how these two parameters influence motion detection.

A motion occurs, shown in the progression from figure A to figure B. The resulting pixel changes (depending on the sensitivity setting) are shown in figure C (grey). The **"Sensitivity"** setting refers to the capacity of the sensor to detect motion in the picture. The higher the set value, the more pixel changes are detected in the picture. When motion is detected, the pixel changes (depending on the sensitivity setting) are saved on the server as alarm pixels (pink areas in figure D). The **"Percentage"** value describes the percentage of the "alarm pixels" in relation to the total number of pixels in the selected area. If the specified percentage of alarm pixels is reached or exceeded, an alarm is triggered. To ensure reliable motor detection, a high sensitivity setting and low percentage value is recommended.

11. Camera tampering detection

The video server supports tampering detection. If detection is enabled, the alarm can be used as an event for a notification (see “Application”).

“Enable video server tampering detection” The sensor system is activated.

“Triggering behaviour” The period defines how long a tampering event must continue before an alarm is triggered.

The following tampering events are checked:

- Camera rotation
- Camera masking
- Camera defocussing

⚠ You can set tampering detection as a trigger in the camera function “Application/Event setup”.

12. Camera control

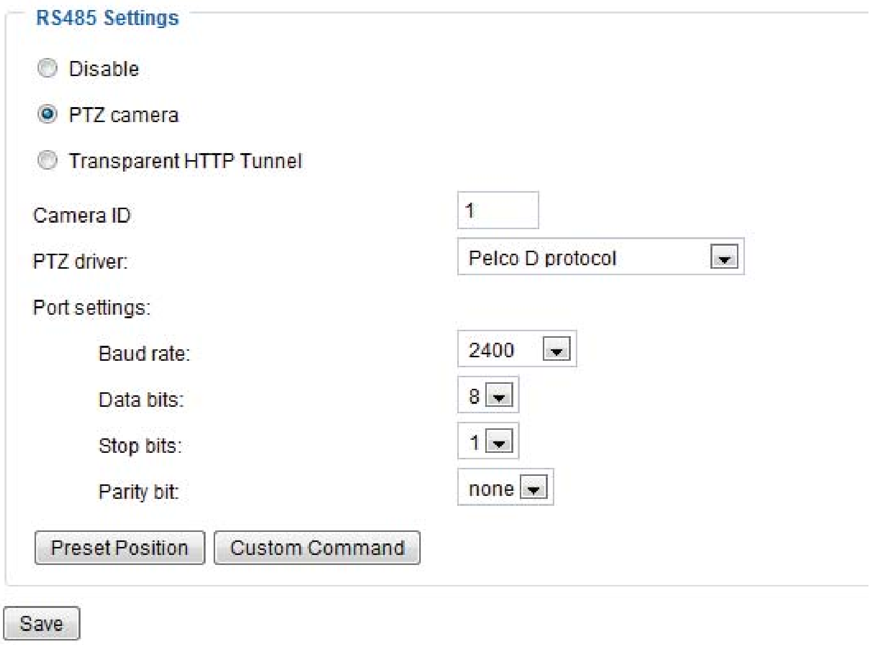
The video server includes an option for analogue PTZ camera control.

RS485 Settings

“Disable” RS485 control is switched off.

“PTZ camera” Here, enter the relevant parameters for the PTZ camera. The following protocols are supported: Pelco-D, Pelco-P, Samsung scc643, DynaDome/SmartDOME, Lilin PIH-7x00.
If none of these protocols are supported by your PTZ camera, select “Custom camera”.

“Transparent HTTP Tunnel” If your PTZ device supports RS485 commands via a network interface, you can select this option. Refer to the operating manual of your PTZ device for the necessary parameters.



RS485 Settings

○ Disable

● PTZ camera

○ Transparent HTTP Tunnel

Camera ID	1
PTZ driver:	Pelco D protocol
Port settings:	
Baud rate:	2400
Data bits:	8
Stop bits:	1
Parity bit:	none

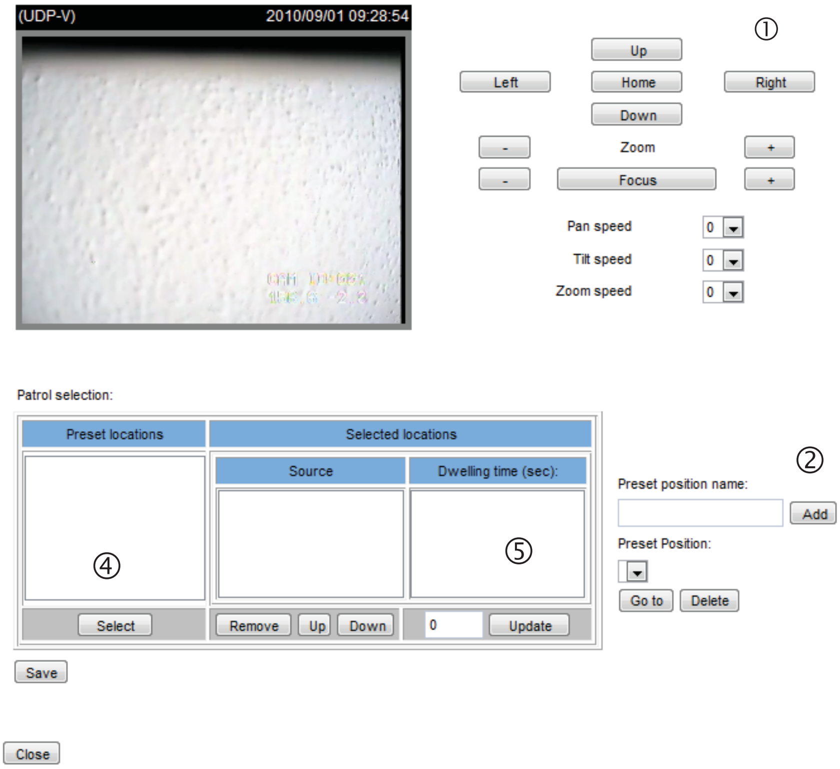
Refer to the operating manual of your PTZ device for the exact PTZ commands.

“Camera ID” Defines the camera ID.
“PTZ driver” Defines the protocol of the connected PTZ device.
“Baud rate” Enter the appropriate baud rate.
“Data bits” Enter the appropriate data bits.
“Stop bits” Enter the appropriate stop bits.
“Parity bit” Defines the parity.

Preset positions and setting up a patrol

Up to 20 preset positions can be saved in the video server. Proceed as follows:

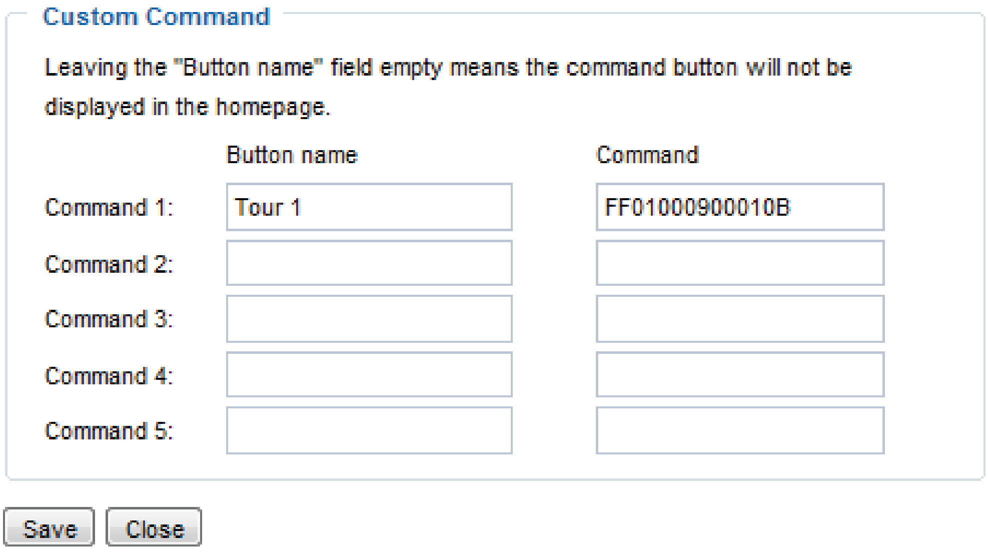
1. Move the camera picture into the desired position using the direction keys
2. Give the current position a preset name and click “Add”. The name appears in the preset locations list Wiederholen Sie die
3. Repeat steps 1-2 to add more preset locations
4. Highlight the preset locations that you wish to use for a patrol, and confirm these with “Select”
5. Adjust the dwelling time for each of the preset locations if required.
6. Save your settings



To begin the patrol, press “PATROL” in the live picture of the video server. Press “STOP” to stop this).

Custom command

The “Custom Command” menu item allows you to access individual functions of your PTZ device or PTZ camera directly.
This function is usually used to call up saved preset locations or pre-defined patrols.



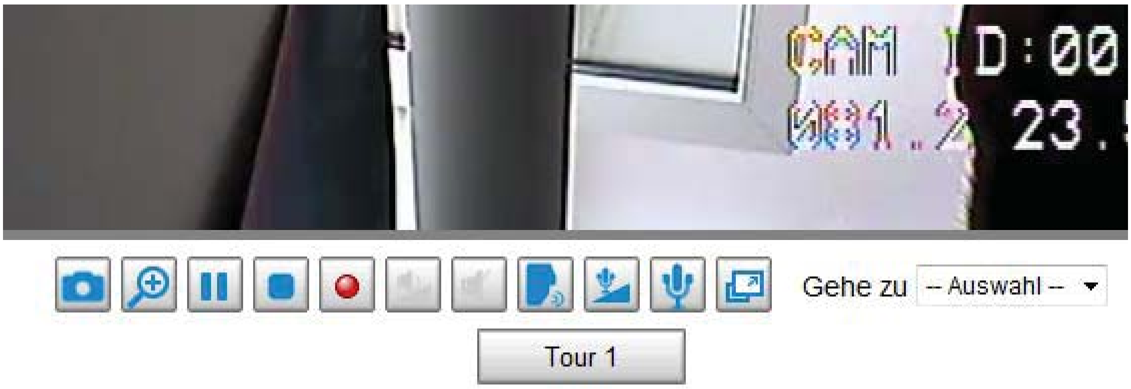
Custom Command

Leaving the "Button name" field empty means the command button will not be displayed in the homepage.

	Button name	Command
Command 1:	Tour 1	FF01000900010B
Command 2:		
Command 3:		
Command 4:		
Command 5:		

Save Close

You can use this function to create your own command buttons for operating and setting the connected PTZ device in the live picture of the video server.
The specific button function is described using a hexadecimal code (depending on the applicable PTZ protocol).
All ABUS speed-dome cameras use the PELCO D/P protocol.
Up to 5 user-defined buttons can be created.
Enter the desired name of the button (e.g. Tour 1) under “Button name”.



⚠ If you entered “Custom camera” as the camera protocol, you must define basic functions such as “up”, “down”, “left” and “right” as custom commands. Refer to the manual for the PTZ device for the applicable codes.

⚠ If you do not specify a button name, the button will not appear in the live picture.

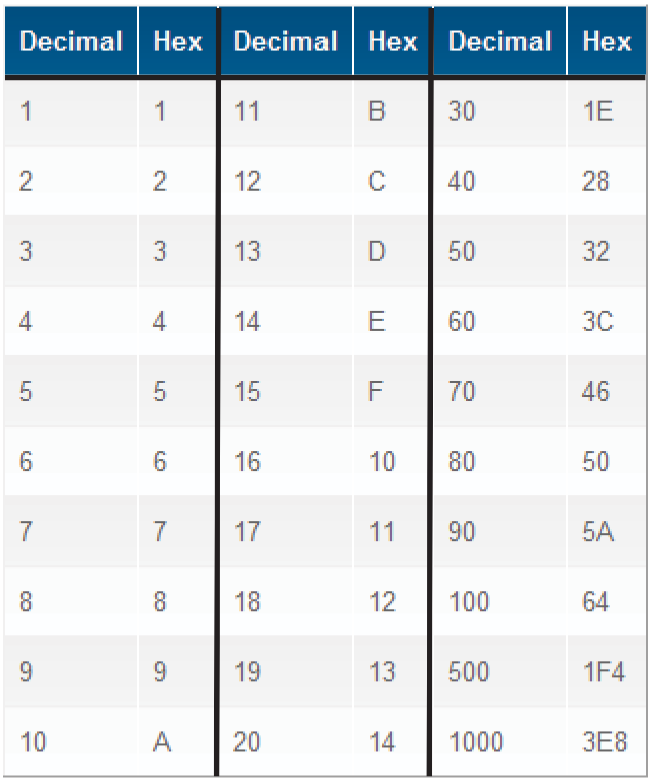
⚠ The Pelco D/P protocol functions only with hexadecimal numbers.

Enter the HEX code for the desired function under "Command"
(e.g.: FF 01 00 09 00 01 0B**).**

⚠ The code must not include any spaces or special characters.
FF 01 00 09 00 01 0B → FF01000900010B

Preface to hexadecimal numbers

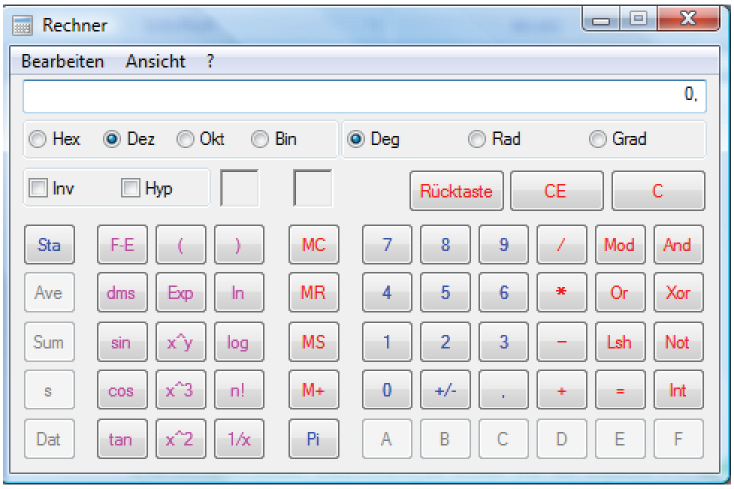
In the following chapter, a number of examples are used to explain the hexadecimal number system.



Decimal	Hex	Decimal	Hex	Decimal	Hex
1	1	11	B	30	1E
2	2	12	C	40	28
3	3	13	D	50	32
4	4	14	E	60	3C
5	5	15	F	70	46
6	6	16	10	80	50
7	7	17	11	90	5A
8	8	18	12	100	64
9	9	19	13	500	1F4
10	A	20	14	1000	3E8

The hexadecimal number system is based on numbers from 0-9 and letters from A-F. Note that the hexadecimals are added for the calculation of checksums.

An useful aid for converting decimal into hexadecimal numbers and adding hexadecimals is the Microsoft Windows calculator, which should be set to “Scientific” mode.



0,

○ Hex ● Dez ○ Okt ○ Bin

● Deg ○ Rad ○ Grad

□ Inv □ Hyp

Dome control commands for TV7600, TV6702, TV7604 (Pelco)

Command structure

Word 1	Word 2	Word 3	Word 4	Word 5	Word 6	Word 7
Synch byte (always FF)	Address (ID of the analogue camera)	Command 1	Command 2	Data 1	Data 2	Checksum word 2-6

Checksum calculation:

Word 7= word 2 + word 3 + word 4 + word 5 + word 6

Word explanation:

”Word1” is always “FF”
“Word2” is the ID of the analogue camera
“Word3”–“Word4” define the different PTZ functions (“save preset”, “start patrol” etc.)
“Word5”–“Word6” define e.g. the numbering of the preset locations and patrols.
If you wish to go to a preset location, you also have to define which preset location number is to be selected.
“Word7” is the sum of words 2-6, and is also referred to as the checksum

Example: “Go to preset location 1” has the command: FF 01 00 07 00 **01** 09

Word 1 is always FF
Word 2 is always the ID of the speed dome
Word 3 and word 4 define the function: “Go to preset location”
Words 5 and 6 define the preset location to which the video server should go.
Word 7 is the checksum

Explanation: In word 6, the hex number 01 stands for preset 1.
If you would then like to go to preset location 15, you would enter 0F for word 6.

Example: “Go to preset location 15“ has the command: FF 01 00 07 00 **0F** 17
This procedure is the same when selecting patrols or other calculable function structures.

Do not forget to recalculate the checksum every time the command is changed.
In the above example, changing the command from preset 1 to preset 15 resulted in the checksum increasing by 14.

Overview of commands:

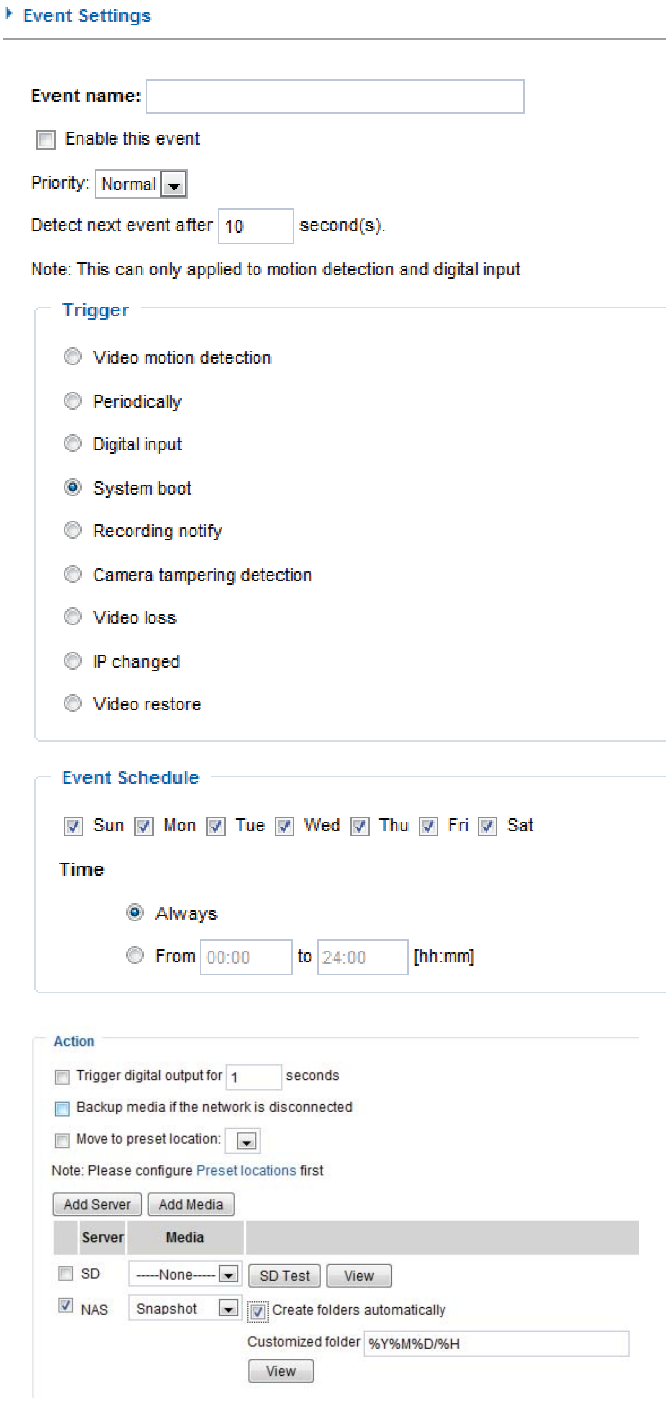
Command	Word 3	Word 4	Word 5	Word 6
Down	00	10	00	2A
Up	00	08	00	3C
Rotate Left	00	04	2E	00
Rotate Right	00	02	06	00
Stop	00	00	00	00
Menu	00	11	00	00
Start Patrol	00	00	09	01 to 08
Scan	00	0F	00	01
Zoom Out	00	20	00	01
Zoom Wide	00	40	00	01
Focus Near	01	00	00	01
Focus Far	00	80	00	00
Iris Close	04	00	00	00
Iris Open	02	00	00	00
Save Preset	00	03	00	01 to C8
Delete Preset	00	05	00	01 to C8
Go to Preset	00	07	00	01 to C8
Set Auxiliary	00	09	00	01 to 08
Clear Auxiliary	00	0B	00	01 to 08
Remote Reset	00	0F	00	00
Set Zone Start	00	11	00	01 to 08
Set Zone End	00	13	00	01 to 08
Write Char. To Screen	00	15	X Position 00 to 28	ASCII Value
Clear Screen	00	17	00	00
Alarm Acknowledge	00	19	00	Alarm No.
Zone Scan On	00	1B	00	00
Zone Scan Off	00	1D	00	00
Set Pattern Start	00	1F	00	00
Set Pattern Stop	00	21	00	00
Step Through Pattern	00	23	00	00
Set Zoom Speed	00	25	00	00 to 03
Set Focus Speed	00	27	00	00 to 03
Camera Default Setting	00	29	00	00
Auto Focus auto/on/off	00	2B	00	00-02
Auto Iris auto/on/off	00	2D	00	00-02
AGC auto/on/off	00	2F	00	00-02
BLC on/off	00	31	00	01-02
Auto White Balance on/off	00	33	00	01-02

13. Application

This allows you to automate tasks in the video server. The application configuration comprises 3 sections: event, server and medium. A typical application example may look like the following: due to motion detection (event), an email (server) with an alarm picture (medium) is sent to a user.

Event setup
Click **“Add”** to create a new event. Up to 3 events can be set.

“Event name” Assign a unique name to the event, under which the event configuration is to be saved
“Enable this event” Select this option to activate the programmed result.
“Priority” Events with higher priority are completed first
“Detect next event after” Time between events to be executed (e.g.: with motion detection)



Event Settings

Event name:

□ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Note: This can only applied to motion detection and digital input

Trigger

○ Video motion detection
○ Periodically
○ Digital input
● System boot
○ Recording notify
○ Camera tampering detection
○ Video loss
○ IP changed
○ Video restore

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always
○ From 00:00 to 24:00 [hh:mm]

Action

□ Trigger digital output for 1 seconds
□ Backup media if the network is disconnected
□ Move to preset location:

Note: Please configure Preset locations first

	Server	Media	
□	SD	-----None-----	SD Test View
☑	NAS	Snapshot	☑ Create folders automatically Customized folder %Y%M%D/%H View

13.1 Trigger settings

“Video motion detection” Activate the desired motion window.
“Periodically” The event is triggered periodically. Maximum setting is 999 minutes.
“Digital input” Triggered if a signal is present at the alarm input (e.g.: door contact).
“System boot” Event is triggered when the system is rebooted (after a power failure).
“Recording notify” If the destination storage (medium) is full or if a cyclic recording is overwritten, an alarm is triggered.
“Camera tampering detection” An alarm is triggered if the system detects that the connected analogue camera has been tampered with.

“Video loss” An alarm is triggered if the video signal is interrupted.
“IP changed” As long as a new IP address is assigned to the video server, an alarm is triggered.
“Video restore” Triggered when the video signal is restored following a malfunction.

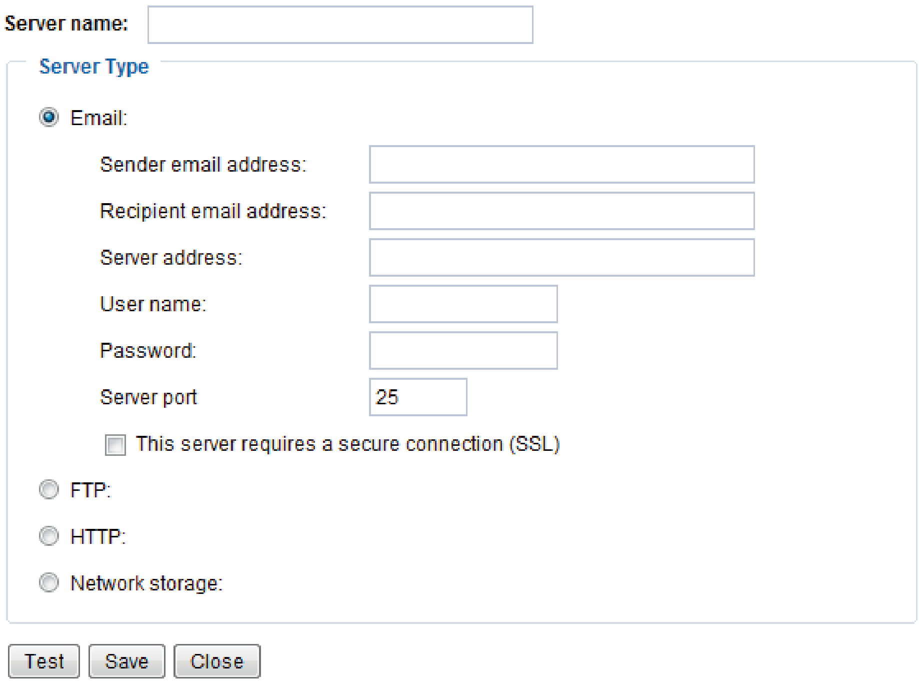
Event schedule

“**Sun**” – “**Sat**” allows you to select the day of the week for executing an event.
“**Always**” Activates the event at all times (24 hours).
“**From**” – “**to**” The event times are restricted.

13.2 Server configuration

You can save up to 5 servers in the network camera. Click **“Add”** to configure a new server. The server of type **“SD”** is pre-configured and defines the SD card unit as the destination for saving data. You can configure the following server types:

- Email: enter the access data here
- FTP: enter the access data here. Address convention: ftp.abus-sc.com
- HTTP: enter the access data here. Address convention: http://abus-sc.com/cgi-bin/upload.cgi
- Network storage: Address convention: \\192.160.0.5\NAS



Server name:

Server Type

● Email:

Sender email address:

Recipient email address:

Server address:

User name:

Password:

Server port 25

□ This server requires a secure connection (SSL)

○ FTP:

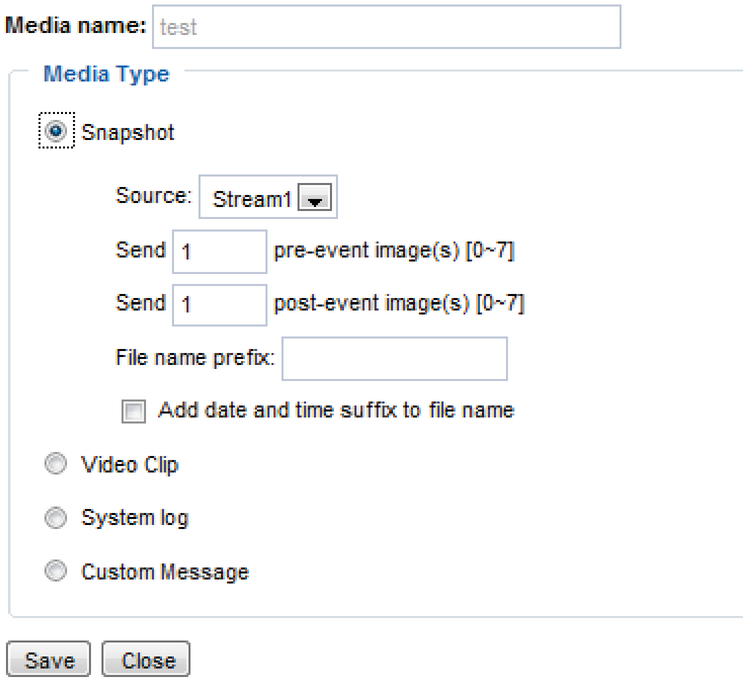
○ HTTP:

○ Network storage:

Once you have entered the access data, save your settings. Before closing the window, it is advisable to execute a **“Test”**. The result is displayed in a new window of the browser.

13.3 Media settings

You can save up to 5 media settings in the video server.



Media name: test

Media Type

● Snapshot

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix:

□ Add date and time suffix to file name

○ Video Clip

○ System log

○ Custom Message

“**Media name**” Unique name for the medium.

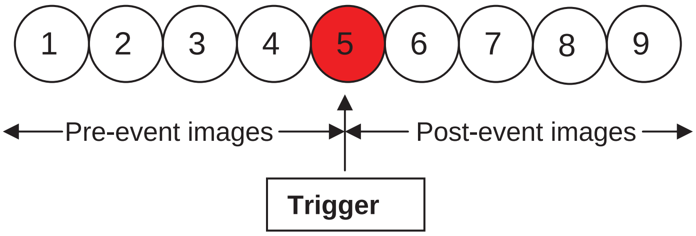
There are 4 different media types:

- Snapshot (JPEG file)
- Video clip (MP4 format)
- System log (TXT log)
- Custom message (TXT format)

Each medium that you create can only be linked with one event.
Assigning a medium twice results in the incorrect functioning of the video server.
If you wish to use the same media type for two events, you must create two separate media types beforehand.

Snapshot

“**Source**” The recording can be made from video streams 1–4.
“**Send pre-event image(s)**” Number of snapshots before an event.
“**Send post-event image(s)**” Number of snapshots after an event.



“**File name prefix**” Enter a name that will prefix the snapshot file name.
“**Add date and time suffix to file name**” Adds the date and time to the snapshot so that you can more easily distinguish between the file names of snapshots either in sequential or event-controlled operation. Example: “video@20030102_030405.jpg” means that the JPEG picture was taken on January 2, 2003 at 03:04:05 (i.e., just after 3:04 am). If you omit this suffix, the file is updated with the name “video.jpg” on the external FTP server according to the specified time interval.

The data name is structured as follows:
Prefix_YYYYMMDD_HHMMSS : ABUS_20091115_164501

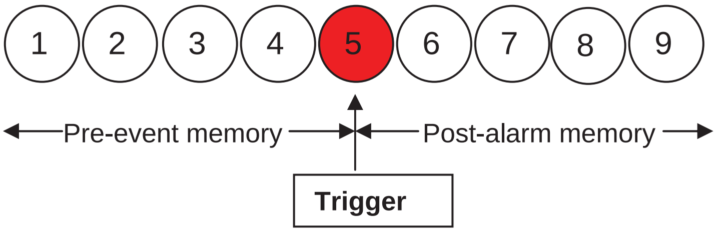
- Prefix: see file name prefix
- Y: placeholder for year, YYYY = 2009
- M: placeholder for month, MM = 11
- D: placeholder for day, DD = 15
- H: placeholder for hours, HH = 16
- M: placeholder for minutes, MM = 45
- S: placeholder for seconds, SS = 01

Video clip

“**Source**” The recording can be made from video streams 1-4.

⚠ The video stream that is configured in “Audio and Video” under “Select caching stream” is offered as a source.

“Pre-event recording” Pre-event recording interval in seconds (max. 9 seconds).
“Maximum duration” Maximum duration for each file (max. 10 seconds).



“Maximum file size” Maximum size of the file in kByte (max. 800 kByte).
“**File name prefix**” Enter a name that will prefix the video recording file name.
(see snapshot section for details)

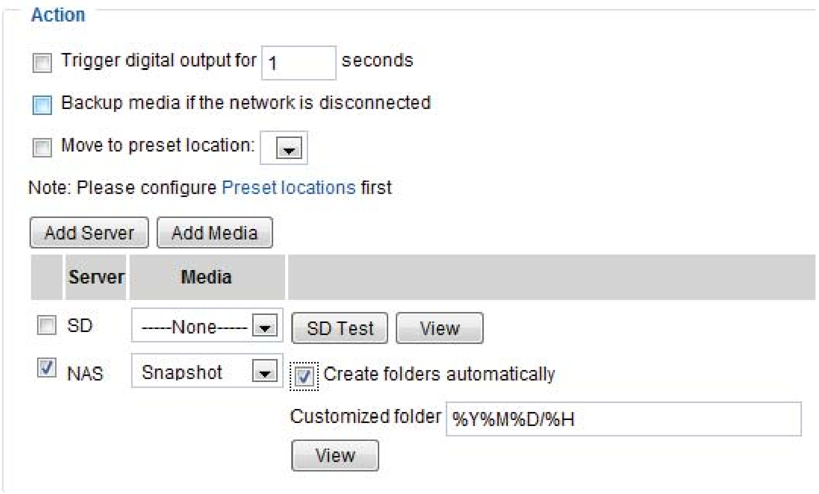
Log file

Saves the current system log contents in a text file.

Custom Message

A user-defined message in the form of a text file is sent additionally.

13.4 Action



Action

☐ Trigger digital output for 1 seconds

☐ Backup media if the network is disconnected

☐ Move to preset location: ▾

Note: Please configure Preset locations first

	Server	Media	
☐	SD	-----None----- ▾	SD Test / View
☑	NAS	Snapshot ▾	☑ Create folders automatically Customized folder %Y%M%D/%H View

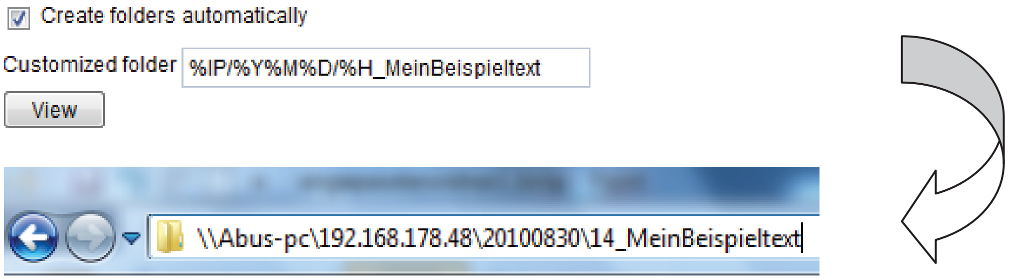
Here, you can configure the action that is to be executed if an alarm has been triggered.
“Trigger digital output for” When this option is enabled, the relay output for the video server is activated.
“Move to preset location” A preset location is activated when the alarm is triggered.
“Server” the selected medium is sent on a particular server (e.g. an email is sent with a snapshot).

“Create folders automatically” Folders are automatically created in the directory of the network drives

“Customized folder” The unique name of the folder is determined using variables.
The variables that are available can be found in the table below.

Symbol	Example/function
/	*Create a new folder*
%IP = IP address	*192.168.0.1*
%N = Event name	*Motion_W1*
%Y = Year	*2010*
%M = Month	*03*
%D = Day	*04*
%H = Hour	*14*
“Example text”	*“Example text”*

Example:
The following entry would generate this path.



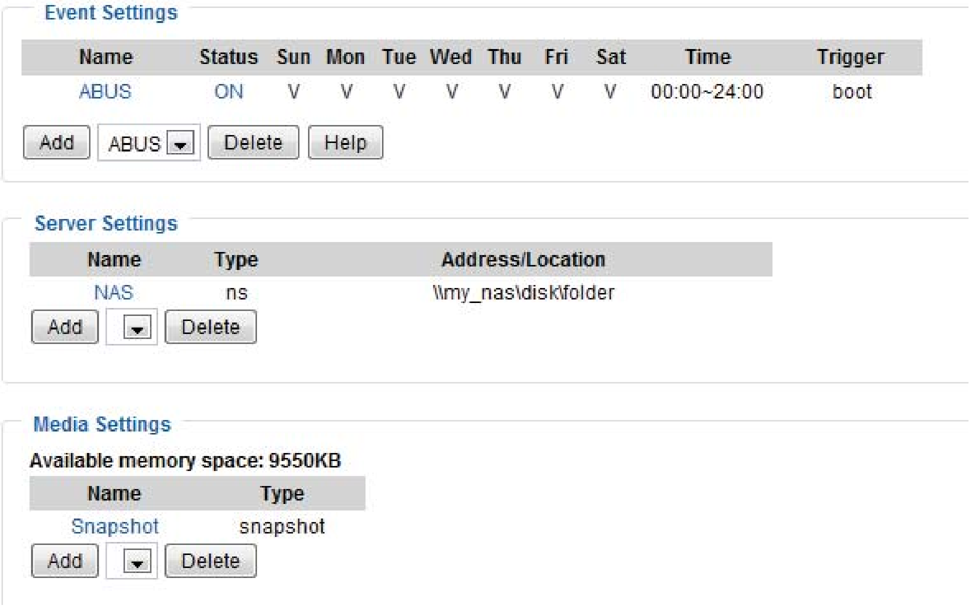
☑ Create folders automatically

Customized folder %IP/%Y%M%D/%H_MeinBeispieltext

\\Abus-pc\192.168.178.48\20100830\14_MeinBeispieltext

13.5 Application overview

Here, you can view all the “Events”, “Media types” and “Servers” that are configured in the video server. You can check, delete and add the different settings here.
You can also check the different parameters such as name, status, trigger, address.



Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	boot

Server Settings

Name	Type	Address/Location
NAS	ns	\\my_nas\disk\folder

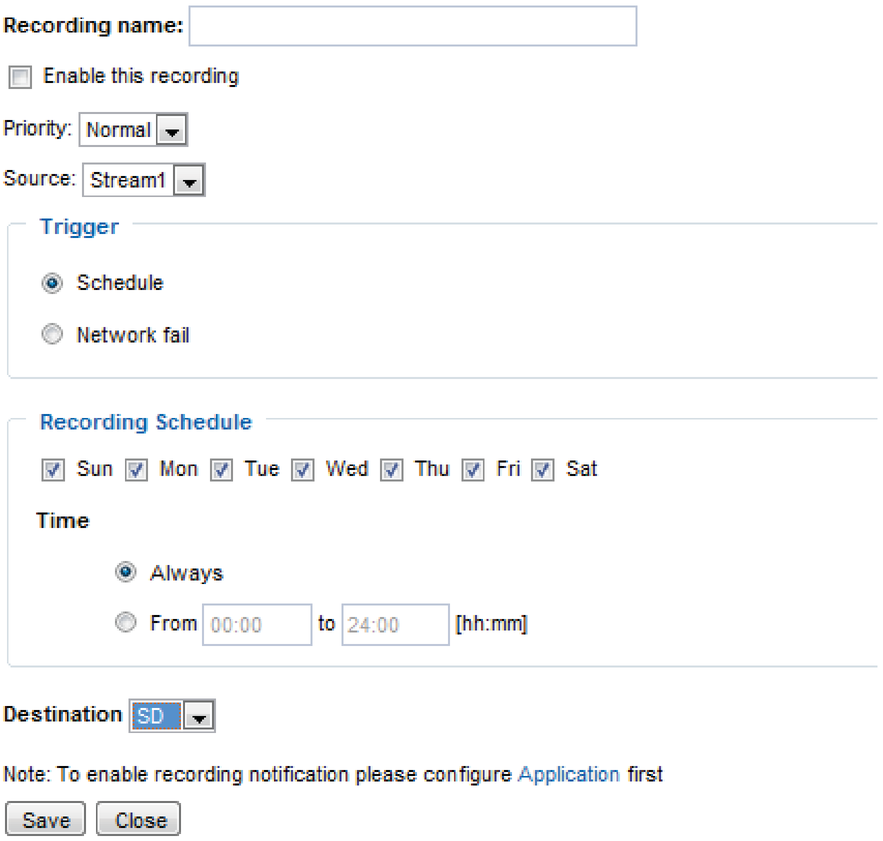
Media Settings

Available memory space: 9550KB

Name	Type
Snapshot	snapshot

14. Recording

The recording section allows you to set up recordings with the option of setting up permanent video recordings for SD cards or network shares. You can save up to 2 video settings in the video server.
Click **“Add”** to create a new recording.



Recording name:

□ Enable this recording

Priority: Normal

Source: Stream1

Trigger

● Schedule

○ Network fail

Recording Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

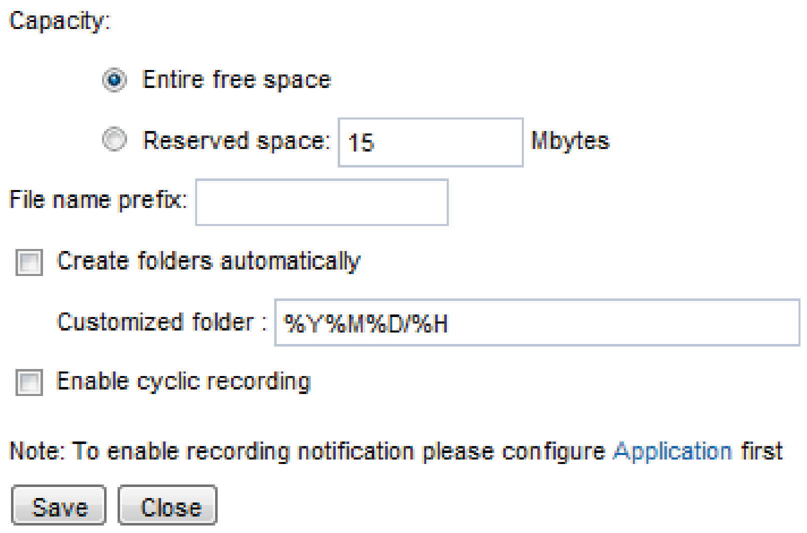
● Always

○ From 00:00 to 24:00 [hh:mm]

Destination SD

Note: To enable recording notification please configure Application first

Destination: **“Network drive”**



Capacity:

● Entire free space

○ Reserved space: 15 Mbytes

File name prefix:

□ Create folders automatically

Customized folder : %Y%M%D/%H

□ Enable cyclic recording

Note: To enable recording notification please configure Application first

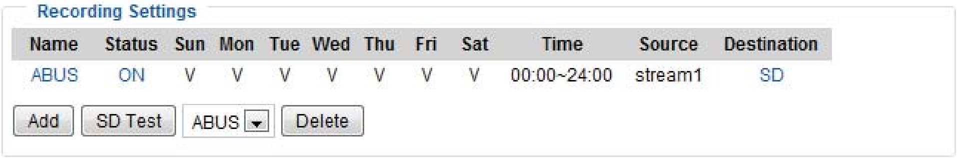
“**Recording name**” A unique name for a recording entry.
“**Enable this recording**” Select this option to activate the recording entry.
“**Priority**” Recordings with a higher priority are executed first.
“**Source**” The recording can be made from video streams 1-4.
“**Schedule**” The recording schedule is used.
“**Network fail**” If a network error occurs, the data is automatically saved onto SD card.
“**Sun**” – “**Sat**” allows you to select the day of the week for a recording.
“**Always**“ Activates the recording at all times.
“**From**“ – “**to**” The recording times are restricted.
“**Destination**” SD card or network folder.
“**Entire free space**” The maximum amount of space on the destination storage medium is used.
“**Reserved space**” Defines how many MB of free memory space should be reserved.
“**Enable cyclic recording**” Activates the cyclic recording function. If the set value is reached during the data recording, the oldest data is overwritten.

For more detailed information about “Create folders automatically”, refer to section “13.4 Action”.

If the “Customized folder” option is enabled, the cyclic recording function cannot be used.

Recording overview

“Name (video)” Opens the recording configuration page.
“Status (ON)” Sets the recording status to ON or OFF.
“Destination (SD)” Opens a file list with the saved recordings.



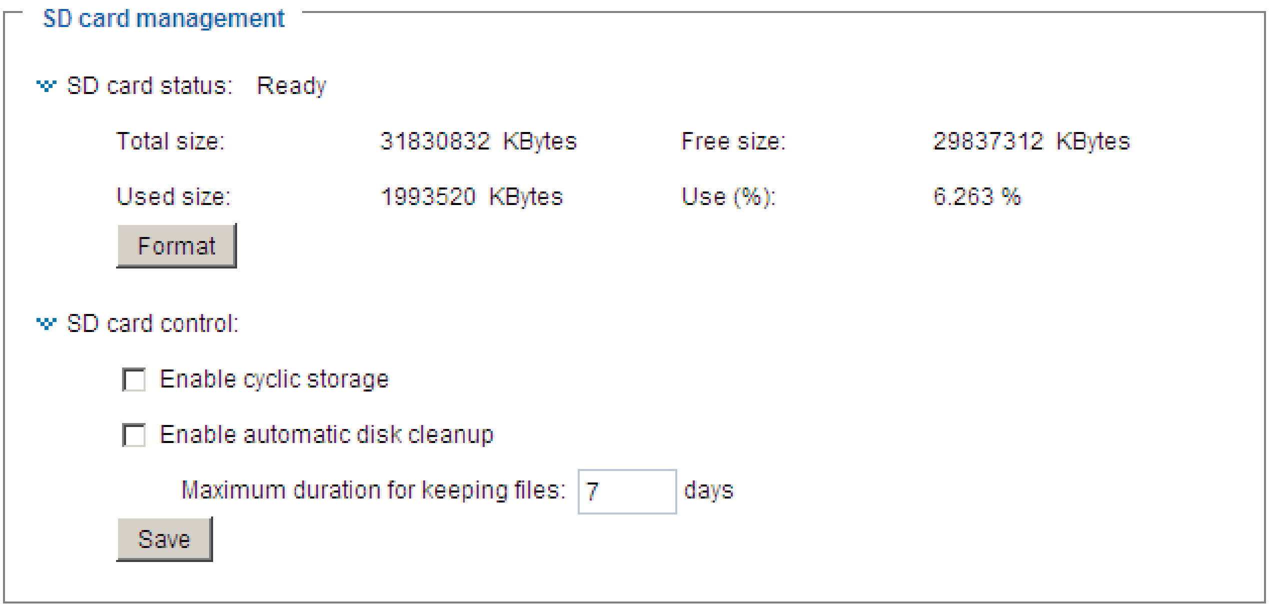
Recording Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
ABUS	ON	V	V	V	V	V	V	V	00:00~24:00	stream1	SD

15. Local memory

This section explains how you can manage the local memory (SD card) of the video server. Cards of type SD/SDHC Class 6 of up to 32 GByte are supported.

SD card management



SD card management

SD card status: Ready

Total size:	31830832 KBytes	Free size:	29837312 KBytes
Used size:	1993520 KBytes	Use (%):	6.263 %

Format

SD card control:

□ Enable cyclic storage

□ Enable automatic disk cleanup

Maximum duration for keeping files: 7 days

Save

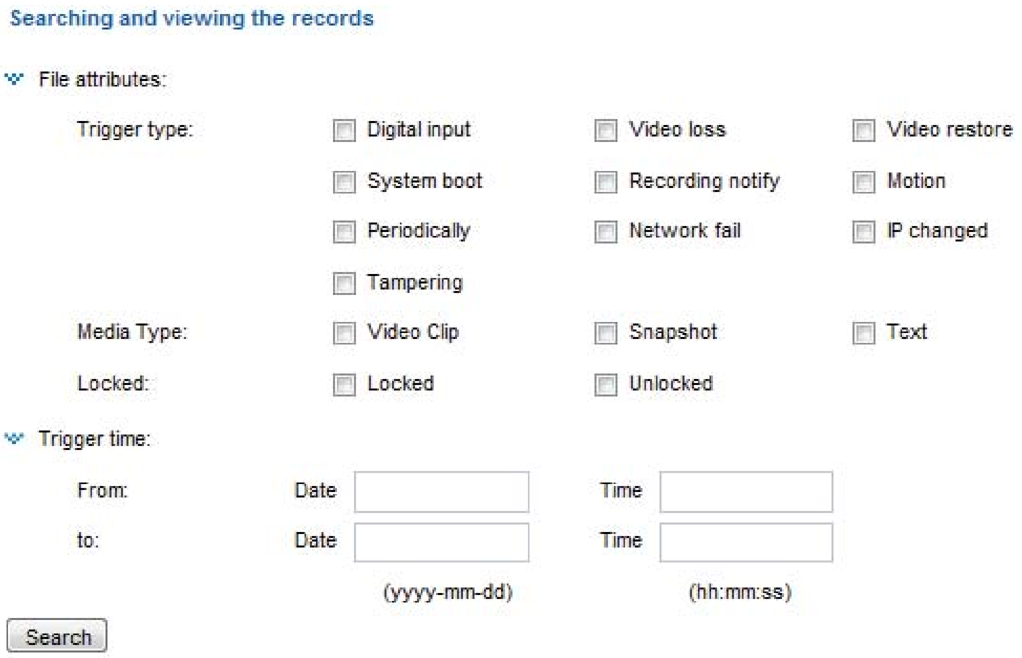
Use the **"Format"** function if you are using the card in the video server for the first time.

Select the **"Enable cyclic storage"** option if the oldest data should be overwritten when the storage capacity of the SD card is full.

If you select **"Enable automatic disk cleanup",** the contents of the SD card are deleted after the maximum duration for keeping files is reached.

Searching and viewing the records

If no criteria are selected, the list of results will always include all recordings.



Searching and viewing the records

File attributes:

Trigger type:	□ Digital input	□ Video loss	□ Video restore
	□ System boot	□ Recording notify	□ Motion
	□ Periodically	□ Network fail	□ IP changed
	□ Tampering		
Media Type:	□ Video Clip	□ Snapshot	□ Text
Locked:	□ Locked	□ Unlocked	

Trigger time:

From:	Date		Time	
to:	Date		Time	
		(yyyy-mm-dd)		(hh:mm:ss)

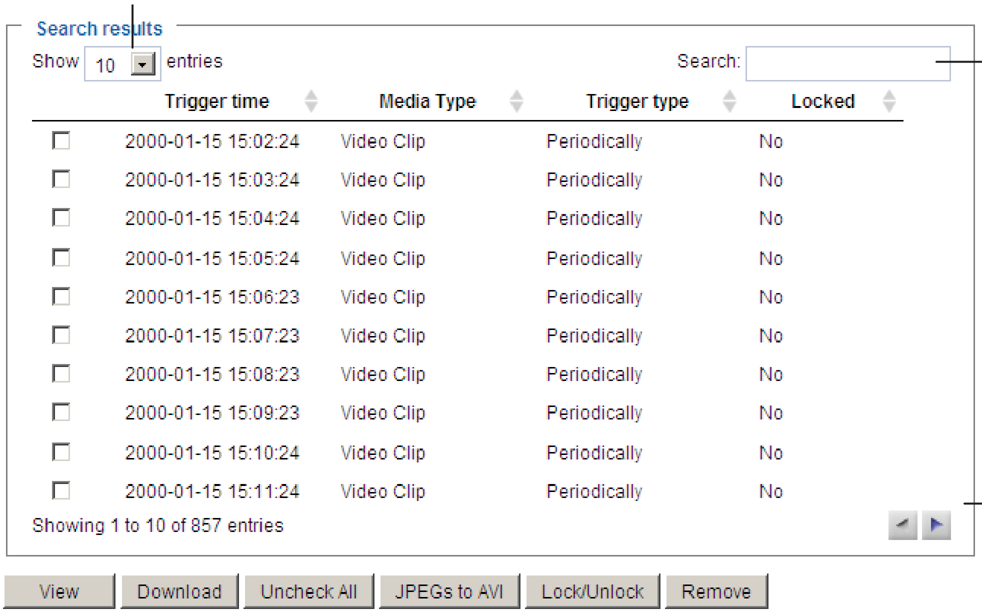
Search

“Trigger type” Select one or more characteristics which apply to a recording that was made on the SD card.
“Trigger time” Select the desired period.

Click “Search”. All the recordings that meet your criteria are displayed in the list of results.

List of results

Number of entries on one page



Search

Scroll pages

Search results

Show 10 entries Search:

	Trigger time	Media Type	Trigger type	Locked
□	2000-01-15 15:02:24	Video Clip	Periodically	No
□	2000-01-15 15:03:24	Video Clip	Periodically	No
□	2000-01-15 15:04:24	Video Clip	Periodically	No
□	2000-01-15 15:05:24	Video Clip	Periodically	No
□	2000-01-15 15:06:23	Video Clip	Periodically	No
□	2000-01-15 15:07:23	Video Clip	Periodically	No
□	2000-01-15 15:08:23	Video Clip	Periodically	No
□	2000-01-15 15:09:23	Video Clip	Periodically	No
□	2000-01-15 15:10:24	Video Clip	Periodically	No
□	2000-01-15 15:11:24	Video Clip	Periodically	No

Showing 1 to 10 of 857 entries

“View” Shows the selected recording in a new window.
“Download” Allows you to download the selected recording.
“JPEGs to AVI” You can select several JPEG single picture recordings (selection box) and convert these into an AVI file.
“Lock/Unlock” Individual recordings can be locked. Locked recordings will not be overwritten through cyclic storage. Press the button again (unlock) to remove this attribute.
“Remove” The selected recording is deleted.

You can also evaluate the data stored on the SD card using the SD card reader on your PC. The recorded data is displayed according to file type with the date and time in the file name.

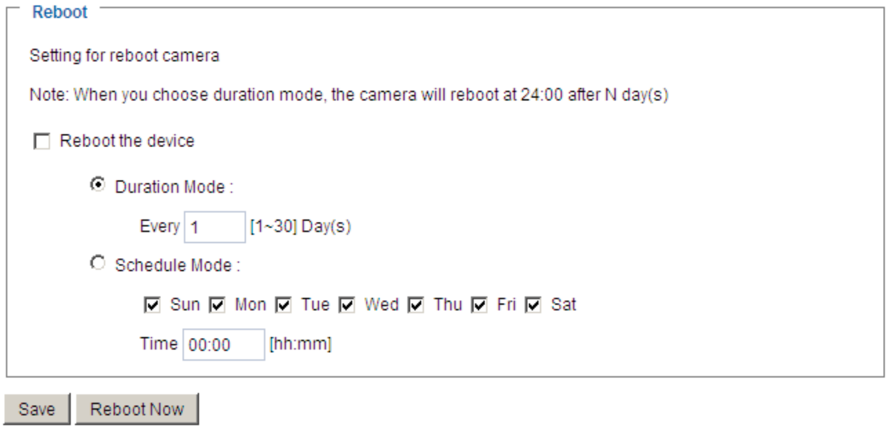
16. Log file

Click this link on the configuration page to display the system log file. The contents of the file supply useful information about the configuration and the connection following a system start. The standard of the log file is RFC 3164. You can also send data to a log server. Enable “Remote Protocol” and enter the IP address and the port number of the server.

17. Parameter list

Click this link on the configuration page to display all system parameter sets. This information can be provided for support cases.

18. Management



Reboot

Setting for reboot camera

Note: When you choose duration mode, the camera will reboot at 24:00 after N day(s)

□ Reboot the device

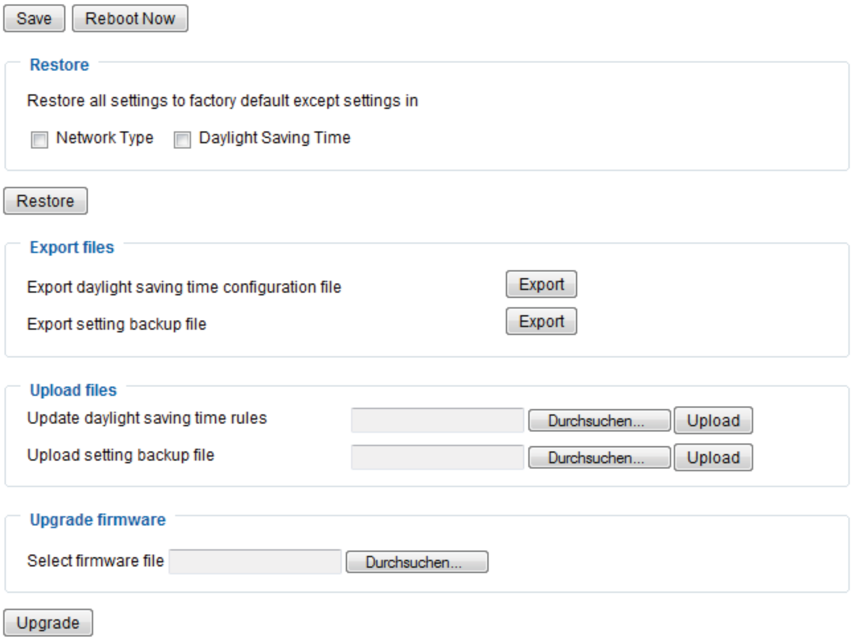
● Duration Mode :

Every 1 [1~30] Day(s)

○ Schedule Mode :

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time 00:00 [hh:mm]



Restore

Restore all settings to factory default except settings in

□ Network Type □ Daylight Saving Time

Export files

Export daylight saving time configuration file

Export setting backup file

Upload files

Update daylight saving time rules

Upload setting backup file

Upgrade firmware

Select firmware file

Reboot

Press the “Reboot Now” button to restart the video server. You can also configure an automated device reboot. This may be helpful if network problems occur. We recommend rebooting the video server on a weekly basis if you experience problems.

Restore

Click to restore the factory settings. All previous settings are discarded.

Export files

Press to export your video server settings into a file. You can also export and save the daylight saving time configuration file.

Upload files

Press “Browse...” and select the correct configuration file.
Then press “Upload” and wait until the settings have been restored.

Upgrade firmware
Like an update with the installation wizard, you can update the firmware of the video server here. You can download the latest firmware from www.abus-sc.com. Select the firmware file (*.pkg) and press “Upgrade”. The update takes a short time. When you restart the video server, it is started with the new firmware.

Never disconnect the video server from the power supply during an firmware upgrade, otherwise you risk causing irreparable damage.
A firmware upgrade can last up to 10 minutes.

19. Maintenance and Cleaning

19.1 Function Test

Regularly check the technical safety of the product, e.g. check the housing for damage.

If safe operation is no longer possible, cease operating the product and safeguard it against accidental operation.

Safe operation is no longer possible if:

- the device shows visible damage,
- the device no longer functions, and
- the device has been stored in adverse conditions for a long period of time, or
- the device has been subject to stress during transportation.

This product is maintenance-free for you. There are no components to service or anything inside the product to check. Never open it.

19.2 Cleaning

Clean the device with a clean, dry cloth. The cloth can be dampened with lukewarm water if it gets dirty.

Make sure that liquid does not get into the inside of the device as this will cause damage.
Do not use any chemical cleaning products as this could damage the surface of the housing.

20. Disposal

Devices that have been marked accordingly may not be disposed of as domestic waste. At the end of its service life, dispose of the product according to the applicable legal requirements.
Please contact your dealer or dispose of the products at the local collection point for electronic waste.

21. Technical data

Model number	TVIP40000
Camera type	Videoserver
Resolution	QCIF, CIF, 4CIF, D1 176 x 144 – 720 x 576 (intermediate levels can be freely selected)
Pixels (total)	720x576
Pixels (effective)	720x576
Digital zoom	4 x
Image compression	H.264, MPEG-4, MJPEG
Frame rate	H.264 720X480@30FPS, 720x576@25FPS
	MPEG-4 720X480@30FPS, 720x576@25FPS
	MJPEG 720X480@30FPS, 720x576@25FPS
Video norm	PAL, NTSC
Number of parallel streams	4
Number of maximum users	10
Motion detection	3 zones
Pre-alarm/post-alarm memory	Yes
Image overlay	Date, camera name, private zones
Alarm inputs (NO/NC)	1
Digital output	1 (12VDC@400mA)
Audio	Audio output (Speaker Out), audio input, 2-way audio
Alert message	E-mail / FTP / HTTP notification / relay output / NAS drive / SD card
Supported browsers	Mozilla Firefox or Internet Explorer 6.x and higher
Software supported	eytron VMS, ONVIF support
SD card	max. 32 GB (SD/SD-HC)
RS-485 port	Yes
PTZ protocols	Pelco D, Pelco P, LiLin, Samsung scc643, DynaDome / SmartDome
Network connection	RJ45 Ethernet 10/100 Base-T with PoE
Network protocols	IPv4, IPv6, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, CoS, QoS, SNMP, 802.1X
Encryption	HTTPS SSLv3
Access protection	IP address filter, user name, password, 3 authorisation levels
Power supply	12 VDC, 24 VAC, 802.3af PoE
Current consumption	Max. 5.0 Watt
Operating temperature	0 °C ~ 55 °C
Dimensions (W x H x D)	75 x 35 x 150 mm
Certification	CE, RoHS, C-Tick

22. URL Commands

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. Please refer to Appendix for complete URL command list.

23. License information

We point at the fact that the videoserver TVIP40000 among other things include Linux software source codes that are licensed under the GNU General Public Licence (GPL). To assure a GPL compliant usage of the used source codes we point at the licence terms of GPL.

Licence text

The licence text of the GNU General Public Licence can be found on the included software CD or on the ABUS Security-Center Homepage under http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL

Source Code

The used source codes are available on the ABUS Security-Center Homepage under
http://www.abus-sc.de/DE/Service-Downloads/Software?q=GPL
for free download.

Operation of the total system

With a download of the software packages (source codes) it is not possible to built a running total system. Therefore additional software applications and the network video server hardware is needed.

24. Technology license information

H.264, MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

H.264, MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE H.264, MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. SEE HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:
TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM